BIBLIOTECA CASS

**La CAJS reconoce la importancia de reflexionar sobre las tensiones y relaciones entre los derechos laborales y la privacidad. Considerando los valores de individualidad, autonomía y libertad inherentes a toda persona, y teniendo en cuenta que la privacidad es un derecho humano fundamental que protege los aspectos íntimos de la vida frente a injerencias externas, se subraya la necesidad de abordar estas tensiones. Asimismo, se destaca —como han señalado otros organismos internacionales— que estos derechos son esenciales para las personas trabajadoras y constituyen una condición fundamental para alcanzar un trabajo decente. ʃ Breviarios CASS es una colección de las Comisiones Americanas de Seguridad Social. La serie incluye textos elaborados por uno o más autores, que profundizan en temas de interés para la CASS, abordando antecedentes, tendencias actuales y futuros ámbitos de trabajo. Los textos se preparan con el propósito de ser lo más accesibles posible para toda la membresía.**

CISS CONFERENCIA INTERAMERICANA DE SEGURIDAD SOCIAL

CAJS COMISIÓN AMERICANA JURÍDICO SOCIAL

BIBLIOTECA CASS

Privacidad y trabajo

BIBLIOTECA CASS

# Privacidad y trabajo

Luz Angela Cardona Acuña
María Teresa González Nava
EDITORAS

CISS CONFERENCIA INTERAMERICANA DE SEGURIDAD SOCIAL
CAJS COMISIÓN AMERICANA JURÍDICO SOCIAL

# Privacidad y trabajo

**Luz Angela Cardona Acuña**
**María Teresa González Nava**
EDITORAS

BIBLIOTECA CASS

# Privacidad y trabajo

**Luz Angela Cardona Acuña**
**María Teresa González Nava**
EDITORAS

CISS
CONFERENCIA INTERAMERICANA DE SEGURIDAD SOCIAL

CAAF
COMISIÓN AMERICANA DE ACTUARÍA Y FINANCIAMIENTO

**CONFERENCIA INTERAMERICANA DE SEGURIDAD SOCIAL (CISS)**
**COMISIÓN AMERICANA DE ACTUARÍA Y FINANCIAMIENTO (CAAF)**
**2024**

## Conferencia Interamericana de Seguridad Social



ISBN en trámite
Impreso en México
Noviembre, 2024.

Biblioteca CASS es una publicación de periodicidad irregular, editada por la Conferencia Interamericana de Seguridad Social. Dirección: San Ramón s/n, Col. San Jerónimo Lídice, Alcaldía Magdalena Contreras, C.P. 10100, Ciudad de México. Teléfono: 5553774700. Sitio web: https://ciss-bienestar.org/

Citación sugerida: Cardona Acuña, Luz Angela y María Teresa González Nava (eds.), *Privacidad y trabajo* (México: Conferencia Interamericana de Seguridad Social, 2024), 192 p.



**Advertencia**

La Conferencia Interamericana de Seguridad Social se compromete con el uso de un lenguaje inclusivo. Sin embargo, al no haber consenso sobre la forma más adecuada de implementarlo en español, y para evitar una sobrecarga gráfica que conllevaría el uso de expresiones como «o/a», «x», «@», o «las y los», se ha optado por emplear el masculino genérico clásico, entendiendo que todas las menciones en este género incluyen tanto a mujeres como a hombres.

## Agradecimientos

La Comisión Americana Jurídico Social (CAJS) agradece a todas las personas que contribuyeron con sus capítulos para esta primera obra de la Biblioteca CASS. En especial, expresa su gratitud a quienes participaron en el evento que dio origen a estos textos por sus preguntas, reflexiones, comentarios y cuestionamientos, los cuales enriquecieron y refinaron el proceso de conceptualización y redacción.

# Índice

# PRESENTACIÓN

La Conferencia Interamericana de Seguridad Social (CISS) tiene como objetivos contribuir y cooperar en el desarrollo de la seguridad social en el continente americano, fomentar la cooperación y el intercambio de experiencias entre las instituciones de seguridad social y con organizaciones afines, así como investigar, recopilar y difundir los avances y estudios de los sistemas de seguridad social.

Para cumplir estos objetivos, la CISS cuenta con las Comisiones Americanas de Seguridad Social (CASS), que actúan como órganos técnicos de apoyo. Estas comisiones están integradas por personas expertas de nuestros miembros y abordan temas como los riesgos profesionales, las personas mayores, los asuntos jurídicos, la salud y el bienestar, la organización y la administración de los sistemas de seguridad social, y la actuaría y el financiamiento.

Como parte de sus actividades, las CASS han retomado el proyecto editorial de Biblioteca CIESS, iniciado en 2009. Con un espíritu renovado, pero inspirado en esta valiosa experiencia, se publican los Biblioteca CASS. Se trata de libros en los que colaboran especialistas en áreas prioritarias para las Comisiones, teniendo en cuenta su importancia para la seguridad social y la actualidad temática de cada Comisión. La audiencia objetivo está conformada por personas interesadas en la seguridad social. Estos textos, redactados en un estilo accesible, presentan los aspectos fundamentales de los temas seleccionados.

En este contexto, la Comisión Americana Jurídico Social (CAJS) presenta esta primera obra de la colección *Privacidad y trabajo*. Este documento, resultado del esfuerzo coordinado de la CAJS con personas expertas del continente americano, busca reflexionar

sobre las tensiones y relaciones entre los derechos laborales y la privacidad. Para ello, se analizan los aspectos relativos a la individualidad, la autonomía y la libertad que se reconocen como inherentes a todo ser humano, y se considera que la privacidad es un derecho humano fundamental que sirve como salvaguarda de los aspectos íntimos de la vida de las personas frente a interferencias externas. Al mismo tiempo, se analiza cómo estos derechos son un componente integral de los derechos de las personas trabajadoras y una condición esencial para lograr un trabajo decente.

Me complace presentar este libro de la Biblioteca CASS, con la esperanza de que sirva como un recurso valioso para nuestra membresía en el análisis de las legislaciones nacionales y en la consideración de acciones por parte de los Estados y las empresas para la protección de ambos derechos. Felicito a los coordinadores de la Biblioteca CASS y agradezco al equipo de trabajo que apoyó el proceso de conceptualización, redacción y publicación de esta obra.

**Alvaro Velarca Hernández**
Secretario General

# Sobre este libro

## Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE)

Además de ochenta años de su fundación, la Conferencia Interamericana de Seguridad Social (CISS) se consolida como organismo internacional técnico y especializado de carácter permanente, que contribuye al desarrollo de la seguridad social en nuestro continente, al impulsar la creación de espacios de reflexión, investigación, diálogo e intercambio internacional.

Prueba de ello, es la labor de la Comisión Americana Jurídico Social (CAJS), órgano técnico estatutario de la CISS especializado en el análisis del marco jurídico existente y aplicable para la exigibilidad y el acceso a la seguridad social con perspectiva de políticas incluyentes bajo la tutela de personas expertas de todo el continente en temas legislativos y normativos.

En este contexto, como parte de la agenda 2024-2025 la CAJS celebró el 19 de enero de 2024 el conversatorio virtual denominado «Derecho del Trabajo y Privacidad», con la participación de las y los siguientes panelistas expertos en la materia: la doctora María Villa Fombuena, profesora de la Universidad de Sevilla, España; la maestra Stella Sofía Vanegas Morales, socia del despacho Vanegas Morales Consultores de Colombia; el maestro

Federico Anaya Ojeda, presidente ejecutivo del Instituto Latinoamericano del Derecho del Trabajo y de la Seguridad Social de México; el licenciado Gilberth Díaz Vázquez, presidente del Sindicato de Trabajadores y Trabajadoras de la Educación de Costa Rica, y el doctor Jorge Ulises Carmona Tinoco, profesor investigador del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México.

En dicho conversatorio, se reflexionó sobre las tensiones y relaciones entre el trabajo y el derecho a la privacidad, teniendo en cuenta que este último salvaguarda los aspectos íntimos de todo ser humano, como la individualidad, la autonomía y la libertad. En la actualidad, establecer los límites entre el uso de los datos personales, los avances tecnológicos y la protección de la privacidad como derecho humano supone un reto, ya que no se trata simplemente de un concepto de no interferencia. Este concepto se extiende a otorgar a las personas el control sobre sus datos personales, una información valiosa tanto en la relación laboral como en sus actividades cotidianas, ya que puede revelar aspectos íntimos de su vida. La falta de protecciones legales integrales no solo expone a las personas a violaciones de su privacidad, sino que también podría socavar sus derechos más amplios en el lugar de trabajo.

Es por ello que se debatió sobre la definición de privacidad de la Organización Internacional del Trabajo (OIT), que la considera un componente integral de los derechos de las personas trabajadoras y una condición esencial para el trabajo. También se habló de las disparidades que existen en cuanto al tratamiento de los datos personales en la legislación de los países del continente americano, señalando que algunos carecen de una regulación sólida o de directrices claras sobre las restricciones legítimas y ra-

zonables a la privacidad, a pesar de los diversos instrumentos internacionales que responsabilizan a los Estados de su protección.

A este respecto, la Corte Interamericana de Derechos Humanos ha declarado explícitamente que los Estados tienen la obligación de proteger a sus ciudadanos de los riesgos que enfrenta el derecho a la privacidad en la era digital y de los desafíos que plantean las nuevas herramientas tecnológicas. Esto marca un cambio fundamental en el paradigma, pasando de una concepción estática de la protección de la privacidad a un conjunto dinámico de mecanismos de protección, y de un derecho pasivo a un deber activo de los gobiernos para salvaguardar las libertades personales contra intrusiones injustificadas.

Este fructífero intercambio sentó las bases para que las y los participantes del conversatorio se unieran en la conceptualización y realización de la obra *Privacidad y trabajo*, como una contribución dogmática al derecho social. En ella se plantean distintos escenarios con el fin de proponer soluciones flexibles ante las vicisitudes que acontecen en la era digital: la intimidad, el trabajo y el uso adecuado de los datos personales.

En este contexto, el doctor Carmona aborda en el primer capítulo la vida privada, la privacidad y la intimidad como derechos humanos y sus implicaciones en el ámbito laboral. Asimismo, se refiere al marco básico de los derechos humanos, los deberes del Estado, los límites y restricciones en su ejercicio, su interacción con el derecho al trabajo y los derechos laborales, los derechos humanos laborales y la importancia de los instrumentos que garantizan los derechos humanos.

Por su parte, la doctora María Villa Fombuena reflexiona, en el segundo capítulo, sobre las relaciones y tensiones entre los de-

rechos laborales y la privacidad, esta última como derecho fundamental, y sus limitaciones desde la perspectiva del derecho comparado, así como sobre las posibilidades y los riesgos de la tecnología actual y futura, y la necesidad de su regulación y control específico.

