Facultad de Jurisprudencia

Maestría en Derecho Laboral y de la Seguridad Social

El derecho a la intimidad del trabajador como límite al control empresarial ante el uso de herramientas tecnológicas y la Inteligencia Artificial: Estudio comparado de la regulación en Colombia y España.

Presentado por:

Sofía Jazmín Erazo Herrera

Wilfredo Sanguineti Raymond (Universidad de Salamanca)
Adriana Camacho Ramírez (Universidad del Rosario)

Bogotá, D.C. 1 de junio de 2026

Facultad de Jurisprudencia

Maestría en Derecho Laboral y de la Seguridad Social

El derecho a la intimidad del trabajador como límite al control empresarial ante el uso de herramientas tecnológicas y la Inteligencia Artificial: Estudio comparado de la regulación en Colombia y España.

Modalidad: Estancia Académica Internacional (Universidad de Salamanca) – Cohorte 2025/2026

Presentado por:

Sofía Jazmín Erazo Herrera

Bajo la tutoría de:

Carlos Parrado Delgado

Bogotá, D.C. 1 de junio de 2026

Tabla de contenido

Declaración de originalidad y autonomía

Declaro(amos) bajo la gravedad del juramento, que he(mos) escrito el presente trabajo sustenta la propuesta de solución a una problemática en el campo de conocimientos del programa de Maestría por mi(nuestra) propia cuenta y que, por lo tanto, su contenido es original.

Declaro(amos) que he(mos) indicado clara y precisamente todas las fuentes directas e indirectas de información y que este PAE no ha sido entregado a ninguna otra institución con fines de calificación o publicación.

Firma digital

Sofía Jazmín Erazo Herrera

Firmado en Bogotá, D.C. el 1 de junio de 2026

Declaración de exoneración de responsabilidad

Declaro(amos) que la responsabilidad intelectual del presente trabajo es exclusivamente de su(s) autor(es). La Universidad del Rosario no se hace responsable de contenidos, opiniones o ideologías expresadas total o parcialmente en él.

Firma digital

Sofía Jazmín Erazo Herrera

Firmado en Bogotá, D.C. el 1 de junio de 2026

Resumen Ejecutivo

El derecho a la intimidad del trabajador como límite al control empresarial ante el uso de herramientas tecnológicas y la Inteligencia Artificial: Estudio comparado de la regulación en Colombia y España

La digitalización del entorno laboral transformó la forma como se ejecuta el trabajo humano, obligando al derecho laboral a replantear los mecanismos de protección de los derechos intrínsecos al contrato de trabajo y aquellos inherentes al ser humano. Es así como la implementación de dispositivos digitales en la ejecución de la labor contratada y la posibilidad de que el empresario acceda a información que estos almacenan, lleva a cuestionarse para qué fines puede emplear la misma, así como, qué garantías prevén los ordenamientos jurídicos colombiano y español para la protección de los derechos inespecíficos de los trabajadores, como lo es, el derecho a la intimidad o a la autodeterminación informativa.

Palabras clave

Control empresarial; intimidad del trabajador; autodeterminación informativa, protección de datos personales; digitalización del trabajo; vigilancia tecnológica.

Abstract

The digitalization of the work environment transformed the way human labor is carried out, compelling labor law to reconsider the mechanisms for protecting rights intrinsic to the employment contract as well as those inherent to the human being. In this context, the use of digital devices in the performance of contracted work, and the possibility that employers may access the data these devices store, raises the question of the purposes for which such information may be used, as well as what safeguards colombian and spanish legal systems provide for the protection of workers' non-specific rights, such as the right to privacy and informational self-determination.

Key words

Management authority; worker privacy; informational self-determination, personal data protection; digitalization of work; technological surveillance.

1. Introducción.

Tras la cuarta revolución industrial, los procesos productivos variaron por la introducción de tecnologías que automatizaron los mismos, sin que la maquinaria precise de la supervisión humana. Incluso, autores analizan el inicio de una quinta revolución industrial producto de la aplicación de la IA y la robótica al sector industrial (Carro Suárez & Sarmiento Paredes, 2022).

Es en este contexto que los derechos inespecíficos, que no son exclusivos de las relaciones laborales, pero sí son inherentes a todos los ciudadanos (Palomeque López & Álvarez de la Rosa, 2008, pp. 113 - 114), hallaron un nuevo relieve, pues trasladar la actividad del trabajador a través de herramientas tecnológicas, incidió en la forma en cómo se ejerce el poder de dirección e inspección del empresario al paso que abrió la posibilidad de este a acceder a información privada y semiprivada de los trabajadores.

Es por ello que el tratamiento de datos personales, con los cuales se identifica a una persona (López Balaguer & Ramos Moragues, 2020), debe regularse en una normativa clara y no dejarse al arbitrio de las partes, pues recurrir a los medios de intercambio de información para ejecutar las actividades contratadas atañe el potencial riesgo de su destinación indebida en la medición del desempeño laboral o en los procesos organizativos del trabajo (Baz Rodríguez., 2021).

Es preciso cuestionarse entonces para qué fines pueden emplearse los datos que se tratan cuando se utilizan herramientas digitales o la inteligencia artificial en la ejecución de la actividad contratada. En ese horizonte, el objetivo general de la investigación es analizar desde un enfoque de derecho comparado entre Colombia y España, cuáles son los límites al control empresarial que se ejecuta a través de herramientas tecnológicas.

De manera específica, se busca examinar el alcance del derecho a la intimidad y la protección de datos personales del trabajador en un entorno laboral digitalizado. Para el efecto, se analizará el marco jurídico colombiano aplicable al control empresarial en relación con el uso de herramientas tecnológicas. En contraste, se estudiará la regulación española en materia de privacidad del trabajador y control tecnológico; identificarán las similitudes y diferencias entre ambos sistemas jurídicos; para finalmente identificar los principales retos jurídicos de la legislación actual.

Así, la pregunta de investigación se formula en los siguientes términos: ¿Cuáles son los límites al control empresarial en el uso de herramientas tecnológicas frente al derecho a la privacidad del trabajador, de acuerdo con la legislación colombiana y española?

En este sentido, se plantea como hipótesis que el ordenamiento jurídico colombiano protege el derecho a la intimidad y del *habeas data* del trabajador en normativas generales. Sin embargo, la regulación específica sobre los límites en el uso de herramientas tecnológicas no se encuentra desarrollada en detalle. Ello da espacio a un margen amplio de interpretación respecto del alcance del poder de dirección del empleador en relación con el acceso y la gestión de la información almacenada en dispositivos digitales que se utilizan en la cadena de producción.

Por su parte, la legislación española presenta un desarrollo más específico en la materia, principalmente a partir de su constitución nacional, el Estatuto de los Trabajadores, el Reglamento General de Protección de Datos (RGPD) y el Reglamento de Inteligencia Artificial (RIA), que definen parámetros más precisos sobre la gestión de la información del trabajador.

Esta investigación se desarrolla bajo un enfoque cualitativo de carácter jurídico, centrada en el análisis normativo, doctrinal y jurisprudencial de la protección del derecho a la intimidad y autodeterminación informativa del trabajador en el marco de carácter comparado. Por ello, se eligió

un método jurídico-dogmático, para analizar el contenido de normas constitucionales, legales y reglamentarias vigentes en Colombia y España, así como su interpretación por parte de la doctrina y los criterios jurisprudenciales de las autoridades judiciales, lo que permite identificar las similitudes y diferencias en la regulación bajo estudio.

Con tal objeto, se desarrollaron cuatro capítulos, el primero de ellos, sobre el contexto de la definición del poder de dirección del empleador en relación con el uso de dispositivos electrónicos y automatizados; el segundo, para desarrollar la normativa colombiana actual; el tercero relativo a la normativa española; y, el cuarto consistente en un análisis de derecho comparado, al cabo de los cuales se arribará a un acápite de conclusiones.