En el tercer capítulo, la maestra Stella Vanegas analiza el ejercicio razonable de los derechos por parte de los titulares (de los datos personales) y los deberes de los responsables (quienes los tienen en posesión), y subraya la importancia de que tanto empleados como empleadores sean conscientes de sus derechos y obligaciones en relación con los datos personales.

En el cuarto capítulo, el licenciado Gilberth Díaz Vázquez diserta sobre la intimidad y la privacidad en el trabajo y propone soluciones desde la negociación colectiva laboral. Aborda temas como las tensiones entre la privacidad y la intimidad como derecho humano de la persona trabajadora y la libertad de la empresa, la protección contra arbitrariedades patronales, los usos inadecuados de la información, incluido el acoso laboral, y también nos habla del consentimiento previo, libre e informado y de las cláusulas de protección del derecho a la intimidad y a la privacidad en la negociación colectiva.

El maestro Federico Anaya Ojeda plantea en el capítulo quinto la gestión de la privacidad en el trabajo desde la perspectiva de la eficacia, refiriéndose a las políticas de privacidad empresarial, el consentimiento, la obtención de datos, su monitoreo y vigilancia. También trata temas como las auditorías y el cumplimiento normativo sobre la retención y eliminación de datos personales, y finalmente, la privacidad y la tecnología futura en el trabajo.

Los capítulos sexto y séptimo, a cargo de Luz Ángela Cardona Acuña y María Teresa González Nava, respectivamente, están

dedicados a las conclusiones, la agenda para el futuro y los pasos a seguir respecto al derecho a la privacidad, uno de los derechos humanos esenciales que dan contenido y substancia a la dignidad humana. Debe reconocerse que existe un ámbito de la vida de cada persona que solo le concierne a ella y que queda reservado para los demás.

Esperamos que este trabajo colectivo se convierta en una obra de consulta imprescindible en el ámbito de la seguridad social, tanto para quienes toman decisiones en los sectores público y privado como para las personas estudiosas de la materia y las personas trabajadoras, ya que ofrece aportaciones actualizadas e innovadoras sobre la privacidad en el trabajo desde una perspectiva jurídica integral.

CAPÍTULO I

# La vida privada, privacidad e intimidad y sus implicaciones laborales

**Jorge Ulises Carmona Tinoco**
Investigador
Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (UNAM)

## Introducción

Los derechos humanos, un término ampliamente aceptado y utilizado a nivel global en diversas lenguas y regiones del mundo, se refieren a los derechos fundamentales inherentes a todas las personas. Estos derechos están destinados a afirmar y proteger la dignidad intrínseca de cada individuo, garantizando aspectos como su integridad, libertad, interacción social y desarrollo personal. Los derechos humanos incluyen las condiciones, los recursos y los servicios necesarios para que cada individuo pueda llevar una vida plena en sociedad.

El reconocimiento de los derechos humanos ha sido fruto de una labor prolongada, marcada por numerosos desafíos. A lo largo de sus diversas etapas, ha habido un denominador común: la lucha contra las atrocidades y los abusos perpetrados por aquellos en posiciones de poder. Esta lucha ha abarcado la injusticia, la

opresión, la exclusión, la desigualdad y la inequidad, entre otras formas de violación de los derechos humanos. En esta evolución se entrelazan acontecimientos históricos significativos, así como también ideas en torno a la dignidad inherente de la persona humana, la libertad, la igualdad y los límites del ejercicio legítimo del poder. Además, se considera el papel primordial que el Estado debe desempeñar para garantizar que todos sus ciudadanos tengan las condiciones necesarias para llevar una vida digna.

En la actualidad, los derechos humanos están reconocidos tanto a nivel interno como internacional, plasmados en las constituciones de los Estados y respaldados por un número creciente de tratados internacionales en vigor. Estos desarrollos tienen sus raíces principalmente en la segunda mitad del siglo XIX y principios del XX, en eventos como las denominadas «intervenciones por causas de humanidad», la abolición de la esclavitud y la protección de las personas trabajadoras contra la explotación laboral (Sepúlveda, p. 14). Buergenthal añade el concepto de la responsabilidad estatal por daños a extranjeros y la salvaguarda de las minorías, así como el establecimiento del sistema de mandatos y minorías de la Liga de las Naciones (pp. 9-19). También se destaca la fundación de la Organización Internacional del Trabajo en 1919.

Tras la conciencia compartida provocada por los dolorosos eventos de la Segunda Guerra Mundial, los derechos humanos obtuvieron un reconocimiento internacional pleno, lo que dio forma a un Derecho Internacional de los Derechos Humanos que incluye un catálogo cada vez más extenso de normativas, así como de organismos y procedimientos de protección supranacional.

En la actualidad, los derechos humanos abarcan, de manera enunciativa e ilustrativa, tres categorías principales: los derechos

civiles y políticos, que comprenden las libertades fundamentales como la vida, la integridad personal, diversas libertades individuales, la privacidad, el acceso a la justicia y el debido proceso, entre otros; los derechos económicos, sociales y culturales, que incluyen aspectos como la salud, la educación, el trabajo, la seguridad social, la vivienda, la alimentación, el agua y la cultura; y los derechos de solidaridad, como el derecho a un medio ambiente saludable, a la paz y al desarrollo.

La lucha por el reconocimiento y la efectividad de los derechos humanos continúa y se enfrenta a retos cada vez más complejos, particularmente aquellos derivados de los avances tecnológicos y su impacto en diversas esferas de la vida humana. Por ejemplo, la privacidad de las personas trabajadoras puede verse comprometida de diversas maneras, ya sea durante el acceso al trabajo, en el lugar de trabajo o incluso fuera de él, debido a las actividades laborales. La implicación de la privacidad como un derecho inherente a la dignidad humana en contextos laborales requiere una comprensión profunda de su naturaleza y características. Este breve trabajo tiene como objetivo explorar dichas dimensiones.

## 1. El marco básico de los derechos humanos

### 1.1. La noción y los principios de los derechos humanos

El hecho de que un determinado aspecto de la vida de una persona se considere un derecho no es cosa menor, ya que implica, como principio básico, que ese derecho está vinculado a la dignidad del ser humano, a ese mínimo irreductible que nos reconoce un valor intrínseco y que nos distingue como especie. Los derechos humanos, al ser la vía para salvaguardar la dignidad humana, se sustentan en diversos principios característicos que

se enuncian en el ámbito internacional desde hace varias décadas, como la *universalidad*, *la interdependencia*, la *indivisibilidad* (proclamados en el punto 5 de la Declaración y el Programa de Acción de Viena de la ONU de junio de 1993) y la *progresividad*.

La *universalidad* se reconoce como el fundamento central de la noción de derechos humanos, lo que implica que tales derechos son inherentes a la persona humana (Nikken, pp. 11-19), independientemente del tipo de Estado, región, nacionalidad, familia, sistema económico o político, religión o creencias en los cuales haya nacido y se desenvuelva. Es decir, la mera condición de ser humano es suficiente para ser titular de los derechos fundamentales o derechos humanos.

Sin embargo, es importante distinguir entre el reconocimiento de los derechos y su efectividad, ya que una cosa es ser titular de los mismos y otra tener las condiciones para su plena realización. Esta distinción subraya la necesidad de luchar de forma dinámica y constante por los derechos humanos en todo el mundo. Asimismo, aunque los derechos humanos son universales y aplicables a todas las personas, su alcance no es absoluto; es decir, los derechos de una persona tienen límites donde comienzan los de otra o los de la colectividad, y viceversa. En su ejercicio, los derechos humanos pueden ser modulados, estar sujetos a reglas e incluso restringidos bajo ciertas condiciones.

El principio de *interdependencia* implica que la satisfacción o la afectación de un derecho humano en particular tiene efectos en el disfrute y la eficacia de otros (CNDH, p. 11). Por ejemplo, cumplir con los parámetros del derecho a la educación puede tener efectos positivos en el ejercicio de libertades como la de expresión o el acceso a la información, así como en la capacidad para exi-

gir el cumplimiento de otros derechos. De igual manera, la afectación a la integridad personal puede tener consecuencias en el derecho a la salud o en la capacidad para desempeñar un trabajo adecuadamente. Una detención arbitraria y prolongada podría violar derechos humanos colaterales, como los derechos políticos, especialmente si ocurre durante un período electoral.

La *indivisibilidad* es un principio que ha acompañado a los derechos humanos desde su concepción original, y significa que los Estados no pueden seleccionar algunos derechos para satisfacerlos mientras ignoran otros; por el contrario, deben velar por todos los derechos humanos en su conjunto. Cada ser humano es titular de todos los derechos humanos reconocidos, ya sean civiles, políticos, económicos, sociales, culturales, ambientales, entre otros, y ninguno de ellos puede ser vulnerado, recortado o ignorado por ninguna razón. Este principio permitió en su momento el reconocimiento pleno de los derechos sociales como derechos humanos, ya que anteriormente se consideraban meras aspiraciones sin exigibilidad o justiciabilidad, a diferencia de los derechos civiles y políticos (Carmona, pp. 11-19).

El principio de *progresividad* indica que los derechos humanos son estándares mínimos susceptibles de evolucionar y ampliar su alcance. Por lo tanto, las medidas adoptadas para cumplir con estos derechos deben permitir su avance periódico hacia mejores estándares, sin retroceder en ningún momento. Es decir, una vez alcanzado un cierto estándar, este debe conservarse y solo pueden implementarse medidas de retroceso en circunstancias excepcionales y plenamente justificadas, que sean compatibles con el resto de los derechos humanos. Según Nikken, tanto la universalidad como la progresividad son consecuencia de que los derechos son atributos inherentes al ser humano (pp. 11-19).

### 1.2. Los deberes básicos de los Estados frente a los derechos humanos

Para garantizar el cumplimiento efectivo de los derechos humanos, los Estados, sus respectivos gobiernos, autoridades y funcionarios públicos tienen una serie de deberes correlativos reconocidos. Estos deberes básicos o genéricos incluyen el respeto, la protección, la garantía y la promoción, los cuales, incluso en el caso de México, están expresamente reconocidos constitucionalmente en el artículo 1º de su Carta Magna.

El respeto a los derechos humanos se refleja en la conformidad de la conducta de los operadores jurídicos, quienes son responsables de la creación y aplicación de las normas legales. Esto implica que las acciones, abstenciones o comportamientos de estos operadores no deben obstaculizar el ejercicio de las libertades o derechos reconocidos, sino más bien asegurar que las personas tengan acceso a los bienes, servicios o recursos necesarios para realizarlos plenamente.

Por otro lado, la protección de los derechos humanos implica que los operadores jurídicos deben garantizar la prevalencia de la dignidad humana en todos los ámbitos, no solo en las relaciones entre individuos y el gobierno y sus autoridades, sino también en la sociedad en general. Esto se debe a que los derechos de las personas generan una correlación de deberes hacia los derechos humanos de los demás y hacia el bienestar común. Por este motivo se hace referencia a la transversalidad u horizontalidad de los derechos humanos.[1] En este sentido, corresponde a los Estados, en virtud del

---

[1] El artículo 32 de la Convención Americana sobre Derechos Humanos (CADH) ilustra de mejor manera este punto al señalar: «Artículo 32. Correlación entre Deberes y Derechos. 1. Toda persona tiene deberes para con la familia, la comunidad

deber de protección, supervisar y fiscalizar el respeto del bien jurídico protegido por los derechos humanos, especialmente en las relaciones de poder asimétrico presentes en la sociedad o en situaciones que involucren a personas en situación de vulnerabilidad.

En términos generales, el deber de *garantía* obliga a que los Estados dispongan de vías jurídicas para exigir y hacer valer los derechos humanos. De poco servirían catálogos extensos y robustos de derechos humanos si no existieran mecanismos para garantizar su eficacia ante su incumplimiento; como dice un antiguo adagio inglés, «*no remedy, no right*» (si no hay forma de hacerlo efectivo, un derecho no existe como tal). De manera más concreta, este deber requiere contar con instancias y procedimientos accesibles, sencillos y eficaces, principalmente de naturaleza jurisdiccional, para asegurar el respeto, la protección y la realización de los derechos.

En décadas recientes se ha reconocido la importancia de la promoción de los derechos humanos, lo que conlleva el deber de que tanto los operadores jurídicos como las personas en general conozcan y tomen conciencia de los derechos humanos, ya sea como titulares de los mismos o como agentes responsables de su realización. La promoción busca empoderar a las personas mediante el conocimiento y la apropiación de sus derechos inherentes. Además, este deber busca fomentar una cultura de los derechos humanos que impregne la sociedad, situando la dignidad humana en el centro de las interacciones y relaciones tanto entre individuos como con el gobierno.

---

y la humanidad. 2. Los derechos de cada persona están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bien común, en una sociedad democrática».

Los deberes genéricos de los Estados con respecto a los derechos humanos se desglosan en otros más específicos que garantizan, eficazmente, el disfrute de los derechos humanos. Estos incluyen la armonización o desarrollo de normativa secundaria, la modificación de prácticas administrativas y criterios o precedentes jurisdiccionales, la fiscalización y vigilancia, la formulación de políticas públicas y la integración de los presupuestos públicos con una perspectiva de derechos humanos.

### 1.3. Los límites y las restricciones permitidas al ejercicio de los derechos humanos

Los derechos humanos no son absolutos y su ejercicio puede estar sujeto a reglas o restricciones, e incluso, en casos excepcionales, algunos de ellos pueden suspenderse temporalmente. Sin embargo, es fundamental destacar que, en ninguna circunstancia, pueden ser ignorados, desconocidos o vulnerados. El marco de los derechos humanos ofrece vías para que las restricciones impuestas a un derecho concreto o a un conjunto de derechos puedan considerarse legítimas o, de lo contrario, sean incompatibles con la dignidad humana, así como para resolver los posibles conflictos entre los derechos de diversas personas en un caso concreto.

Nos centraremos en la primera hipótesis, es decir, el marco para la restricción legítima de los derechos humanos. Este marco parte de la premisa previamente mencionada de que los derechos humanos en su ejercicio no son absolutos y, por lo tanto, pueden ser regulados y, en ciertos casos, limitados. A nivel internacional, se han establecido parámetros para analizar si las restricciones impuestas a los derechos humanos en casos concretos son legítimas o no. En el primer caso, estas restricciones serían permisibles

y estarían dentro del respeto a los derechos, mientras que en el segundo caso implicarían una violación de los derechos humanos que conllevaría diversas consecuencias o responsabilidades, pero en todo caso el deber de proporcionar una reparación integral.

La prohibición de imponer restricciones contrarias a los derechos humanos se deriva de los compromisos internacionales asumidos por los Estados. El Pacto Internacional de Derechos Civiles y Políticos de 1966 (PIDCP) establece en su artículo 5 lo siguiente:

> 1. Ninguna disposición del presente Pacto podrá ser interpretada en el sentido de conceder derecho alguno a un Estado, grupo o individuo para emprender actividades o realizar actos encaminados a la destrucción de cualquiera de los derechos y libertades reconocidos en el Pacto o a su limitación en mayor medida que la prevista en él.
> 2. No podrá admitirse restricción o menoscabo de ninguno de los derechos humanos fundamentales reconocidos o vigentes en un Estado Parte en virtud de leyes, convenciones, reglamentos o costumbres, so pretexto de que el presente Pacto no los reconoce o los reconoce en menor grado.

En el ámbito regional, la CADH es aún más enfática y prevé en sus artículos 29, incisos a y b, y 30, las siguientes normas de interpretación:

> Ninguna disposición de la presente Convención puede ser interpretada en el sentido de:
> a) permitir a alguno de los Estados Parte, grupo o persona, suprimir el goce y ejercicio de los derechos y libertades reconocidos en la

> Convención o limitarlos en mayor medida que la prevista en ella; b) limitar el goce y ejercicio de cualquier derecho o libertad que pueda estar reconocido de acuerdo con las leyes de cualquiera de los Estados Parte o de acuerdo con otra convención en que sea parte uno de dichos Estados;
>
> ...
>
> Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas.

La Convención Americana establece un segundo nivel de garantía para los derechos que contempla, ya que sujeta las limitaciones o restricciones de los mismos a la necesaria reserva de ley, tanto en sentido formal como material. Esto significa que dichas limitaciones deben estar establecidas por ley, por razones de interés general, y que los medios previstos en la propia ley deben ser adecuados para alcanzar su propósito. En otras palabras, la ley no debe servir como un pretexto para imponer medidas que no estén alineadas con sus objetivos originales.

La Corte Interamericana de Derechos Humanos (COIDH) ha desarrollado y detallado a través de su jurisprudencia (COIDH, 2020) una especie de «test» para evaluar la legitimidad de las restricciones a los derechos humanos. Este test se compone, en resumen, de los siguientes parámetros:

1. Legalidad de la medida restrictiva, que exige que la restricción esté prevista en una ley formal y material.

2. Finalidad de la medida restrictiva, que se concreta en la exigencia de que la restricción sea de las permitidas o contempladas por la CADH, ya sea en disposiciones específicas o aquellas que prevén finalidades generales legítimas, como pueden ser, por ejemplo, la salvaguarda de los derechos o libertades de los demás o las exigencias del bien común.
3. Necesidad en una sociedad democrática y proporcionalidad de la medida restrictiva, esto es, si: a) satisface una necesidad social imperiosa, esto es, está orientada a satisfacer un interés público imperativo; b) es la que restringe en menor grado el derecho protegido; y c) se ajusta estrechamente al logro del objetivo legítimo.

De acuerdo con estos parámetros, no es suficiente que la restricción esté contemplada en una ley y tenga base en la Convención Americana sobre Derechos Humanos (CADH); además, debe ser socialmente apremiante, la menos invasiva o restrictiva entre las opciones posibles y, por último, ser el medio más idóneo para alcanzar el objetivo legítimo que la motiva. En resumen, el régimen aplicable a los derechos humanos en general exige el cumplimiento de estos criterios.

## 2. La interacción entre la vida privada, la privacidad e intimidad con el derecho al trabajo y los derechos laborales

### 2.1. Aproximación al derecho humano a la vida privada, la privacidad y la intimidad

El derecho a la vida privada, considerado como un género del cual derivan la privacidad y la intimidad como especies, está expresamente reconocido en los instrumentos internacionales de derechos humanos. Entre ellos se encuentran la Declaración Universal de los Derechos Humanos (artículo 12), el Pacto Internacional de

Derechos Civiles y Políticos (artículo 17), la Convención Americana sobre Derechos Humanos (artículo 11), la Convención Europea de Derechos Humanos (artículo 8) y en la mayoría de las constituciones de los países del mundo. A pesar de su reconocimiento, uno de los principales desafíos a los que se enfrentan estos derechos enunciados radica en la falta de uniformidad en la utilización de su nomenclatura y en sus diferencias específicas (Sanz Salguero, 2018, p. 131).

Siguiendo a Villanueva, el derecho a la vida privada puede definirse «como la prerrogativa que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público» (citado por Sanz Salguero, 2018, p. 134). Por otro lado, Ruth Gavison considera que en la privacidad coexisten tres elementos: el secreto, el anonimato y la soledad, destacando que es un estado que puede perderse por elección de la persona o por la acción de un tercero (citado por Sanz Salguero, 2018, p. 135). Finalmente, Sanz Salguero (2018) afirma que el derecho a la intimidad es «aquel que resguarda la esfera más interna o profunda del ser humano y que solo concierne al individuo, esfera que incluye el pensamiento, el ámbito psicológico de cada uno, las creencias (espirituales y religiosas), las tendencias sexuales y amorosas, y las convicciones morales» (p. 140).

A los efectos de este capítulo, se define la vida privada como aquella parte de la vida de una persona en la que esta puede expresar libremente su identidad, ya sea en sus relaciones con los demás o de manera individual, y que queda fuera del acceso o el escrutinio públicos, por decisión de la propia persona, por su naturaleza inmanente o por el contexto de relaciones en juego, a menos que sea un delito o constituya una conducta considerada como tal.

La vida privada es posible si se protege de intromisiones o de molestias injustificadas en el lugar donde se desarrolla, como lo es el domicilio, o el lugar donde se ejerce la ocupación habitual; los medios a través de los cuales se manifiesta la individualidad, como la correspondencia, escritos, grabaciones, o las comunicaciones en general; lo que identifica e individualiza a la persona, como son los datos personales y su uso y destino; las relaciones humanas y afectos más cercanos, como las relaciones familiares, afectivas o aquellas que la persona, si así lo decide, no debe revelar a otros; o las actividades, creencias, conductas o manías más íntimas o que solo a ella incumben, elementos que dan origen a los derechos a la privacidad y a la intimidad.

La vida privada y los derechos circundantes a ella forman un amplio mosaico dinámico de posibilidades, que difícilmente puede ser exhaustivo. Un aspecto fundamental es que la vida privada y los derechos que le son inherentes o relacionados acompañan a la persona en el contexto de su desenvolvimiento cotidiano, no solo en sus relaciones con las autoridades, sino también con los demás, incluyendo el desempeño de sus actividades laborales. Esto implica que hay aspectos de la vida privada, privacidad e intimidad que deben ser respetados, protegidos y garantizados, también en el ámbito laboral, sea este público o privado, lo cual se abordará en un apartado posterior.

### 2.2. Los derechos humanos laborales

Los derechos humanos se integran por los derechos y libertades individuales, conocidos como derechos civiles y políticos, pero también por los denominados derechos económicos, sociales, culturales y ambientales (DESCA), entre los que se encuentra el

derecho al trabajo y los derechos en el trabajo. Los DESCA o derechos sociales son aquellos derechos humanos que representan los estándares mínimos para gozar de una vida digna, permitiendo que las personas puedan, por una parte, satisfacer necesidades vitales básicas y, por otra parte, desarrollar sus capacidades como integrantes de la sociedad (Carmona, 2022, p. 12).