2. Poder de dirección del empleador.

La transformación del sector productivo ocasionada por el avance de las TIC y herramientas automatizadas, consolidó modelos de control diferentes al clásico presencial, el cual fue desplazado por sistemas digitales para objetivos como la medición de la productividad (Ballesteros, 2017). En consecuencia, la subordinación[1] entendida desde su concepción tradicional como la facultad de dar órdenes en cuanto al modo, tiempo y lugar de la prestación del servicio (Hernández Rueda, 1997), mutó, pues ésta ya no se dedica a vigilar el cumplimiento de horarios o exigir la presencia en el

[1] La doctrina ha definido distintas clases de subordinación. Por ejemplo, el autor Jaramillo Jassir en su libro del 2011, recogió los conceptos desarrollados en un inicio por Lodovico Barassi en su libro "*Il Contratto di Lavoro nel Diritto Positivo Italiano*", analizando las distintas modalidades de la subordinación, a saber, la técnica entendida como el control "*técnico-funcional*" sobre las condiciones operativas; la económica que es la dependencia del trabajador al ingreso obtenido con su labor; o, la jurídica definida cómo la facultad de imponer órdenes y variar las condiciones del trabajo.

sitio de trabajo, sino que conlleva la verificación del cumplimiento de objetivos previamente definidos.

Sin embargo, esta facultad no es ilimitada, pues los derechos inespecíficos aún representan un freno al control empresarial, incluso cuando este se despliega por medios tecnológicos en ejercicio de la libertad de empresa (Jiménez Silva et al., 2022).

Dicha modificación en la dinámica de la relación laboral precisa de límites jurídicos claros al poder de dirección, bien sea constitucionales, legales o convencionales, pues el trabajador en ningún momento deja de ser titular de las prerrogativas inherentes al ser humano (Frías, 2020). Es por ello, que el ordenamiento jurídico debe responder a la necesidad de armonizar, por un lado, la libertad de empresa, y por otro, la protección de los trabajadores, para que al incorporar medios tecnológicos en el proceso productivo no derive en la vigilancia desproporcionada de aquel.

Como sería el caso de los medios digitales a través de los cuales se recopila información personal, como los sistemas de geolocalización, videovigilancia sistemas, biométricos y el uso de dispositivos corporativos o personales para la ejecución de la actividad, cuya destinación debe responder a un fin consentido y legítimo para mantener un equilibrio entre la intimidad del trabajador y la supervisión del empleador, ajustando ésta última conforma a criterios de proporcionalidad y necesidad (Aguilera, 2020).

Otro escenario a considerar, es que en la práctica, los sistemas de vigilancia operan de manera automatizada, lo que hace que la actividad del trabajador se registre de forma indefinida durante la jornada laboral (Baz, 2021). A raíz de esto, el volumen de datos recopilados a través de los medios de interfaz inmediata dificulta su adecuado almacenamiento y tratamiento responsable. En conjunto, estas circunstancias muestran que el control digital, aunque es una herramienta útil

para la organización del trabajo, requiere de límites para su aplicación que respondan al nuevo contexto laboral digitalizado (Frías Ávila, 2020).

3. Protección de la intimidad y de los datos en Colombia.

En Colombia, la tutela al derecho a la intimidad está consagrada en el artículo 15 de la Constitución Política, dirigida a amparar a los individuos en su ámbito personal, familiar y el "*buen nombre*" (Asamblea Nacional Constituyente, 1991). Este precepto impuso en cabeza del Estado la obligación de salvaguardar tales prerrogativas de las intromisiones propias o de terceros. Igualmente, reconoció a sus titulares el derecho a determinar cómo debe tratarse su información, como expresión del ejercicio del derecho a la autodeterminación informática o *habeas data*, que por desarrollo jurisprudencial adquirió la categoría de derecho autónomo separado del derecho a la intimidad y la connotación de irrenunciable, so pena de viciar de nulidad absoluta cualquier acto dispositivo de aquel (Corte Constitucional, Sentencia C-748/2011).

En un inicio, el ordenamiento colombiano sólo protegía los datos de origen financiero a través de la Ley 1266 de 2008, (Congreso de la República de Colombia, 2008). Posteriormente, la Ley Estatutaria 1581 de 2012 instauró un régimen general que expandió el alcance el amparo a datos administrados por entidades públicas o privadas, salvo por contadas excepciones como los datos almacenados en bases de uso personal, los de seguridad pública o periodística. También previó una clasificación de los datos sensibles y públicos (Congreso de la República de Colombia, 2012).

En punto a los principios, esta disposición recoge en su artículo 4º, los de "*legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y*

confidencialidad" (Congreso de la República de Colombia, 2012). Estos, están encaminados a que el titular pueda determinar, conocer, y en especial, consentir los fines para los cuales se destinará su información, mediante mecanismos de protección como el conocimiento previo e informado respecto al uso del dato salvo por disposición legal o judicial que lo sustituya, o la garantía de conocer y revisar la información tratada que no esté sometida a reserva, la cual, en todo caso, no le es oponible a su titular.

Aquellos también son un límite para el encargado de tratar la información, e imponen obligaciones como la de adoptar medidas para evitar la adulteración del dato, su acceso no autorizado o la de informar con suficiencia al titular de la información sobre su destinación y mantener la reserva de la misma.

La Corte Constitucional ha estructurado una línea clara respecto a la gestión de la información, estructurando un régimen de protección que varía según la naturaleza del dato. En este sentido, ha determinado que la información pública se enmarca en el ejercicio amplio del derecho a ser informado bajo la égida del artículo 20 de la Constitución Política, lo cual presupone su acceso libre, sin la intimidad constituya un freno a su divulgación.

Por el contrario, la información privada al residir en el núcleo esencial de la privacidad, goza de una protección reforzada bajo los artículos 15 y 250 superiores, de modo que su obtención se encuentra supeditada a una orden judicial o autorización expresa del titular. Bajo este mismo esquema de reserva, los datos sensibles adquieren la categoría de información reservada, para evitar posibles escenarios de discriminación.

Dentro de esta taxonomía, surge la categoría de información semiprivada, en la que se incluyen los datos que no son íntimos, reservados ni estrictamente públicos. Se diferencia por cuanto su conocimiento puede interesar a un grupo específico o en general a la sociedad, de manera

que son de circulación restringida, y por tanto, su acceso está vinculado al cumplimiento de una función por quien pretende conocerlas.

Para definir los contornos de protección de la intimidad, la jurisprudencia constitucional distingue los espacios "*públicos, privados, semiprivados y semipúblicos*", según el intercambio, interacción o integración de los ciudadanos En cuanto al lugar de trabajo, clasifica este espacio en la categoría de "*semiprivado*" (Corte Constitucional, Sentencia T407/2012).

También la Corte Constitucional concluyó que el acceso a la información contenida en un dispositivo digital suministrado a una trabajadora para el ejercicio de sus funciones, sin su autorización, transgredió su derecho a la intimidad porque el depósito transitorio de la información en el computador institucional no se traduce en un consentimiento implícito para su acceso y divulgación (Corte Constitucional, Sentencia T-405/2007).

En contraste, en la sentencia T 768 de 2008, al conocer del caso de un trabajador que fue grabado sin su autorización con una cámara ubicada fuera del circuito de monitoreo, determinó que este no sufrió afectación alguna porque no es posible asimilar la protección extendida al lugar de trabajo con la del domicilio, pues en el entorno laboral las actividades trascienden la esfera individual. Es así como el carácter semipúblico de las relaciones de trabajo determina el goce del derecho a la privacidad en relación con las facultades de supervisión del empleador (Corte Constitucional, Sentencia T-768/2008).