Estos derechos han sido objeto de un paulatino reconocimiento en los Estados y a nivel internacional. Entre ellos se encuentran los derechos relacionados con el trabajo, la salud, la educación, la seguridad social, la vivienda, el agua, la alimentación, el medio ambiente, así como la protección de la familia. Desde enfoques diferenciados, se reconocen las necesidades específicas de las mujeres, niñas, niños y adolescentes, las personas adultas mayores, las personas con discapacidad y los pueblos indígenas, entre otros grupos de población. Como acertadamente afirma Kurczyn:

> … los derechos sociales de las colectividades de los trabajadores, o de las sociedades de los asalariados, son una respuesta a la defensa de los derechos esenciales inherentes a la persona del trabajador cuando surgen las luchas de intereses de clase; o bien cuando se trata de derechos humanos de solidaridad como puede ser sobre el medio ambiente, que surgen cuando se cierne la amenaza de la naturaleza en medio de la cual habita el individuo y de la que depende su salud y forma digna de vida integral, así como respecto de los derechos humanos correspondientes a los intereses difusos o inespecíficos (Kurczyn, 2016, pp. 82-83).

Cumplir con los derechos humanos es una tarea que involucra al Estado, el cual debe coordinarse con el resto de los actores so-

ciales para cumplir con los deberes que permitan la realización de los DESCA, especialmente para las personas o grupos en situación de vulnerabilidad. En el ámbito concreto de los instrumentos para garantizar los derechos y hacerlos justiciables, las figuras jurídicas, procedimientos y procesos han ido adaptándose para atender la incidencia de los derechos humanos en casos concretos.

En el caso específico de los derechos laborales, es importante recordar que la Constitución Política de los Estados Unidos Mexicanos de 1917 se reconoce como un documento pionero que contempló la protección de trabajadores y campesinos, seguido por la Constitución rusa de 1918 y la de Weimar de 1919. A nivel internacional, cabe mencionar el establecimiento de la Organización Internacional del Trabajo (OIT) y la adopción de los primeros seis convenios en materia laboral en esa organización, que datan de 1919, varias décadas antes de que se contemplara el derecho al trabajo y los derechos en el trabajo en las constituciones de muchos Estados y en los instrumentos de derechos humanos en el marco de la ONU, el Consejo de Europa y la OEA (Carmona, 2022, p. 15).

En la actualidad, existe una necesaria convergencia entre el derecho internacional laboral, derivado principalmente de los convenios de la OIT e instituciones afines, y el derecho internacional de los derechos humanos (Belmont, pp. 28-30). Esta convergencia se proyecta en el ámbito de los Estados y su legislación doméstica, dando lugar a lo que podemos denominar derechos humanos laborales, como los estándares mínimos de derecho al trabajo y en el trabajo consustanciales a la dignidad humana.[2] Por tal motivo, son universales, indivisibles, interde-

[2] Este marco se nutre además de otros componentes, tales como la jurisprudencia

pendientes y progresivos. Su vigencia debe ser respetada, protegida, garantizada y promovida por los Estados, y tener eficacia también en las relaciones entre particulares en general.

En el ámbito de la ONU, los derechos humanos laborales se recogen en la Declaración Universal de los Derechos Humanos y en los tratados posteriores sobre la materia, especialmente en el Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966 (PIDESC). En el Consejo de Europa, se adoptó la Carta Social Europea en 1965. En el marco de la OEA, tales derechos se reconocieron en la Declaración Americana de Derechos y Deberes del Hombre de 1948, en el artículo 26 de la Convención Americana sobre Derechos Humanos de 1969, y ampliamente en el Protocolo Adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales conocido como Protocolo de San Salvador (PSS) de 1988.

En los tratados internacionales de derechos humanos que se aplican en diversos países del continente americano, como son el PIDESC y el PSS en sus respectivos artículos 6 a 8, el derecho al trabajo y los derechos en el trabajo abarcan aspectos individuales y colectivos, como la libertad de trabajo, condiciones de trabajo equitativas y satisfactorias tales como la remuneración, la seguridad, la salubridad y el descanso, entre otros. También incluyen el derecho a formar sindicatos y a la huelga, así como a la seguridad social que corresponde a todas las personas por igual. En el ámbito de la OIT, los principios de derechos laborales y los derechos humanos esta-

---

internacional, conjuntos de principios, reglas y recomendaciones que constituyen el corpus laboral de la dignidad humana, fundamento del concepto conocido como trabajo *decente*.

ban contemplados en la propia Constitución de la Organización y en la Declaración de Filadelfia de 1944. Varios de los convenios pueden considerarse una extensión o complemento de los derechos humanos en el trabajo, al igual que un número importante de recomendaciones. También cabe destacar la Declaración de la OIT relativa a los principios y derechos fundamentales en el trabajo y su seguimiento, publicada en 1998 y enmendada en 2022.

La relación entre el derecho al trabajo y los derechos laborales con la privacidad es un caso prototípico de interrelación de derechos humanos y de la necesidad de protección jurídica ante restricciones ilegítimas, contrarias a los derechos humanos, principalmente de las personas trabajadoras. Nos ocuparemos de ello en el siguiente apartado.

### 2.3. La vida privada, la privacidad y la intimidad en el contexto del derecho al trabajo y los derechos en el trabajo

En el catálogo de lo que denominamos derechos humanos laborales no se señala en particular el derecho a la vida privada, a la privacidad o a la intimidad. Esto no significa en modo alguno que sean derechos que no tengan incidencia o puedan ser excluidos, dejados fuera de consideración o sometidos a la libre voluntad de quienes integran una relación laboral, pues son derechos inherentes a la persona humana. Además, es necesario fijar la atención en la naturaleza y el alcance de ese conjunto de derechos, dado que han venido cobrando cada vez más relevancia y atención de la mano de las nuevas tecnologías de identificación, información y comunicación. Las actividades laborales no han quedado exentas del impacto de las nuevas tecnologías, tanto en los sitios de trabajo como en las nuevas modalidades, como el trabajo remoto. Los

avances tecnológicos, cuya utilidad es innegable, tienen a su vez el potencial de exponer y poner en riesgo aspectos propios de la vida privada, la privacidad o la intimidad, que, insistimos, son inherentes a la persona humana como parte de su dignidad.

Este tema cuenta con un interés académico creciente e importante, que va nutriéndose con un número cada vez mayor de trabajos que abordan muchos de sus diversos ángulos y aristas. Además, en el ámbito laboral, e incluso en el prelaboral y el acceso al trabajo, existen diversos derechos humanos que deben ser considerados y respetados, aunque se ejerzan dentro de un margen de reglas, condiciones y requisitos consensuados, pues hay un núcleo de derechos irreductible, irrenunciable e inalienable, fuera de lo decidible o negociable, por ser inherente a la dignidad humana. Determinar el alcance tanto de los derechos como de sus posibles restricciones legítimas en casos concretos requiere considerar un cúmulo importante de principios, normas y criterios.

Esto se debe a que en el ámbito laboral se producen interacciones, relaciones humanas, jurídicas y prácticas de diversa índole. Por ejemplo, entre empresarios y trabajadores, entre los propios trabajadores, entre sindicatos, trabajadores y empresarios, o entre autoridades laborales, de salud o fiscales y empresas, empresarios, sindicatos y trabajadores. En todas estas relaciones e interacciones, las nuevas tecnologías, el video y las telecomunicaciones desempeñan un papel cada vez más importante. Esto obliga a considerar la incidencia e interrelación de los diversos derechos humanos que entran en juego.

En resumen, el punto central es cómo, desde los derechos humanos involucrados, es posible conciliar el acceso al trabajo, las condiciones de trabajo y la salvaguarda de la vida privada, la priva-

cidad y la intimidad que asisten a toda persona. Esto permitiría, en un caso concreto, que el ámbito de la vida privada o algunas de sus manifestaciones pudieran ser objeto de vigilancia o escrutinio de manera consensuada, o que se puedan recabar, guardar y utilizar para fines lícitos datos personales, sin que esto pueda decidirse de manera unilateral, sin consentimiento previo e informado y, menos aún, sin que pueda renunciarse en situaciones asimétricas de poder.

Los derechos humanos pueden ser regulados y también pueden existir restricciones legítimas, que se centran en la licitud, la razonabilidad, la necesidad y la ponderación, como extremos que deben satisfacerse para ajustarse a los márgenes y los medios en los que la privacidad puede quedar expuesta o ceder a la hora de acceder a un trabajo o durante la existencia de una relación laboral. Si bien tales márgenes y medios no pueden estar completamente definidos de antemano, pues dependen del caso concreto, se pueden lograr avances en la normativa sobre protección de datos personales en los diversos países y, también, generar protocolos de actuación, guías de buenas prácticas o, en definitiva, determinar lo que en modo alguno es aceptable bajo ninguna circunstancia.

En el ámbito internacional, existen algunos documentos que podrían servir como parámetros de aplicación y de creación de legislación, regulación, protocolos o guías. Nos referimos a la Observación general 17, elaborada por el Comité de Derechos Humanos de Naciones Unidas, que vigila el cumplimiento al PIDCP por parte de los Estados, y al *Repertorio de recomendaciones* de la OIT para proteger los datos personales del trabajador, publicados en 1996.

El Comité de Derechos Humanos de la ONU, encargado de velar por el cumplimiento del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) por parte de los Estados, ha elaborado perió-

dicamente unas observaciones generales para interpretar el pacto y guiar a los Estados en el cumplimiento del mismo. Los criterios que derivan de ellas se consideran jurisprudencia internacional. La Observación General número 16 del Comité, emitida en 1988, se dedica al artículo 17 del mencionado Pacto, que contempla el derecho a la vida privada y la protección de esta, la familia, el domicilio y la correspondencia, en los siguientes términos:

> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

A juicio del Comité, en la referida Observación General se expone que «este derecho debe estar garantizado respecto de todas esas injerencias y ataques, provengan de las autoridades estatales o de personas físicas o jurídicas». Asimismo, el término «ilegales» significa que *no puede producirse injerencia alguna, salvo en los casos previstos por la ley*, mientras que la expresión «injerencias arbitrarias» somete incluso lo que prevé la ley a su conformidad con otras disposiciones del Pacto, sus propósitos y objetivos, y a ser, en todo caso, *razonable en las circunstancias particulares de cada caso* (párrafos 3-4).

En opinión del Comité: «Como todas las personas viven en sociedad, la protección de la vida privada es por necesidad relativa. Sin embargo, las autoridades públicas competentes solo deben pedir aquella información relativa a la vida privada de las personas cuyo conocimiento resulte indispensable para los intereses de la sociedad en el sentido que tienen con arreglo al Pacto» (párrafo

7). Este parámetro también se puede aplicar al ámbito laboral y a la información que pueden pedir los empleadores para acceder al trabajo o en el marco de una relación laboral ya existente.

Otro de los puntos relevantes de la Observación General que se cita es que:

> … la integridad y el carácter confidencial de la correspondencia estén protegidos de jure y de facto. La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída de otro modo. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones… Por lo que respecta al registro personal y corporal, deben tomarse medidas eficaces para garantizar que esos registros se lleven a cabo de manera compatible con la dignidad de la persona registrada… (párrafo 8).

Para el Comité, la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por parte de las autoridades públicas como de particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y que nunca se la utilice para fines incompatibles con el Pacto. De igual manera, la persona debe tener el derecho de verificar si hay datos suyos almacenados, el porqué de su almacenamiento, qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos, y poder pedir su rectificación o eliminación (párrafo 10).

En el ámbito de la OIT, consideramos que cuenta con un documento pionero y visionario sobre los temas que nos ocupan, pues en 1996 publicó el *Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores*, que tiene un carácter tanto técnico como político, ya que es el propio Consejo de Administración de la OIT quien determina su publicación (OIT, 1996, p. 631). Como se reconoce en el propio *Repertorio*..., se aborda un problema que va más allá del campo de la seguridad y la salud en el trabajo, pero que desde entonces (hace cerca de veintiocho años), se considera un asunto de actualidad.

En su preámbulo, el *Repertorio* aclara la cuestión, al menos en lo que respecta a los datos personales recabados de los trabajadores, que forman parte de los componentes de la vida privada, la privacidad o la intimidad:

> Los datos que los empleadores recaban acerca de los trabajadores y de los candidatos a un puesto de trabajo atienden varios propósitos: acatar la legislación, respaldar la selección de candidatos, la formación y la promoción del personal; salvaguardar la seguridad personal y laboral, el control de calidad, el servicio que se presta a la clientela y la protección de los bienes. Varias leyes nacionales y normas internacionales han establecido procedimientos de carácter obligatorio para el tratamiento de datos personales. La utilización de técnicas informáticas de recuperación de datos, los sistemas automatizados de información relativa al personal, la vigilancia electrónica y los exámenes genéticos y toxicológicos ponen de manifiesto la necesidad de elaborar disposiciones para proteger los datos que se refieran específicamente a la utilización de los datos personales de los trabajadores, con el fin de salvaguardar

> la dignidad de estos, proteger su vida privada y garantizarles el ejercicio de su derecho fundamental a decidir quiénes podrían utilizar determinados datos, con qué finalidad y en qué circunstancias. (OIT, 1996, p. 632).

Dado que se trata de un documento extenso, cuya lectura y consideración es, en nuestra opinión, imprescindible, destacaremos solo algunos de sus aspectos más relevantes. Las recomendaciones expresadas abarcan tanto al sector privado como al público; el tratamiento de los datos personales de las personas trabajadoras debe limitarse a asuntos directamente pertinentes para la relación laboral; los empleadores deberían evaluar periódicamente los métodos de tratamiento de datos para mejorar la protección de la vida privada de los trabajadores; también destacamos la importancia de la información y el consentimiento por parte del trabajador; y que en la protección de los datos personales y en la elaboración de una política de empresa que respete la intimidad de los trabajadores deberían cooperar estos, así como los empleadores y los representantes.

Como se puede apreciar, los parámetros normativos, directrices y recomendaciones derivadas de los documentos mencionados están en armonía con el mismo objetivo: allanar el camino para encontrar puntos de equilibrio, acotar excesos y brindar las bases para la necesaria razonabilidad y ponderación de las acciones y medidas que pudieran afectar o poner en riesgo la dignidad humana de las personas trabajadoras.

### 3. La importancia de los instrumentos de garantía de los derechos humanos

Un sistema jurídico cuyo eje central sean los derechos humanos debe contar con normatividad, organismos y procedimientos

para prevenir las transgresiones de los mismos. De ahí la importancia de la vigilancia o fiscalización estatal y, a su vez, que, en caso de que estas se produzcan, se pueda restablecer el disfrute de tales derechos a sus titulares, así como reparar integralmente las afectaciones causadas. La existencia de normatividad, organismos y procedimientos que permitan la exigibilidad y aplicación institucional de los derechos es un mandato ineludible en los Estados, pero no se debe perder de vista que los derechos humanos reconocidos en la Constitución o en los tratados internacionales pueden aplicarse directamente en situaciones concretas ante la falta o deficiencia de la normatividad pertinente.

La Observación General 17 del Comité de Derechos Humanos de la ONU y el *Repertorio* de la OIT en la materia coinciden en ello, pues de acuerdo con la primera se debe contar con medios y órganos ante los que las personas puedan denunciar la violación del derecho a la vida privada, privacidad o intimidad (párrafo 6). El *Repertorio* aclara aún más la cuestión al señalar:

> Toda ley, reglamento, convenio colectivo, directiva laboral o política elaborada de conformidad con las disposiciones de este Repertorio debería contemplar un procedimiento para que los trabajadores puedan poner en tela de juicio su observancia por parte del empleador. Deberían establecerse procedimientos para recibir y atender las quejas presentadas por los trabajadores. Estos procedimientos deberían ser sencillos y de fácil acceso para los trabajadores (Recomendación 11.13).

En el mismo sentido, los Estados tienen la obligación de contar con instrumentos que garanticen los derechos humanos, un

tema que ha sido ampliamente estudiado por los autores en defensa de la Constitución como parte del *sector de garantía*, y dentro de este, en lo que se conoce como jurisdicción constitucional de la libertad, que hace referencia a aquellas figuras e instrumentos jurídicos cuyo objetivo genérico es restituir la vigencia de la normativa constitucional que protege los derechos humanos cuando ha sido transgredida o desconocida (Fix-Zamudio, 1999).

Desde la perspectiva del derecho internacional de los derechos humanos, uno de los derechos inherentes a toda persona reconocidos desde la Declaración Universal de Derechos Humanos (artículo 8) y la Declaración Americana de los Derechos y Deberes del Hombre (artículo XVIII, última parte), es contar con un recurso o procedimiento sencillo y breve que la ampare contra actos que violen sus derechos previstos en la Constitución. Tal derecho se contempló posteriormente en el PIDCP (artículo 2.3) y con mayor precisión en la CADH, cuyo artículo 25.1 establece lo siguiente:

> 1. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales.

En esta línea de desarrollo, si bien todas las instancias del Estado deben participar en el respeto y la protección de los derechos humanos en el ámbito de sus atribuciones, por instrumentos de garantía se entienden aquellos que tienen por objeto la salvaguarda de los derechos humanos y que culminan

en decisiones finales (por inimpugnables) o terminales (por no estar inicialmente sujetas a un control jurídico ulterior).

A partir de estas consideraciones, se puede deducir que los Estados tienen un papel central en el respeto de los derechos, pero también en la supervisión y fiscalización para que estos estén protegidos en las relaciones laborales del ámbito privado. Asimismo, en el ámbito laboral, las partes contratantes y los actores involucrados, como los sindicatos, tienen un importante margen para adaptar los derechos y su vigencia a los casos concretos, siguiendo pautas que eviten que los trabajadores tengan que ceder más allá de lo razonable, necesario y ponderado. Los conflictos que pudieran surgir al respecto deben tener una vía para ser canalizados y resueltos por las propias partes, a través de instancias de autocomposición, y tener acceso al aparato de justicia estatal, así como a los instrumentos de garantía jurisdiccional y no jurisdiccional de los derechos humanos.

En México, la garantía jurisdiccional de los derechos humanos ha sido tradicionalmente llevada a cabo a través del juicio de amparo, que se vio fortalecido y ampliado para proteger los derechos de fuente internacional gracias a las profundas reformas constitucionales de 6 y 10 de junio de 2011, que situaron a las normas de derechos humanos de los tratados internacionales en un rango constitucional. A esta protección se suma la garantía no jurisdiccional de tales derechos, que desde el 6 de junio de 1990 está a cargo de la Comisión Nacional de los Derechos Humanos (CNDH), y posteriormente también de los organismos públicos de protección de tales derechos en las entidades federativas, en su respectivo ámbito de competencia, que establecieron luego de la reforma que elevó a rango constitucional el sistema no jurisdiccional de protección de derechos en 1992.

A través del juicio de amparo, los derechos se protegen frente a normas generales, actos u omisiones de autoridades o, más específicamente, de personas servidoras públicas que los trasgredan o desconozcan (artículo 103 de la Constitución). El amparo puede interponerse contra leyes, actos u omisiones, o contra sentencias o resoluciones que pongan fin a un juicio, lo que determina el tipo de procedimiento de una sola instancia o de dos instancias, a través de las cuales se tramita el amparo.

En el caso de los órganos públicos no jurisdiccionales, pueden recibir, tramitar y decidir quejas contra actos u omisiones de naturaleza administrativa provenientes de cualquier autoridad o servidor público, con excepción de los del Poder Judicial de la Federación, que violen tales derechos (artículo 102 constitucional, apartado B). Tanto estos órganos, como los dedicados a la protección de la trasparencia y datos personales, pueden también interponer acciones y controversias constitucionales en su ámbito de competencia (artículo 105 constitucional).

Como se puede observar, en ambos instrumentos de garantía, es necesario que sean personas en funciones oficiales la fuente o mediación de la afectación a los derechos básicos de que se trate, ya sea por actos u omisiones. Cabe especificar que el amparo, de ser concedido, culmina en una sentencia que busca restablecer a la persona afectada en el goce del derecho o derechos conculcados, mientras que el procedimiento de queja no jurisdiccional puede terminar con la emisión de una recomendación pública, que busca la reparación integral de las violaciones cometidas, misma a la que se le da seguimiento hasta su total atención luego de ser aceptada por la autoridad o autoridades a las que fue dirigida.

De esta manera, las violaciones de los derechos humanos a la privacidad, vida privada e intimidad de las personas trabajadoras pueden plantearse contra leyes, actos u omisiones de autoridades o personas servidoras públicas a través de los mecanismos mencionados. Por otro lado, cuando la vulneración de los derechos de referencia no sea atribuible a autoridades o personas servidoras públicas, sino a personas o entes particulares, estos encuentran una vía diversa de garantía a través de la normatividad y la instancia en materia de protección de datos personales, en específico cuando estos se encuentran en posesión de particulares.

La privacidad, la vida privada y la intimidad generan, entre otros, diversos datos sobre la persona que pueden definirla, identificarla, caracterizarla, particularizarla o distinguirla de los demás. Esto, a su vez, da origen a la noción de datos personales, objeto de regulación y protección en su obtención, tratamiento y posesión, especialmente en el ámbito de relaciones entre particulares. Esta hipótesis será abordada a continuación.