Sin embargo, en la sentencia T 574 de 2017, en cuanto a los sistemas de mensajería instantánea precisó que no es posible definir el alcance de la protección con total exactitud a partir de los criterios anteriores. De modo que en estos contextos acudió al criterio denominado "*expectativa de privacidad*", propio del derecho norteamericano para establecer si determinadas

expresiones son propias de la intimidad o pueden ser conocidas por otros en cada caso (Corte Constitucional, Sentencia T-574/2017).

Para tal fin, el órgano de cierre constitucional realizó un doble análisis, de carácter subjetivo en cuanto a la confianza del titular en la reserva de la información, y objetivo, sobre la oponibilidad de ello a terceros. En torno a esta expectativa, estableció criterios de ponderación como el nivel de apertura del sistema de mensajería, el número de miembros o fines de un grupo en un espacio virtual, la clase de información, si está comprendida bajo los supuestos de los regímenes especiales, la existencia de un acuerdo previo sobre la circulación de la información; y, si existe una obligación de sigilo o reserva por disposición legal o contractual.

En materia laboral, el Código Sustantivo del Trabajo, en el literal b) de su artículo 23, contempla que "*el honor, la dignidad y los derechos mínimos del trabajador o trabajadora*" son un límite a la potestad de dirección del empleador, con arreglo a la normativa internacional en materia de derechos humanos. También, el derecho a la intimidad se enlista en el artículo 115, como uno de los límites a su poder sancionatorio.

Desde la Ley 1221 de 2008, se reguló en Colombia el desempeño de la actividad laboral por medio de Tecnologías de la Información y la Comunicación, sin que se requiera de la asistencia del trabajador en el sitio de trabajo. Este precepto en su artículo 6º recoge el principio de trato igualitario de estos trabajadores en procura de derechos, como por ejemplo, a la intimidad y privacidad.

Por su parte, la reforma al Código Sustantivo del Trabajo de la Ley 2466 de 2025, entre sus artículos 24 a 30, reglamentó el trabajo en plataformas digitales de reparto. Específicamente, el artículo 26, impuso al empleador la obligación de crear un mecanismo para reconocer e individualizar plenamente al trabajador que ejecuta su actividad en esas condiciones. Dicho sistema

quedó sujeto al derecho al *habeas data*, que para su protección autoriza la remisión expresa a la regulación general antes expuesta.

También el artículo 29 que desarrolla el principio de la transparencia cuando se emplean sistemas automatizados, sea para la supervisión o para la toma de decisiones, contempla el deber de informar a los trabajadores digitales sobre el uso de estos medios para parametrizar su actividad y cuando se apoye en ellos para la toma de decisiones que influyan en las condiciones del trabajo, en cuanto al tiempo, cantidad o remuneración, entre otros aspectos.

En desarrollo de lo anterior, ordena al empresario que suministre esta información en un documento que sea claro, comprensible y verídico, e igualmente, que garantice su fácil acceso. Dispone a continuación frente al tratamiento de datos personales que solamente está autorizado para el efecto, siempre y cuando, se ajuste a los fines previamente consentidos por el trabajador.

No obstante, en lo que atañe al uso de la inteligencia artificial, aún no se cuenta con regulación específica. Actualmente el Congreso debate el proyecto de Ley No. 274 de 2025, acumulado con el No. 214 de ese mismo año, por medio del cual se pretende modificar la Ley 1581 de 2012 para ampliar su espectro protector en respuesta a los desafíos que trae consigo el ecosistema digital actual, caracterizado por el uso progresivo de IA que propicia la recolección masiva de información y la automatización en la toma de decisiones (Congreso de la República, 2025).

En tal sentido, justifica los ajustes a la norma en que aquella no abarca estos escenarios, por tanto, la falta de regulación puede ser aprovechada por quienes accedes a esta información que se recolecta de manera masiva sin una supervisión efectiva, amenazando prerrogativas como el derecho a la intimidad y a la "*autodeterminación informativa*", entre otros.

Para este propósito, propone una protección reforzada para el tratamiento de datos personales almacenados en cualquier sistema de información, en específico, frente a aquellos que se relacionen con una actividad comercial, la parametrización del comportamiento de su titular, su perfilamiento, la toma de decisiones automatizadas o cuando así lo determine la norma o un contrato.

En complemento de lo anterior, busca ampliar el catálogo de derechos de los titulares de los datos, incorporando garantías frente a "*decisiones automatizadas*" o de segmentación de usuarios que limiten sus derechos fundamentales o tengan un efecto discriminatorio. En estos eventos, propone que los titulares tengan el derecho a recibir información clara sobre el proceso y exigir un mínimo de intervención humana en la decisión, siempre que ello no comprometa información confidencial de la empresa.

De igual manera, propone reconocer el derecho a solicitar la supresión del dato en los siguientes supuestos, cuando esto sea prohibido o no sea debidamente autorizado; por revocatoria del titular sin que tenga otra base legítima en respaldo; o, cuando de ello dependa el goce efectivo de otro derecho fundamental. Asimismo, se plantea extender el concepto de datos sensibles para comprender en esta categoría a los datos de georreferenciación, los genéticos, los "*neurodatos"*.

En cuanto a los fines legítimos, el proyecto en cita formula como tales la necesidad de cumplir una obligación legal o la derivada de un negocio jurídico, sin perjuicio de la autorización de su titular, de debe ser previa, libre, informada, inequívoca y especifica en cuanto a los fines de su destinación, cuyo consentimiento debe ser obtenido por un medio objeto de consulta posterior.

En conjunto con el artículo 30 de la Ley 2466 de 2025, este proyecto busca igualmente imponer al responsable del tratamiento del dato, la obligación evaluar el impacto de estas herramientas automatizadas. Con esa finalidad, prevé la prerrogativa a solicitar la "*revisión*

humana" de las decisiones de estos sistemas, y en el caso específico del ámbito laboral, cuando ello incida en la ejecución del contrato de trabajo.

En conclusión, el régimen de protección del derecho a la intimidad y el *habeas data* en Colombia ha transitado desde una concepción estática hacia un modelo que pretende adaptarse a las nuevas realidades tecnológicas. Es así como el marco legal vigente, con la reciente regulación sobre plataformas digitales incorporada en la Ley 2466 de 2025, ha reforzado el deber de transparencia y el respeto a la dignidad del trabajador de plataformas digitales de reparto, ante el procesamiento automatizado de datos que plantea desafíos que superan a la normativa tradicional, pero sólo frente a ese supuesto.

Por tanto, la efectividad de estas garantías dependerá de la capacidad del sistema jurídico para transitar hacia una protección reforzada y específica, como la propuesta en los actuales proyectos de ley que buscan ampliar la aplicación de la normativa general a la protección de datos personales frente al uso medios de recopilación automatizada de la información, donde mecanismos como el consentimiento informado, previo y documentado, la expectativa de privacidad y la intervención humana en decisiones algorítmicas se convierten en los pilares que impidan que la eficiencia contrarie la autodeterminación informativa y la esfera privada del individuo.

4. Protección de la intimidad y de los datos en España.

En España, la intimidad también encuentra amparo a nivel constitucional como parte de los derechos vinculados a la esfera personal. En específico, el artículo 18 de la Constitución Española

contempla el límite al uso de la informática a efectos de garantizar "*el honor, la intimidad personal y familiar de los ciudadanos*" (Jefatura del Estado, 1978).

El artículo 1º de la Ley Orgánica 1/1982, de 5 de mayo, en desarrollo del artículo 18 superior, resaltó que los derechos al "*honor, intimidad personal, familiar y a la propia imagen*" son, entre otras características, irrenunciables, precaviendo escenarios que matizaban su ejercicio, siempre bajo autorización o consentimiento de su titular, de carácter revocable.

En materia laboral, el artículo 20.3 del Estatuto de los Trabajadores extiende al empresario la potestad de adoptar medidas de supervisión orientadas a comprobar el cumplimiento de las obligaciones, siempre bajo la égida de la dignidad. (Jefatura del Estado, 2015).

A su vez, el artículo 20 bis, añadido por la Ley Orgánica 3/2018 de 5 de diciembre, contempla el derecho a la intimidad del empleado en el ecosistema digital. Dicha disposición salvaguarda esta prerrogativa cuando se empleen dispositivos de esta clase para ejecutar la actividad contratada, o ante mecanismos de videovigilancia o geolocalización (Jefatura del Estado, 2018).

También debe tenerse en cuenta el Reglamento (UE) 2016/679 (RGPD) cuando el control involucre el tratamiento de información personal, desarrollado y adaptado al ordenamiento interno español por la Ley Orgánica 3/2018 de 5 de diciembre. Luego entonces, el poder de dirección del empleador en ese evento debe enmarcarse en los principios allí contemplados que lo limitan a fines legítimos, bajo parámetros de licitud, lealtad y transparencia en defensa del titular.

En particular, el principio de "*minimización de datos personales*", que sujeta las operaciones sobre estos a lo estrictamente necesario de conformidad con los fines para los que son gestionados; y el de seguridad que impone la obligación de garantizar una protección adecuada,

para evitar su consulta no autorizada, ilícita o su pérdida. Este precepto también enlista principios como la exactitud y el tratamiento consentido por el afectado (Reglamento UE 2016/679, 2016).

Por otro lado, el numeral 2º del artículo en mención, impone al responsable la obligación de acatar dichas exigencias y la carga probatoria de demostrarlo, "*responsabilidad proactiva*". Además, en su artículo 6º condiciona la licitud del dato al consentimiento previo de su titular frente al tratamiento para fines específicos. Entre tanto, su artículo 7º, considera como intromisiones ilegales, revelar información sensible que sea conocida por la actividad profesional u oficio del titular (Reglamento UE 2016/679, 2016).

Por otro lado, la Ley Orgánica 3/2018 de 5 de diciembre respecto a los datos especiales, dispone que el consentimiento no basta para levantar la prohibición de su tratamiento cuando se pretenda principalmente diferenciar al individuo por elementos inherentes a su personalidad, como su ideología o afiliación sindical, entre otras, salvo bajo los supuestos del artículo 9.2 del Reglamento (UE) 2016/679, de ser procedente y bajo el amparo de una Ley. En otras palabras, excluye la autocomposición de las partes en esos casos (Jefatura del Estado, 2018).

En cuanto a la intimidad y la videovigilancia, el artículo 89 de la Ley Orgánica, regula su uso como mecanismo de control de la actividad laboral, habilitando el procesamiento de imágenes para supervisar la actividad contratada dentro de los límites legales. Esta disposición se armoniza con el artículo 20.3 del Estatuto de los Trabajadores, de modo que si bien no se requiere el consentimiento el trabajador, si se impone al empleador el deber de informar suficientemente sobre la existencia del sistema de vigilancia y su finalidad (Jefatura del Estado, 2018).

Dicha obligación se satisface con la instalación de un medio informativo en el lugar de trabajo que sea visible, al menos, con la indicación de que se está recopilando la información, quien lo hace y los derechos del vigilado conforme a los artículos 15 a 22 del Reglamento (UE) 2016/679.

No obstante, se prohíbe expresamente utilizar los datos recogidos para propósitos ajenos a los inicialmente previstos, así como la instalación de estos sistemas en espacios de descanso.

Asimismo, el principio de minimización incide en la configuración de estos sistemas, ya que sus capacidades técnicas deben evitar captaciones excesivas o desproporcionadas de información. De igual forma, el acceso a las grabaciones debe limitarse al personal autorizado, a fin de impedir usos indebidos o divulgaciones no justificadas de las imágenes, como una manifestación del principio de seguridad.

Con relación a la geolocalización, el artículo 90 de la Ley Orgánica autoriza su utilización, siempre y cuando se derive del contrato de trabajo y de las facultades de dirección. En dichos casos, dispone que el trabajador debe ser informado suficientemente sobre la existencia del sistema, sus características, e igualmente los derechos inherentes a la protección de sus datos (Jefatura del Estado, 2018).

En todo caso, por virtud de los principios expuestos, cuando se emplean mecanismos de esta clase no puede destinarse la información recopilada para una finalidad distinta de la que le dio lugar. Ello implica que el tratamiento orientado, por ejemplo, al registro de la jornada, debe recaer sobre la información estrictamente necesaria para ese propósito, sin que pueda derivar en el control permanente de la localización del trabajador, pues el empleador no está habilitado para supervisar la actividad en condiciones excesivas que lleven a una vigilancia permanente. De acuerdo con este criterio, la incorporación de mecanismos de control tecnificados sólo encuentran sustento en una verdadera necesidad cuando no sea posible recurrir a mecanismos menos invasivos para alcanzar la finalidad perseguida por ese medio.

En cuanto a la inteligencia artificial, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, regula las prohibiciones y fines para la utilización de un sistema IA,

entendiendo como tal, según su artículo 3º, a cualquier "*sistema basado en máquinas*", diseñado para funcionar con cierta autonomía y "*capacidad de adaptación*", mediante la inferencia de información de entrada, en función de objetivos determinados, para generar resultados como predicciones o decisiones que potencialmente incidan en contextos virtuales o presenciales (Reglamento UE 2024/1689, 2024)

En su artículo 5º enlista las prácticas prohibidas de la inteligencia artificial, en concreto, el literal c) define como una de ellas, la evaluación o clasificación de las personas naturales o jurídicas según su comportamiento o características individuales conocidas, a través de inferencias o predicciones, de suerte que provoque un trato desfavorable en un ámbito ajeno al del origen de los datos o cuando resulte desproporcional en relación con la finalidad inicial del tratamiento.

A su vez, el literal f) proscribe su aplicación para parametrizar las emociones de las personas físicas en los lugares de trabajo, salvo por motivos médicos o de seguridad. Mientras que su literal g) proscribe su uso para la clasificación a los individuos con base en sus datos biométricos con el fin de inferir características inherentes al individuo, como su etnia, afiliación política o sindical, a menos de que se trate de una clasificación biométrica a partir de datos adquiridos de forma lícita o en cumplimiento del Derecho.

Entre tanto, su artículo 14 ordena la supervisión humana de los sistemas de IA de alto riesgo durante su uso; es decir, incluir herramientas de interfaz entre el humano y la máquina proporcionales al riesgo, nivel de autonomía y contexto, cuyo objeto es reducir al mínimo los riegos para los derechos fundamentales que puedan surgir cuando se utiliza un sistema de IA conforme a su finalidad prevista o cuando se le da un uso irrazonable previsible, cuando no corresponde a la finalidad prevista por el comportamiento humano o interacción con otros sistemas.

La jurisprudencia española asumió una posición protectora del derecho a la intimidad, entendido como el poder de excluir a terceros del acceso a la esfera personal y familiar del individuo (Moreno Bobadilla, 2016). En esa línea, el Tribunal Constitucional Español ha dejado sentado que la incorporación del trabajador a una relación laboral no supone la pérdida de su condición de sujeto de derechos fundamentales, ni habilita al empleador para intervenir indiscriminadamente en su esfera privada. De este modo, se ha consolidado la postura de que el contrato de trabajo genera una subordinación funcional, pero nunca absoluta, pues encuentra un límite claro en la dignidad del trabajador y la intimidad (Monereo Pérez, 2023).