En México, los datos personales y su protección fueron reconocidos constitucionalmente mediante una reforma constitucional publicada el 1 de junio de 2009, que añadió un segundo párrafo al artículo 16 de la Constitución en el que se establece lo siguiente en relación con la protección de los datos personales:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional,

disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

La garantía institucional de tales derechos se encargó constitucionalmente al mismo organismo autónomo especializado encargado de velar por el derecho de acceso a la información pública, previsto en el artículo 6, apartado A, fracción VIII, de la Ley Fundamental, denominado a partir de 2014 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Las entidades federativas y la Ciudad de México también deben contar con este tipo de órganos en su ámbito competencial (artículo 116, fracción VIII y 122, fracción VII).

De conformidad con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDP), publicada el 5 de julio de 2010, son sujetos regulados por la misma los particulares, ya sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales (artículo 2). Asimismo, a efectos de dicha ley, los datos personales son «cualquier información concerniente a una persona física identificada o identificable» (artículo 3, fracción V) y los datos personales sensibles son «aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. En particular, se consideran sensibles aquellos que puedan revelar aspectos como el origen racial o étnico, el estado de salud presente y futuro, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas y la preferencia sexual» (artículo 3, fracción VI).

De la LFPDP, cabe destacar que los responsables del tratamiento de datos personales deberán observar los principios de licitud,

consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad (artículo 6); que la obtención de datos personales no debe hacerse por medios engañosos o fraudulentos (artículo 7). Existe una presunción razonable de privacidad en todo tratamiento de datos personales (artículo 7); que, con carácter general, dicho tratamiento debe estar sujeto al consentimiento de su titular (artículo 8); y la obligación del responsable de dar a conocer a los titulares de los datos la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (artículo 15).

La LFPDP establece que el INAI tiene facultades de verificación del cumplimiento de la misma (artículos 59 y siguientes), pero también prevé un procedimiento de solicitud de protección de datos (artículos 45 y siguientes), que tramita y decide el propio INAI, con posibilidades de conciliación, y que, en caso de ser favorable a la resolución del titular de los datos, conlleva a que la instancia obligada haga efectivo el ejercicio de los derechos objeto de protección (artículo 48). Los titulares de los derechos que consideren que han sufrido un daño o lesión en sus bienes o derechos por el incumplimiento de la LFPDP por parte del responsable, tienen reconocido su derecho a ejercer las acciones que estimen pertinentes en lo que respecta a la indemnización que proceda según la normativa aplicable (artículo 58).

Las resoluciones del INAI pueden ser impugnadas por los particulares mediante el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa (artículo 56) y, a su vez, pueden difundirse públicamente (artículo 57).

Por último, la LFPDP contiene diversas hipótesis que dan lugar a infracciones y sanciones administrativas (apercibimientos y multas), así como el procedimiento para imponerlas (artículos

61 a 66). Asimismo, se contemplan como delitos en esta materia a quien, estando autorizado para tratar datos personales con ánimo de lucro, provoque una vulneración de la seguridad en las bases de datos bajo su custodia; al que, con el fin de obtener un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que pueda incurrir el titular o la persona autorizada para transmitirlos; o a quien lleve a cabo tales conductas con respecto a datos personales sensibles, hipótesis en la que las penas previstas deben duplicarse (artículos 67 a 69).

Esta breve síntesis muestra que existe un marco normativo e institucional que protege la privacidad, la vida privada y la intimidad, así como los datos que pueden reflejarlas, como derechos oponibles al poder público y a los particulares en el ámbito nacional.

Por último, la protección jurisdiccional y no jurisdiccional de los derechos humanos se ve complementada por la supervisión internacional de los organismos de Naciones Unidas, en particular, a partir de la aceptación de la competencia de los comités encargados de la vigilancia de los tratados que admiten quejas, de las labores de supervisión de la Comisión y de la labor de la Corte, ambas interamericanas de protección de los derechos humanos, así como de la propia labor en este sentido de los órganos pertinentes de la OIT (ILO, 2007).

#### 4. Conclusiones

a) Los derechos humanos se basan en la dignidad humana, que es inherente a todo individuo por el simple hecho de ser humano, sin condición alguna posterior. Entre los derechos humanos reconocidos se encuentran el derecho a la vida privada, así como otros derechos relacionados, como la privacidad y la intimidad,

que permiten el libre desarrollo de la personalidad y acompañan a las personas en sus interacciones con los demás.

b) Los derechos humanos se caracterizan por los principios de universalidad, indivisibilidad, interdependencia y progresividad. Los Estados tienen la responsabilidad de salvaguardar y garantizar la efectividad de los derechos, lo cual implica deberes básicos de respeto, protección y garantía. Asimismo, tanto las personas físicas como jurídicas tienen la obligación de respetar los derechos y la dignidad de los demás, así como los que conciernen a la colectividad.

c) La vida privada, la privacidad y la intimidad son derechos humanos reconocidos en las constituciones, tratados y convenciones internacionales, y son inherentes a la dignidad de todas las personas. Estos derechos deben observarse y respetarse en todos los ámbitos en los que las personas interactúen, incluidas las actividades y relaciones laborales, tanto públicas como privadas.

d) Los avances tecnológicos han generado nuevos fenómenos que afectan al ámbito de lo privado, exponiéndolo o poniéndolo en riesgo. En el contexto laboral, los trabajadores pueden ver comprometidos sus derechos, lo que hace urgente revisar, a la luz de los derechos humanos, posibles respuestas, medidas o estrategias para garantizar que el acceso al trabajo y su desarrollo no comprometan ni la vida privada ni la información de los trabajadores.

e) Los derechos humanos están interrelacionados y su ejercicio no es absoluto, lo que implica que pueden ser regulados o restringidos legítimamente, siempre y cuando se respeten los principios de legalidad, necesidad y proporcionalidad. Existen desarrollos internacionales que ofrecen pautas para ello, y que involucran deberes por parte de los Estados, pero también posibilidades para que los actores involucrados generen reglas y protocolos de actuación.

f) Si bien los derechos humanos pueden delimitarse, es fundamental contar con instancias para la presentación de quejas y la resolución de controversias, tanto en ámbitos privados como públicos. Es responsabilidad ineludible del Estado contar con mecanismos de protección, vigilancia y fiscalización del cumplimiento de los derechos, así como garantías jurisdiccionales y extrajudiciales accesibles para los trabajadores que vean vulnerados sus derechos. En última instancia, existen opciones internacionales de garantía de los derechos humanos y laborales, tanto en la ONU, la OEA como en la OIT.

**Bibliografía**


Aragüez Valenzuela, Lucía, «Debates emergentes en materia laboral y de privacidad: sistemas de videovigilancia, algoritmos digitales e identificación biométrica de la persona trabajadora», en *Thémis-Revista de Derecho*, núm. 79 (Lima: Pontificia Universidad Católica del Perú, 2021), pp. 451-466.

Baz Rodríguez, Jesús, «Protección de datos y garantía de los derechos digitales laborales en el nuevo marco normativo europeo e interno», en *Ars Iuris Salmanticensis* (Estudios), vol. 7 (Salamanca: Universidad de Salamanca, junio de 2019), pp. 129-171.

Belmont Lugo, José Luis, «Una aproximación a las relaciones e influencias entre los derechos humanos y los derechos laborales», en Comisión Nacional de Derechos Humanos y Tribunal Federal de Conciliación y Arbitraje, *Los derechos humanos laborales* (Ciudad de México: Comisión Nacional de los Derechos Humanos-Tribunal Federal de Conciliación y Arbitraje, 2017), pp. 13-90.

Buergenthal, Thomas *et al.*, *Manual internacional de derechos humanos* (Caracas/San José: IIDH-Editorial Jurídica Venezolana, 1990), pp. 9-19.

Carmona Tinoco, Jorge Ulises, «Panorama de la evolución, reconocimiento y protección internacional de los derechos económicos, sociales, culturales y ambientales (DESCA), en el marco de la ONU», en María Elisa Franco Martín del Campo, Guillermo Zepeda Lecuona y Pedro Salazar Ugarte, *Aportes de Sergio García Ramírez al derecho social*, vol. III (Ciudad de México: UNAM-Colegio de Jalisco-Instituto de Estudios Constitucionales del Estado de Querétaro, mayo 2022), p. II-35.

Cobos Campos, Amalia Patricia, «El derecho a la intimidad de los trabajadores y el acceso del patrón a los correos electrónicos empresariales y privados», en *Espaço Jurídico: Journal of Law*, vol. 18, núm. 1 (Florianópolis: Universidad do Oeste de Santa Catarina, Brasil, abril de 2017), pp. 49-63.

Comisión Nacional de los Derechos Humanos (CNDH), *Los principios de universalidad, interdependencia, indivisibilidad y progresividad de los derechos humanos* (Ciudad de México: Comisión Nacional de los Derechos Humanos, 2018).

Corte Interamericana de Derechos Humanos, *Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos Humanos: Restricción y suspensión de derechos humanos*, núm. 26 (San José, Costa Rica: Corte Interamericana de Derechos Humanos y Cooperación Alemana, GIZ, 2020).

Cruz Caicedo, Maritza *et. al.*, *Nuevas tecnologías y derecho del trabajo* (Bogotá: Universidad Externado de Colombia, 2020).

Fix-Zamudio, Héctor, *Protección jurídica de los derechos humanos. Estudios comparativos*, 2ª ed. (Ciudad de México: CNDH, 1999).

International Labor Organization (ILO), «Labor Rights, Human Rights», en *International Labor Review*, vol. 137, núm. 2 (Ginebra: ILO, 1998), pp. 127-133.

International Labor Organization (ILO), *Protecting Labour Rights as Human Rights: Present and Future of International Supervision*, George P. Politakis (ed.). Actas del coloquio internacional con motivo del 80º aniversario de la Comisión de Expertos en Aplicación de Convenios y Recomendaciones de la OIT (Ginebra: ILO, 2007).

Kurczyn Villalobos, Patricia, «Apuntes sobre los derechos humanos en el ámbito laboral. Los derechos sociales», en Patricia Kurczyn Villalobos (coord.), *Derechos humanos en el trabajo y la seguridad social*. Liber Amicorum: en homenaje al doctor Jorge Carpizo (Ciudad de México: UNAM, 2016).

Morales Corrales, Pedro y Alejandro Morales Cáceres, «El impacto de las nuevas tecnologías en las relaciones laborales», en *Ius et Praxis, Revista de la Facultad de Derecho*, núm. 52 (Lima: Universidad de Lima, julio de 2021), pp. 357-391.

Nikken, Pedro, «El concepto de derechos humanos», en Instituto Interamericano de Derechos Humanos, *Antología básica en derechos humanos* (San José, Costa Rica: Instituto Interamericano de Derechos Humanos, 1994), pp. 11-19.

Organización Internacional del Trabajo (OIT), «Recomendaciones de la OIT para proteger los datos personales del trabajador», en *Revista Internacional del Trabajo*, vol. 115, núm. 5 (Ginebra: OIT, 1996), pp. 629-640.