Al respecto, la jurisprudencia ha señalado que el poder de dirección encuentra su justificación en la necesidad de organizar la actividad productiva, para cumplir el objeto del contrato de trabajo y garantizar el giro ordinario de la empresa, pero no puede extenderse hasta vaciar el contenido esencial de los derechos del trabajador. Así, el Tribunal Constitucional de España en la sentencia STC 142/1993 estableció que la intimidad no se proyecta sobre todos los aspectos de la actividad laboral, ya que quedan fuera de su núcleo los hechos relativos al desempeño del trabajador (Tribunal Constitucional de España, 1993).

Así, el Tribunal Constitucional indicó que la imposición de ciertas limitaciones al trabajador puede ser correcta cuando obedezca a obligaciones contractuales y haya una proporcionalidad en ello, como se sostiene respecto a la imposición de limitaciones en la sentencia STC 73/1982 (Tribunal Constitucional de España, 1982).

Previo al desarrollo normativo del RGPD y el RIA, el Alto Tribunal en la sentencia STC 292/2000, al estudiar la constitucionalidad de los artículos 21.1, 24.1 y 24.2 de la Ley Orgánica 15/1999 (LOPD), estableció que el derecho fundamental a la protección de datos consagrado en el 18.4 CE, incluye como elemento esencial e irrenunciable la facultad de obtener información sobre

la destinación y responsables de los datos, al paso que marcó la diferencia entre el derecho a la intimidad, entendido como "*la protección a la esfera intima*", del derecho a la "*autodeterminación informativa*", entendido como la protección de los datos, cualquiera sea su naturaleza (Tribunal Constitucional de España, 2000).

Incluso más adelante, en la sentencia STC 196/2004, declaró nulo un despido basado en una prueba obtenida en contravía al derecho a la intimidad. En esa oportunidad, puso de relieve la importancia de valorar cómo se obtiene un dato y la necesidad de contar con el consentimiento informado del trabajador sobre su tratamiento, contemplado excepciones al reconocimiento médico obligatorio en el cual se recopilan datos personales del trabajador, según la necesidad de evaluar las condiciones de trabajo sobre la salud o que su estado represente un riegos para aquel o terceros, aspectos que no pueden valorarse de forma genérica, sino que se deben justificar en cada caso (Tribunal Constitucional de España, 2004).

En la sentencia STC 29/2013, de 11 de febrero de 2013, el Tribunal Constitucional resaltó que no basta con obtener autorización para grabar al trabajador en su lugar de trabajo, sino que era preciso informarle para qué se utilizarían las grabaciones. Así, distinguió entre la licitud y la constitucionalidad del fin en desarrollo del principio de finalidad específica, pues, si bien verificar el cumplimiento del horario de trabajo de un empleado, es un fin legítimo, usar el contenido de la grabación para imponer una sanción sin que previo a ello se informara de esta posibilidad al trabajador, es contrario al artículo 18.4 de la Constitución Española (Tribunal Constitucional de España, 2013).

En la sentencia STC 61/2021, frente a la facultad de monitorizar el dispositivo tecnológico de un trabajador con fines disciplinarios, sin informarle al respecto, concluyó que ello viola su

derecho a la intimidad y secreto de las comunicaciones, aunque el empresario cuente con un permiso general para controlar el uso de los sistemas informático.

En este pronunciamiento, el Tribunal sustentó en parte su determinación en la doctrina del Tribunal Europeo de Derechos Humanos, específicamente, en el caso Barbulescu contra Rumanía de 2017, el cual dejo sentado que la monitorización empresarial de las comunicaciones sólo es admisible si se informa previamente al trabajador de esta posibilidad y si la medida es proporcional, pues su alcance no puede exceder lo estrictamente necesario para alcanzar el fin que lo justifica (Tribunal Constitucional de España, 2021).

También ha afirmado respecto al secreto de las comunicaciones, que el objeto de protección es el acto comunicativo, garantizando la libertad de intercambio frente a injerencias externas. Esto implica que el empresario no puede acceder al contenido de las comunicaciones privadas, incluso cuando se realicen a través de medios corporativos, sin vulnerar el artículo 18.3 de la Constitución Española (Díaz Revorio, 2006).

Es así como la jurisprudencia reconoce que el empresario puede ejercer facultades de vigilancia y control para verificar el cumplimiento de las obligaciones, incluso, siendo tolerables los mecanismos de control técnico sólo bajo la observancia de los principios de proporcionalidad, idoneidad y necesidad.

La transición hacia un entorno laboral digitalizado ha exigido que la jurisprudencia evolucione desde la protección del espacio físico hacia la protección de la esfera virtual y comunicativa. La adopción del RGPD y la reciente regulación de la Inteligencia Artificial (Reglamento UE 2024/1689) marcan un hito fundamental al proscribir prácticas invasivas como la inferencia de emociones o la categorización biométrica discriminatoria y a imponer una "*responsabilidad proactiv*a" al empleador.

En ese orden, la legitimidad del control empresarial está atada a que este supere el triple análisis de proporcionalidad, garantizando que el uso de mecanismos como la videovigilancia, la geolocalización o los algoritmos de supervisión no anulen la intimidad ni la autonomía informativa del individuo. También que los datos tratados en estos procesos respondan a fines legítimos y consentidos previamente por los trabajadores en procura de su derecho a la autodeterminación informática.

Otro punto que robustece al ordenamiento jurídico español es la autonomía colectiva como fuente reguladora de origen extra estatal (Palomeque. 20026). Frente este tema, tanto la disposición europea como la española, abren espacio a la autonomía colectiva para que a través de reglas más puntuales se garanticen los derechos en materia de tratamiento de información personal en contextos laborales digitalizados. Empero, como se dijo en párrafos anteriores, la Ley Orgánica 3/2018 reserva al legislador los temas relacionados con datos de categoría especial, pero si delega al diálogo social en mayor medida la regulación del derecho a la desconexión digital.

Sin embargo, autores como Sierra Hernaiz al analizar el contenido de los acuerdos convencionales en relación con la Ley Orgánica 3/2018, concluyen que en España la negociación fue más bien reactiva que proactiva, pues se han encargado de desarrollar los derechos ya contemplados en estos preceptos, en lugar de ampliar dichas garantías a aspectos relevantes como la salvaguarda de información relacionada con la salud o como la prohibición de discriminación basada en datos que sin pertenecer a la categoría de especiales, pueden derivar en un trato discriminatorio, como ocurre con la edad o el sexo (Sierra Hernaiz, 2020).

En suma, el ordenamiento jurídico español, en armonía con el marco regulatorio de la Unión Europea, ha configurado un sistema de protección del derecho a la intimidad y de la información en el trabajo que trasciende la visión tradicional de la subordinación laboral. A través de la

integración del artículo 18 de la Constitución Española, el Estatuto de los Trabajadores y la Ley Orgánica 3/2018 (LOPDGDD) se ha consolidado un modelo donde la facultad de vigilancia del empresario no es un poder absoluto, sino una prerrogativa funcional estrictamente vinculada a los principios de licitud, lealtad, transparencia y minimización de datos.

También contempla la posibilidad de regular con más detalle el ejercicio de los derechos reconocidos en las disposiciones estudiadas, esto, a través de la negociación colectiva. Empero, hasta ahora no ha adquirido un rol proactivo orientado a extender mayores garantías a las legalmente previstas, pero en todo caso se ha ocupado de desarrollar las ya establecidas como marco regulador de la actividad laboral y del poder de dirección.

5. Puntos concordantes y diferencias de la regulación acerca de la protección del derecho a la intimidad del trabajador en el entorno laboral digitalizado.

Nótese como tanto en España como en Colombia se reconoce el derecho a la intimidad de las personas como un límite frente al uso arbitrario de su información. No obstante, cada ordenamiento regula esta materia de manera distinta, pues la normativa española ofrece un marco más específico respecto al tratamiento de datos personales en el ámbito laboral y al control empresarial en entornos digitales, especialmente a partir de la aplicación del RGPD y del RIA relacionadas con la supervisión tecnológica.

Por su parte, en Colombia la protección se apoya principalmente en los principios constitucionales, en las reglas jurisprudenciales sobre protección de datos personales y los principios desarrollados por la Ley 1581 de 2012. Aun así, ambos modelos coinciden en un objetivo

común, impedir que la información de las personas sea utilizada de forma arbitraria o contraria a su intimidad y derechos.

En Colombia, el análisis se desarrolla a partir de la protección constitucional de la intimidad y del *habeas data*. Ello implica que el tratamiento de la información del trabajador debe responder a criterios de finalidad legítima, proporcionalidad y consentimiento informado. Aunque no existe una reproducción exacta del modelo español, la jurisprudencia colombiana no desconoce que el empleador ejerza control sobre la actividad laboral, siempre que no afecte con ello el núcleo esencial de los derechos del trabajador, ni incurra en prácticas de vigilancia desproporcionadas.

La perspectiva comparada muestra que la normativa colombiana y la española tienen puntos de semejanza en cuando a la forma de entender a la intimidad y la autodeterminación informativa del trabajador como un límite al poder de dirección del empresario ante la incorporación de tecnologías de la información en el mundo del trabajo. Es decir, ambas advierten que este límite es necesario para proteger al trabajador en la relación de subordinación tras la modificación de la forma en cómo se ejerce la misma por el uso de dispositivos digitales.

Desde esta perspectiva, incorporarse a una relación laboral no significa para el trabajador la renuncia absoluta a su esfera privada como consecuencia de la subordinación al empleador, así como tampoco significa para este perder la posibilidad de controlar la actividad en el contexto actual, donde la ejecución de la labor no necesariamente debe realizarse de manera presencial. Por el contrario, el propósito de ambas legislaciones es ofrecer herramientas de ponderación de dos intereses legítimos: por un lado, el de la organización productiva que se impone a través del poder de dirección, y por otro, el de la salvaguarda de los derechos específicos e inespecíficos del trabajador que pueden resultar lesionados ante su ejercicio.

En esa línea de pensamiento, la intimidad y el derecho a la autodeterminación informativa se anteponen como verdaderos límites al ejercicio del control del empresario en ambas normativas, de manera que la introducción de nuevas tecnologías o sistemas automatizados no pueda justificarse únicamente en factores de eficiencia, competitividad o provecho unilateral del empleador, sino que debe integrar también la efectiva protección del trabajador frente a eventuales interferencias en su ámbito personal, en contravía de principios superiores como su dignidad humana.

Esto obedece a que la digitalización ha dado lugar a nuevas formas de intervención empresarial a través de dispositivos tecnológicos, sistemas de comunicación y de plataformas digitales, por lo que es preciso ampliar la protección hacia la gestión de datos, el seguimiento de actividades o el control del comportamiento. En este contexto se evidencia cómo la privacidad y la intimidad se manifiestan de forma dinámica cuando se presta el servicio y no quedan excluidos del entorno laboral.

A esta circunstancia se le puede añadir un elemento en común en ambos ordenamientos: la exigencia de justificación del control empresarial, y es que el poder de dirección no habilita la vigilancia automatizada y prolongada del trabajador sin un límite previo y claro, sino que requiere una fin delimitado por criterios de necesidad, proporcionalidad y razonabilidad. De esta manera, la vigilancia tecnológica solo puede ser considerada como legítima cuando responde a una finalidad concreta, sin llegar a extenderse a otras indeterminadas.

Es así como los principios de minimización y finalidad hacen las veces de límite a la gestión de los datos del trabajador cuando el empleador ejerce su potestad de dirección. Por tanto, la información que recopila debe destinarse a algo concreto, lo que impide su aprovechamiento indebido, acceso desproporcionado o hipervigilancia, fuera de los fines consentidos por su titular.

En esta línea, tanto el ordenamiento español como el colombiano coinciden en que la inclusión de herramientas tecnológicas en la vigilancia supone un riesgo para la afectación de la esfera privada del trabajador. De modo que la automatización de los procesos, la utilización de sistemas de control continuo o la posibilidad de analizar masivamente información generan nuevas formas de vigilancia que pueden ser menos visibles, pero tener un mayor impacto frente a otros derechos inherentes a la persona.

Frente a este asunto, el ordenamiento español y el colombiano igualmente reconocen la necesidad de robustecer y actualizar el alcance de los derechos conforme avanza la innovación tecnológica, mediante la adecuación de las herramientas ya previstas o la formulación de unas nuevas, como el consentimiento informado o la intervención humana en la interfaz con las plataformas de procesamiento automático de datos en el espacio laboral.

Finalmente, resulta obvio que ambos coinciden al reafirmar que el trabajador no pierde la calidad de sujeto por el hecho de ser parte del contrato de trabajo y ejecutarlo bajo la subordinación del empleador. Esto es especialmente relevante en un contexto de control tecnológico, ya que impide identificar la relación laboral con un espacio de disminución de la autonomía individual. Los dos ordenamientos, definitivamente, parten del reconocimiento de que el trabajador posee la facultad de autodeterminación informativa que se debe respetar incluso en el marco de la subordinación.

En ambos casos, la jurisprudencia de cada uno de los países intenta responder a la problemática que surge cuando el entorno digitalizado intensifica el riesgo de intromisión en la esfera privada del trabajador, lo que exige una ponderación estricta de las medidas empresariales adoptadas. No obstante, las distinciones existentes entre los ordenamientos jurídicos colombiano y español son evidentes en cuanto al nivel de desarrollo de una y otra regulación, su especificidad y

la forma de organizar en cada uno de los supuestos de regulación ante el control que se realiza por parte del empresario cuando implementa herramientas tecnológicas para el efecto.

Dichas diferencias van más allá de las características técnicas porque exponen una manera distinta de articular el equilibrio entre el poder empresarial y los derechos fundamentales del trabajador. En el modelo español, la regulación del control empresarial en entornos digitales se encuentra en un estado más desarrollado, lo que se manifiesta al contar con un tipo normativo más denso, estructurado y preciso para las relaciones laborales, mientras que en el caso colombiano por el momento contamos con normativa que remite a disposiciones generales que suponen relegar la protección en cada caso concreto a la valoración de los jueces.

Es así como en España la regulación no solo ampara principios generales, sino que abarca supuestos específicos de vigilancia tecnológica, tales como la videovigilancia, geolocalización, existencia de dispositivos digitales corporativos y sistemas de control de acceso, inclusive, en este ordenamiento marcado por la facultad un poco más amplia con la que cuentan las partes de auto regularse a través del diálogo social. Este nivel de regulación restringe el margen interpretativo dejado a las partes, que puede llevar a la incertidumbre y conflicto de intereses jurídicos en la práctica, al paso que brinda derroteros claros al operador judicial para resolver los asuntos puestos a su consideración que de ello se deriven, en pro de la seguridad jurídica.

Por otro lado, el sistema colombiano se basa en principios sin que la reglamentación del uso de la tecnología contemple cada uno de los instrumentos de control. En el ámbito laboral, su regulación se redirecciona por remisión normativa a reglas generales de protección de datos que no fueron previstas para el contexto del trabajo y que no están actualizadas para responder al avance de las plataformas digitales automatizadas, como es el caso de la Ley 1581 de 2012, por lo que la delimitación del control empresarial depende más de la praxis judicial. Aun incluso, después la

reforma laboral de 2025, que tan sólo se ocupó del caso de los trabajadores digitales de plataformas de reparto.