----------. *Declaración de la OIT relativa a los principios y derechos fundamentales en el trabajo y su seguimiento*, publicada en 1998 y enmendada en 2022 (Ginebra: OIT, 2022).

Reynoso Castillo, Carlos, «Privacidad y protección de datos en las relaciones laborales», en *Revista Alegatos*, núm 95 (Ciudad de México: Universidad Autónoma Metropolitana, 2017), pp. 119-146.

Sánchez Castañeda, Alfredo, «Los derechos humanos laborales en el ámbito internacional: entre una consolidación normativa y desafíos por afrontar», en Comisión Nacional de Derechos Humanos y Tribunal Federal de Conciliación y Arbitraje, *Los derechos humanos laborales* (Ciudad de México: Comisión Nacional de los Derechos Humanos-Tribunal Federal de Conciliación y Arbitraje, 2017), pp. 139-190.

Sanz Salguero, Francisco Javier, «Delimitación de las esferas de la vida privada, privacidad e intimidad, frente al ámbito de lo público», en *Transparencia & Sociedad*, núm. 6 (Chile: Consejo para la Transparencia, 2018), pp. 127-149.

Segura Castañeda, Diana Estefany, «El derecho a la intimidad del trabajador como restricción al poder subordinante del empleador: el incipiente desarrollo en Colombia frente al derecho comparado», en *Revista de Derecho Público*, núm. 34 (Bogotá: Universidad de los Andes, Facultad de Derecho, enero-junio de 2015), pp. 3-26.

Sepúlveda, César, *Estudios sobre derecho internacional y derechos humanos*, 2ª edición (México: Comisión Nacional de los Derechos Humanos, 2000).

CAPÍTULO II

# Reflexiones generales en torno a las relaciones y tensiones entre los derechos laborales y la privacidad[1]

**María Villa Fombuena**
Profesora Titular de Derecho del Trabajo y de la Seguridad Social
CEU Cardenal Spínola, adscrito a la Universidad de Sevilla

## Introducción

Reflexionar sobre la privacidad y los derechos laborales resulta esencial en la sociedad actual, donde tecnología y prácticas laborales están en constante evolución. Los derechos laborales son fundamentales para garantizar tanto condiciones de trabajo justas como un entorno laboral seguro. Esto resulta especialmente relevante en un mundo digital donde las comunicaciones laborales, la gestión de datos, la vigilancia en el lugar de trabajo o las decisiones algorítmicas, entre otros, plantean un verdadero desafío. Por un

1 Este trabajo se enmarca en el Proyecto de Investigación PID2021-122537NB-I00 «La negociación colectiva como instrumento de gestión anticipada del cambio social, tecnológico, ecológico y empresarial», financiado por el Ministerio de Ciencia e Innovación del Gobierno de España.

lado, frente a la posible intromisión en el ámbito más privado de las personas trabajadoras. Por otro, teniendo presente que la tecnología actual otorga habilidades empresariales sin precedentes, lo que la convierte en una poderosa herramienta. En este sentido, encontrar un equilibrio entre la protección de la privacidad y la aplicación empresarial de tecnologías avanzadas como la Inteligencia Artificial o el Big Data para mejorar la productividad supone, además de una ardua tarea, un reto inmenso que requiere la colaboración entre empleadores, trabajadores y legisladores.

En este capítulo se van a abordar las cuestiones principales que pueden ayudar en la consecución de tan ambicioso objetivo.

## 1. La privacidad como derecho fundamental. Su delimitación desde un prisma de derecho comparado

El incremento y la intensificación que ha experimentado el poder de control empresarial de mano de las nuevas tecnologías acarrean un riesgo cierto para el ámbito privado del trabajador. Ámbito que, sin embargo, no resulta siempre claro y que en consecuencia plantea dudas sobre la licitud de algunas de estas prácticas de control aplicadas por las empresas a sus trabajadores.[2]

Como se apuntaba al inicio y se verá más adelante, las posibilidades de uso y el alcance de análisis que permiten las tec-

---

[2] Según los datos estadísticos facilitados por Google, la búsqueda en internet de los términos «intimidad» y «privacidad» en relación con otros como «trabajo» o «empresa» se incrementó en los países latinoamericanos un cien por ciento en el segundo semestre de 2020 con ocasión de la COVID-19, descendió ligeramente en 2021 y experimentó un ascenso continuo desde 2022, volviendo a alcanzar desde entonces el cien por ciento en una amplia mayoría de estos países. Censo disponible en: https://trends.google.es/trends?geo=VE&hl=es

nologías actuales genera en las personas trabajadoras un recelo intenso tanto de los medios y dispositivos utilizados para llevar a cabo la prestación laboral como de los empleados por la empresa en su capacidad de control de esta. Y es aquí donde nace la incertidumbre ante la amplitud de nociones que pueden entrar en funcionamiento: intimidad, privacidad, protección de datos personales, inviolabilidad de las comunicaciones, etc.

Resulta cuanto menos curioso el hecho de que la primera aparición escrita del término «privacidad» tuviera lugar en un país que, en la actualidad, se caracteriza por tener una protección cuestionable precisamente de este derecho esencial. Y es que este vocablo «privacidad» es un anglicismo. Proviene del término inglés *privacy*, que apareció por primera vez en 1890 en la revista *Harvard Law Review*, con ocasión de una crítica en clave jurídica hacia la prensa elaborada por dos reconocidos abogados de Boston (Samuel D. Warren y Louis D. Brandeis), convencidos de la necesidad de proteger la vida privada frente a la falta de escrúpulos de la prensa, a la que acusaban de intromisión en la vida privada por sobrepasar continuamente los límites de la propiedad privada y la decencia para entretener al lector. Ambos sostenían que impedir la publicación de información privada suponía un ejemplo del derecho genérico de todo individuo a no ser molestado (*the right to be let alone*). En este sentido, Warren y Brandeis consideraban que el derecho a la privacidad otorga a la persona plena libertad para decidir en qué medida pueden ser comunicados a otros sus pensamientos, sentimientos y emociones.[3]

---

[3] *Vid.* S. D. Warren y L. D. Brandeis, «Right to privacy», en *Harvard Law Review*, vol. IV, núm. 5, diciembre de 1890, pp. 193-220. Existe también una versión traducida por B.

No obstante, la inclusión de este término en un texto legal de ámbito internacional no se produciría hasta 1948 con la Declaración Universal de Derechos del Hombre, cuyo artículo 12 recogía el derecho a ser protegido por la ley contra injerencias arbitrarias en la vida privada, la familia, el domicilio o la correspondencia, y contra ataques a la honra o a la reputación. Lo que, tal y como se menciona en el capítulo anterior, se reiteró en similares términos en 1966 en el artículo 17 del Pacto Internacional de Derechos civiles y políticos; a cuyo análisis dedicaría en 1988 el Alto Comisionado de las Naciones Unidas para los Derechos Humanos la Observación General N.º 16.[4]

En lo que respecta al ámbito laboral en particular, no sería hasta 1990 cuando el artículo 14 de la Resolución adoptada por las Naciones Unidas en el seno de la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares[5] recogió una protección idéntica para estos.

Volviendo al ámbito genérico y en términos similares a los plasmados hasta la fecha, se pronunciaban el artículo 18 de la Declaración de El Cairo sobre los Derechos Humanos en el Islam de 1990; la Declaración de principios sobre la libertad de expresión en África de la Comisión Africana de Derechos Humanos y de los Pueblos; los artículos 16 y 21 de la Carta Árabe de Derechos Humanos de 2004; el coetáneo Marco de cooperación económica Asia-Pacífico en materia de privacidad; y, aun-

---

Pendás y P. Baselga titulada *El derecho a la intimidad* (Madrid: Editorial Civitas, 1995).

4 *Derecho a la intimidad (Art. 17)*, HRC Observación general N.º 16 (General Comment), 32º período de sesiones, 1988.

5 Resolución 45/158 de la Asamblea General de 18 de diciembre de 1990.

que con mayor controversia, el artículo 21 de la Declaración de Derechos Humanos de la Asociación de Naciones del Sudeste Asiático de 2012. A partir de 2013, la aparición de textos de referencia ha sido aún más prolífica. Desde entonces, la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos han aprobado numerosas resoluciones sobre el derecho a la privacidad en la era digital.[6]

A nivel regional, este derecho ha encontrado amparo tanto en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 (artículo 8) como en el texto de la Convención Americana de Derechos Humanos de 1969 (artículo 11); y posteriormente en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1985; la Recomendación N.º R(99) 5 del Consejo de Europa sobre la protección de la intimidad en Internet de 1999; o en el Protocolo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, relativo a las autoridades de control y a los flujos transfronterizos de datos de 2001.

La mayor regulación de este derecho ha tenido lugar, no obstante, en la Unión Europea, en donde la relación de normas que contemplan la protección de este derecho es amplísima, destacando de manera especial el Reglamento (UE) 2016/679 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; la actual propuesta de Reglamento del Parlamento Europeo y del Consejo sobre

---

[6] Disponibles en: https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy

el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (conocido como Reglamento ePrivacy) y que derogará la Directiva 2002/58/CE; y el recién aprobado Reglamento sobre Inteligencia Artificial. De este conglomerado normativo, tanto el RGPD como el Reglamento ePrivacy resultan normas complementarias, tal y como ha declarado el propio Comité Europeo de Protección de Datos (CEPD).[7] Si la primera protege los derechos sobre los datos de los ciudadanos de la UE recogiendo pautas y obligaciones para que empresas y organizaciones garanticen la privacidad de las personas, la segunda pone el foco en la privacidad de las comunicaciones electrónicas, ofreciendo garantías adicionales de confidencialidad y protección. Por su parte, el Reglamento sobre Inteligencia Artificial, consciente de que la IA implica un nuevo reto para la privacidad, establece un marco normativo integral para el uso de sistemas de IA en los Estados miembros de la UE con robustos estándares de seguridad y defensa de los derechos fundamentales; reflejando un compromiso firme con la protección de la privacidad y la seguridad en el uso de tecnologías. Este trío normativo contribuye así a la consecución del objetivo del Parlamento Europeo de hacer de la protección de la intimidad una prioridad política. Y es que esta institución viene insistiendo en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de la vida privada.