Quiere ello decir que la previsibilidad de las consecuencias jurídicas del control empresarial es mayor en el sistema español donde se encuentran vigentes normas concretas, mientras que para el caso del sistema colombiano el ordenamiento está a medio camino de establecer una protección que responda al nuevo entorno digitalizado y automatizado en el que se desarrollan las relaciones laborales, por tanto, determinar la proporcionalidad y razonabilidad de las medidas de control se ha dejado por el momento en manos del operador judicial quien debe acudir a una norma que aún no está actualizada.

En contraste, el sistema español se caracteriza por una mayor vinculación entre la norma de protección de datos y el derecho del trabajo, lo que permite a los actores de la relación laboral tener un referente legal previo y claro cuando interactúan a través de medios digitales. Por el contrario, el sistema colombiano ostenta una mayor fragmentación normativa, en la que el derecho del trabajo por una parte y el régimen de protección de datos por la otra avanzan de manera paralela sin una interrelación, salvo por la remisión normativa a la Ley general de *habeas data* en torno al tratamiento de datos, la cual se insiste, a la fecha no se ajusta a la nueva realidad digitalizada.

Finalmente, otra diferencia relevante es la forma en cómo la norma regula el riesgo tecnológico. En el modelo español, la lógica de regulación avanza en función de una orientación preventiva de los posibles efectos lesivos del control digital a través de reglas específicas, mientras que en el modelo colombiano, se adopta una lógica reactiva en la que la regulación de la protección se activa a partir de la vulneración de derechos en casos concretos.

Otro punto de discordancia, se encuentra en la relevancia de los mecanismos de autocomposición presentes en el ordenamiento jurídico español, que en contraste con el

colombiano por costumbre menos desarrollado, complementan el sistema normativo establecido y facilitan a las partes la posibilidad de regular de manera previa, clara y suficiente cómo se desenvuelven las actividades ejecutadas en el marco de un contrato laboral.

6. Conclusiones

En primer lugar, se aprecia que, Colombia y en España reconocen en sus ordenamientos que el derecho a la intimidad y la protección de datos personales hacen parte de las garantías tuteladas en el marco de las relaciones laborales. También que dada su relevancia, aquellos funcionan como límites al poder de dirección del empleador. Este enfoque refleja un entendimiento del derecho del trabajo que preserva y resalta la condición humana del trabajador dentro de la organización productiva.

Paralelamente, se estableció que la digitalización en el trabajo modificó cómo se ejercen las facultades de vigilancia y fiscalización del empresario. El control continuo de la actividad laboral a través de dispositivos electrónicos o automáticos conlleva al procesamiento de información, que incrementa la probabilidad de afectar la vida privada del trabajador.

El análisis comparativo llevó a concluir que ambos ordenamientos establecen criterios limitantes al poder de dirección del empresario. Del mismo modo, reconocen que la gestión de los datos personales en materia laboral debe estar sujeta a fines legítimos con arreglo a los propósitos del contrato de trabajo y los derechos del trabajador, pero una de las diferencias más relevantes la encontramos en el grado de desarrollo normativo.

El sistema español en este sentido presenta una regulación más densa y más estructurada del control empresarial tecnológico, fundamentalmente, a través del RGP y el RIA que regulan el

tratamiento de los datos personales de los trabajadores cuando se emplean herramientas digitales o de procesamiento automático en el entorno laboral. En contraposición a lo explicado, el sistema colombiano opera de una forma más dependiente de los principios constitucionales y de las normas generales sobre la protección de datos, lo que concede un mayor margen de interpretación con relación al control empresarial tecnológico.

Asimismo, esto influye en la seguridad jurídica, pues mientras el modelo español se orienta hacia niveles más elevados de previsibilidad y estandarización de las prácticas empresariales de control, el modelo colombiano presenta lagunas, cuya complementación se deja a cargo de la evolución de la jurisprudencial en torno a los límites del poder de dirección en el contexto del entorno digital.

Igualmente, en el ordenamiento jurídico español tiene más peso la facultad autocompositiva para determinar en estos escenarios cómo ha de desarrollarse la relación laboral, lo que complementa las disposiciones legales, pero no amplía las garantías allí ofrecidas.

No obstante, ambos sistemas coinciden en que la información del trabajador no puede ser destinada a fines distintos a los autorizados en la norma y previamente consentidos por aquel, reafirmando de esta manera que el poder de dirección es una potestad condicionada, cuyo ejercicio requiere de una ponderación constante entre la libertad de empresa y la protección de los derechos inespecíficos del trabajador, atendiendo a principios que sirven de criterios orientadores.

A partir de lo mencionado anteriormente, la hipótesis formulada halla fundamento, en la medida en que, el ordenamiento jurídico colombiano, aun reconociendo la protección del derecho a la intimidad y al *habeas data* del trabajador, cuenta con un desarrollo normativo de menor especificidad en comparación con el español, lo que ha relegado a otras fuentes del derecho la definición de los límites al poder de dirección en el entorno digital. Esta comparación demuestra

que la evolución normativa no es homogénea, y en consecuencia, la regulación según su grado de desarrollo incide en cómo se han protegido los derechos inespecíficos tras la digitalización del trabajo.

Como conclusión, uno de los grandes retos jurídicos tiene que ver con la capacidad de los sistemas para adaptar sus mecanismos de protección a entornos de vigilancia tecnológica y recopilación masiva de datos en tiempo real dentro de los procesos productivos. Desde este ángulo, el derecho comparado pone de manifiesto que a pesar de las diferencias en lo que respecta a la estructura normativa de ambos sistemas, continúa existiendo un interés en cuanto a la necesidad de evitar que la digitalización del trabajo dé lugar a vulnerar la privacidad, intimidad y dignidad del trabajador.

No obstante, es claro que ante el avance constante de la tecnología y aplicaciones de decisiones automatizadas, es necesario continuar con el análisis de cómo este panorama cambiante a un ritmo vertiginoso modifica determina la forma en la cual entendemos las relaciones laborales.

Después de este estudio, surgen otras preguntas, como por ejemplo, en el caso de las decisiones automatizadas y la necesidad de la intervención humana, hasta qué punto puede en la práctica garantizarse la protección del trabajador o cómo puede exigir verdaderamente el cumplimiento de las obligaciones a cargo del empleador cuando este hace las veces de responsable y operador de la información personal que recoge en sus dispositivos, máxime cuando incluso un ordenamiento más desarrollado en la negociación colectiva como lo es el Español afronta retos a la hora de abordar mayores garantías para los trabajadores.

También surgen dudas en torno a si sería procedente actualizar no sólo la Ley general en materia de protección de información, sino que, la Ley laboral en temas como las obligaciones especiales y prohibiciones del empleador, facultando al trabajador para que de manera directa, y

no sólo a través de un ejercicio hermeneútico, pueda reclamar la reparación de un eventual perjuicio que se le ocasione con el uso indebido de su información, o, incluso, sustentar un eventual despido imputable al incumplimiento del empleador por el uso indebido de herramientas digitales.

7. Referencias bibliográficas

Aguilera, R. (2020). El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización. CEF, 442. *Revista de Trabajo y Seguridad Social*, 93-134.

Asamblea Nacional Constituyente. (1991). *Constitución Política de Colombia. Colombia*. Gaceta Constitucional No. 116. https://www.secretariasenado.gov.co/constitucion-politica

Baz Rodríguez, J. (2021). La vigilancia tecnificada del trabajo remoto y deslocalizado: geolocalización, teletrabajo y entorno laboral ubicuo. En J. Baz Rodríguez (Ed.), *Los nuevos derechos digitales laborales de las personas trabajadoras en España: Vigilancia tecnificada, teletrabajo, inteligencia artificial, Big Data* (pp. 113-167). Wolters Kluwer.

Carro Suárez, J., & Sarmiento Paredes, S. (2022). El factor humano y su rol en la transición a Industria 5.0: una revisión sistemática y perspectivas futuras. Entreciencias: diálogos en la sociedad del conocimiento, 10(24), e81727. https://doi.org/10.22201/enesl.20078064e.2022.24.81727.

Congreso de la República. (2025). Ponencia para segundo debate al Proyecto de Ley 274 - Gaceta 2196. Gaceta del Congreso. Bogotá: Cámara de Representantes. Obtenido de https://www.camara.gov.co/proteccion-de-datos-personales-093/.

Colombia. (1950). *Código Sustantivo del Trabajo*. Diario Oficial No. 27.407, 9 de septiembre de 1950.

Colombia. Congreso de la República. (2008). *Ley 1266 de 2008 por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países*. Diario Oficial No. 47.219.

Colombia. Congreso de la República. (2012). *Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.

Colombia. Congreso de la República. (2008). *Ley 1221 de 2008 Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones*. Diario Oficial No. 47.052.

Colombia. Congreso de la República. (2025). *Ley 2466 de 2025. Por medio de la cual se modifica parcialmente normas laborales y se adopta una Reforma Laboral para el trabajo decente y digno en Colombia*. Diario Oficial No. 52.829.

Colombia. Corte Constitucional. (2007). *Sentencia T-405 de 2007*. M.P.: Jaime Córdoba Triviño. https://www.corteconstitucional.gov.co/relatoria/2007/t-405-07.htm.

Colombia. Corte Constitucional. (2008). *Sentencia T-768 de 2008*. M.P.: Clara Inés Vargas Hernández. https://www.corteconstitucional.gov.co/relatoria/2008/t-768-08.htm.

Colombia. Corte Constitucional. (2011). *Sentencia C-748 de 2011*. M.P.: Jorge Ignacio Pretelt Chaljub. https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm.

Colombia. Corte Constitucional. (2012). *Sentencia T-407 de 2012*. M.P.: Juan Carlos Henao Pérez. https://www.corteconstitucional.gov.co/relatoria/2012/t-407-12.htm.

Colombia. Corte Constitucional. (2017). *Sentencia T-574 de 2017*. M.P.: Alberto Rojas Ríos. https://www.corteconstitucional.gov.co/relatoria/2017/t-574-17.htm.

Díaz Revorio, F. J. (2006). El derecho fundamental al secreto de las comunicaciones. *Derecho PUCP*, (59), 159–175. https://doi.org/10.18800/derechopucp.200601.007.

Frías Ávila, P. (2020). *Poder subordinante del empleador e intimidad del trabajador en Colombia*. Bogotá: Universidad Externado de Colombia.

Galvis Cano, L. (2012). Protección de datos en Colombia: Avances y retos. *Revista Lebret*, *(4)*, 195–214. https://doi.org/10.15332/rl.v4i4.336.

Hernández Rueda, L. (1997). Instituciones de derecho del trabajo y de la seguridad social. Universidad Nacional Autónoma de México (UNAM) e Instituto de Investigaciones Jurídicas (IIJ).

Jaramillo Jassir, I. D. (2011). *Del derecho laboral al derecho del trabajo*. Editorial Universidad del Rosario. https://repository.urosario.edu.co/items/878854d9-a96f-4539-ad92-ab6403e50435

Jefatura del Estado. (1978). *Constitución Española*. Boletín Oficial del Estado, núm. 311. España.

Jefatura del Estado. (2015). *Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores*. Boletín Oficial del Estado, núm. 255. España.

Jefatura del Estado. (2018). *Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado, núm. 294. España.

Jiménez-Castellanos Ballesteros, I. (2017). Videovigilancia laboral y derecho fundamental a la protección de datos. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social, 136*, 129-156.

Jiménez Silva, C., Ramírez, X. J., & Charre Quispe, M. F. (2022). El ejercicio del poder de dirección del empleador y sus límites frente a los derechos de los trabajadores. *Giuristi: Revista de Derecho Corporativo, 3*(5), 29–51. https://doi.org/10.46631/Giuristi.2022.v3n5.04.

López Balaguer, M., & Ramos Moragues, F. (2020). Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad. *Lex Social: Revista de los Derechos Sociales, 10(2)*, 506-540. https://doi.org/10.46661/lexsocial.5075

Moral Guadilla, P. (2021). Sistemas de geolocalización, control del trabajador y facultad disciplinaria empresarial. [Trabajo de grado, Universidad de Valladolid]. https://uvadoc.uva.es/handle/10324/50965.

Monereo Pérez J., B. d. (2023). Protección de datos personales, intimidad y derechos digitales del trabajador ¿avance o retroceso? Revista Derecho Social Y Empresa, (18), 180–214. https://doi.org/10.18172/redsye.6243.

Moreno Bobadilla, Á. (2016). El derecho a la intimidad en España. *Ars Boni et Aequi,* 12(1), 33-57.

Palomeque López, M. C., & Álvarez de La Rosa, M. (2008). *Derecho del trabajo Manuel Carlos Palomeque López, Manuel Álvarez de la Rosa* (16a. ed). Centro de Estudios Ramón Areces.

Palomeque, M.C. (2026, enero 13). *El reparto de territorios normativos entre la ley y el convenio colectivo* [Conferencia de curso]. Curso de Especialización en Derecho Problemas Actuales del Derecho del Trabajo y Economía Digital, Universidad de Salamanca. España.

Rivas, D. (1996). *La subordinación: criterio distintivo del contrato de trabajo*. Montevideo: Facultad de Derecho Universidad de la República: Fundación de Cultura Universitaria.

Sierra Hernaiz, E. (2020). El papel de la negociación colectiva en el tratamiento de los datos. Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social (152), 115 - 138. https://dialnet.unirioja.es/servlet/articulo?codigo=7464725

Todolí Signes, A. (2021). *Regulación del trabajo y política económica: de cómo los derechos laborales mejoran la economía*. Pamplona: Aranzadi.

Tribunal Constitucional de España. (1993). *Sentencia 142/1993, de 22 de abril*. Recurso de inconstitucionalidad núm. 190/91. Boletín Oficial del Estado, núm. 127.

Tribunal Constitucional de España. (1982). *Sentencia 73/1982, de 2 de diciembre*. Recurso de amparo núm. 197/1982. Boletín Oficial del Estado, núm. 312, de 29 de diciembre de 1982.

Tribunal Constitucional de España. (2000). *Sentencia 292/2000, de 30 de noviembre*. Recurso de inconstitucionalidad 1463-2000. Boletín Oficial del Estado, núm. 4, 8 de enero de 2001.

Tribunal Constitucional de España. (2004). *Sentencia 196/2004, de 15 de noviembre*. Recurso de amparo 1322-2000. Boletín Oficial del Estado, núm. 306, 21 de diciembre de 2004.

Tribunal Constitucional de España. (2013). *Sentencia 29/2013, de 11 de febrero*. Recurso de amparo 10522-2009. Boletín Oficial del Estado, núm. 61, 12 de marzo de 2013.

Tribunal Constitucional de España. (2021). *Sentencia 61/2021, de 15 de marzo*. Recurso de amparo núm. 6838-2019. Boletín Oficial del Estado, núm. 97, 23 de abril de 2021.

Segura Castañeda, D. E. (2015). El derecho a la intimidad del trabajador como restricción al poder subordinante del empleador: el incipiente desarrollo en Colombia frente al derecho comparado. *Revista de Derecho Público*, núm. 34. http://dx.doi.org/10.15425/redepub.34.2015.03

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo*

que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L 119/1.

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

Uriarte, O. E., & Álvarez, O. H. (2002). Crítica de la subordinación. *Ius Et Veritas*, (25), 281-295.