---

[7] Declaración 03/2021, relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas. Adoptada el 9 de marzo de 2021. Disponible en: https://www.edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_es.pdf

Nótese que en la mayoría de los textos europeos su tutela se plantea de manera específica frente al uso de las tecnologías de la información y de las comunicaciones. El motivo responde al empleo normativo de una diferenciación conceptual, al menos, en este espacio geográfico. Y es que privacidad e intimidad no son exactamente lo mismo. Mientras que el término «intimidad» alude a la esfera en la que se desarrollan las facetas más singularmente reservadas de la vida de la persona, como puede ser el domicilio donde realiza su vida cotidiana, la «privacidad» supone un concepto más amplio. Esta última constituye un conjunto de facetas de su personalidad que, aisladamente consideradas, pueden carecer de relevancia propia, pero que, coherentemente enlazadas entre sí, proporcionan un retrato de la personalidad del individuo que este tiene derecho a mantener reservado. Este es precisamente el ámbito que puede resultar menoscabado por la utilización de las tecnologías actuales y en desarrollo. Desde esta óptica se entiende la necesidad normativa planteada de contar con un término propio para hacer referencia a una realidad concreta. Es importante destacar que el derecho a la privacidad es más reciente que el derecho a la intimidad, a pesar de que los textos internacionales los empleen de manera indiferenciada.

### 2. Posibilidades y riesgos de la tecnología actual y futura

Nos encontramos inmersos en una era de continua y revolucionaria innovación tecnológica, donde el avance de las tecnologías digitales no conoce límites, consolidándose como el principal catalizador de cambios tanto en la sociedad como en la economía. Esta evolución es constante e inevitable y marca un nuevo rumbo que redefine nuestra realidad de manera irreversible. En los últi-

mos años, a los progresos en áreas como las telecomunicaciones, la nanotecnología, el internet de las cosas o el Big Data, que han impulsado los pilares fundamentales de la cuarta revolución industrial (digitalización, conectividad y automatización), se le une la Inteligencia Artificial, que nos adentra en una nueva revolución industrial, en la que el protagonismo humano vendrá indiscutiblemente conectado a su interrelación eficaz con las máquinas.

La influencia de esta evolución tecnológica es transversal. La adopción de estas nuevas tecnologías ha redefinido nuestra manera de vivir, de trabajar y de interactuar. En este sentido, la tecnología ha permitido una mayor conectividad entre personas de todo el mundo, facilitando así la comunicación, la colaboración y el acceso a la información; ha contribuido al incremento de la eficiencia en diversos sectores a través de la automatización de tareas repetitivas y la optimización de procesos; ha conducido y seguirá conduciendo a avances significativos en la medicina (como el desarrollo de tratamientos más efectivos o la medicina personalizada); y ha facilitado además herramientas para la innovación y la creatividad en diversos campos. En suma, las posibilidades que ofrece la implementación tecnológica son enormes y muy variadas, pero también complejas, pues dependen en gran medida de cómo se utilicen y cómo se regulen.

A lo anterior se adiciona el hecho de que nos hallamos inmersos en una sociedad profundamente interconectada, donde la tecnología permea cada aspecto de nuestra vida cotidiana. Desde nuestros teléfonos inteligentes hasta nuestros electrodomésticos, prácticamente todos los dispositivos que utilizamos están constantemente transmitiendo una cantidad significativa de datos a través de Internet. Sirvan de ejemplo algunas de las

cifras por minuto facilitadas en el informe *The Internet in every minute 2023*[8], dignas de ser mencionadas, como es el caso de los 241.2 millones de emails enviados, los 18.8 millones de mensajes de texto, los 3.02 millones de fotos realizadas con smartphones o las 271 309 aplicaciones descargadas en sistemas iOS y Android. No obstante, se debe tener presente que todas estas cifras aluden a datos; los cuales por sí solos no tienen mucho significado, pues suponen una simple combinación de unos y ceros.

Ahora bien, este código binario carga, sin embargo, una información muy valiosa. En otras palabras, cuando esos datos se recopilan y se analizan a gran escala utilizando tecnologías como el Big Data y/o la Inteligencia Artificial, se transforman en conocimiento. Por un lado, el Big Data permite identificar patrones, tendencias y correlaciones en los datos para ayudar (a las empresas) a tomar decisiones más informadas y estratégicas. Por otro, la Inteligencia Artificial, especialmente el aprendizaje automático, puede analizar grandes volúmenes de datos de manera rápida y automatizada para identificar perspectivas y generar predicciones consecuentes. En suma, los datos aparentemente insignificantes pueden ser transformados en información realmente valiosa, lo que los convierte hoy en el activo empresarial más preciado. De ahí la obsesión actual de las empresas por acumular la mayor cantidad de datos posible, ya sea para su utilidad actual o futura. Solo hay que observar, cada vez que accedemos a una web o descargamos una aplicación, la inmediatez con la que hace aparición la necesaria aceptación de una política de privacidad con la que, por cierto, vamos a autorizar la invasión de nuestra privacidad.

---

8 Elaborado por eDiscovery Today y Legal Tech Media Group (LTMG).

Reconociendo la magnitud de este impacto, es evidente que la simple implementación de estas tecnologías no es suficiente; deben ser integradas de manera efectiva. Es decir, la digitalización no debe ser vista como un fin en sí mismo ni limitarse únicamente a la incorporación de nuevas tecnologías. Es esencial comprender que su aplicación conlleva no solo cambios fundamentales en los ámbitos económico, social, legal e incluso cultural, sino que también acarrea riesgos. Por ello, la implementación tecnológica debe abordarse de manera responsable y ética para maximizar sus beneficios y mitigar sus riesgos, que no son pocos.

En un plano genérico, podrían identificarse algunos de esos riesgos con:

a) *La ciberseguridad*. Y es que la creciente dependencia de la tecnología, el aumento de la conectividad y la digitalización de los procesos empresariales incrementan la exposición a ataques cibernéticos (como el *malware*, el *phishing* o el *hacking*), lo que a su vez puede comprometer la seguridad de los datos y de las redes y la integridad de los propios sistemas informáticos;
b) *La privacidad*. La recopilación masiva de datos personales por parte de empresas y gobiernos plantea preocupaciones sobre la privacidad de los individuos, especialmente en relación con el uso indebido de datos y la falta de control sobre la información personal, lo que puede desembocar en discriminación, en una vigilancia invasiva o incluso en un abuso de poder;
c) *La manipulación de la información*. Las plataformas de redes sociales y los algoritmos de recomendación pueden ser utilizados para difundir desinformación, noticias falsas

e incluso propaganda. Esto puede acarrear un peligro cierto de erosión de la democracia, de polarización de la sociedad y un debilitamiento de la confianza en los medios de comunicación.

d) *La adicción y la dependencia tecnológica*. Se debe ser consciente de que el uso excesivo de dispositivos electrónicos puede afectar la salud mental, el bienestar emocional y las relaciones interpersonales;

e) *La desigualdad digital*. A medida que la tecnología avanza velozmente se incrementa el riesgo de que aquellos grupos de la población con bajos ingresos o los ubicados en zonas rurales puedan quedar rezagados en términos de acceso y habilidades tecnológicas, lo que sin duda ampliaría la brecha digital y aumentaría la desigualdad económica y social.

En el ámbito de las relaciones laborales, los peligros se identifican sin embargo con:

a) *El desempleo tecnológico*. La automatización y la inteligencia artificial están transformando muchos sectores laborales, lo que no pocos han vaticinado que podría resultar en la pérdida de empleos para aquellos cuyas tareas pueden ser realizadas de manera más eficiente por máquinas, planteando así desafíos económicos y sociales significativos, como la desigualdad y el desempleo estructural.

b) *La falta de habilidades y formación adecuada*. El rápido avance tecnológico requiere que los trabajadores adquieran nuevas habilidades y conocimientos para seguir resultando «atractivos» en el mercado laboral. Precisamente la falta de acceso a una formación adecuada puede dejarles desactualizados y en riesgo de quedar obsoletos.

c) *Condiciones laborales precarias*. La implementación de tecnologías como la automatización y la monitorización constante puede contribuir al empeoramiento de las condiciones laborales, incluyendo una mayor carga de trabajo, falta de privacidad y constante supervisión, lo que puede afectar negativamente la salud y el bienestar de los trabajadores.
d) *La discriminación algorítmica*. Los algoritmos utilizados en la contratación y en la gestión del talento pueden introducir sesgos y discriminación basados en variables como la edad, el género o la etnia, lo que puede perpetuar y amplificar la discriminación existente en el ámbito laboral.

En consecuencia, resulta imprescindible abordar estos riesgos de manera proactiva mediante la implementación de políticas y de regulaciones efectivas, la promoción de la alfabetización digital y la concienciación pública, la formación continua de los trabajadores y el desarrollo de tecnologías éticas, responsables y transparentes.

### 3. Las particularidades del contexto laboral como campo de aplicación

La aceleración del desarrollo tecnológico ha irrumpido de manera brusca en el ámbito empresarial, en el que no solo se han alterado sus rasgos clásicos sino también ciertos aspectos laborales.

En primer lugar, los modelos de negocio actuales han modificado su forma de funcionar para poder actuar en un mercado caracterizado por una competitividad feroz. En este sentido, no solo han fragmentado la producción para poder afrontar en mejores condiciones las fluctuaciones del mercado, sino que igualmente han hecho aparición nuevas formas de financiación a través de mecanismos colaborativos de carácter económico. Por otro lado, en este contexto de tecnificación digital, las empresas

han optado igualmente por una mayor flexibilidad en la organización de su mano de obra, lo que ha dado lugar a nuevas formas de desarrollo de la prestación de trabajo en las que se le permite al trabajador un amplio margen de decisión. Un ejemplo destacado es la intensificación del teletrabajo en los últimos años, especialmente con motivo de la pandemia de COVID-19.

Sin embargo, este amplio margen de capacidad autoorganizativa con el que cuenta el trabajador provoca un efecto doble. Por un lado, merma en cierto sentido la facultad de organización del empleador, pero por otro, y de forma paralela, incrementa su poder de control. Es decir, no solo aumenta la autonomía de decisión y gestión del trabajador, sino que en igual medida lo hace la capacidad y la intensidad de los instrumentos de control de los que puede valerse el empleador. En otras palabras, el poder de organización pierde intensidad en detrimento del poder de control. Para el empleador ya no es imprescindible que el trabajador se someta a estos elementos tradicionales de organización del trabajo. Su interés pasa a focalizarse en la capacidad de controlar tanto la manera en la que el trabajador realiza la prestación como el resultado de esta; y en esa labor las nuevas tecnologías desempeñan un papel crucial, pues permiten una trazabilidad del trabajo sin precedentes.

En segundo lugar, esta globalización digital a la que se viene aludiendo posibilita la obtención de un flujo ilimitado de información y, por tanto, de conocimiento, lo que permite a las empresas optimizar su productividad a través de una utilización eficaz y eficiente de los recursos. Gracias a este aprovechamiento de la información disponible, las empresas pueden identificar oportunidades de mejora, anticiparse a las demandas del mercado, optimizar sus procesos internos y maximizar el rendimiento

de sus recursos. Pero igualmente, en lo que atañe de manera específica al ámbito laboral, este enfoque puede contribuir a alcanzar diversos objetivos de manera óptima.

El primero de ellos sería la mejora de la eficiencia operativa; al recopilar y analizar datos relacionados con el desempeño de los empleados, los procesos de trabajo y el entorno laboral, las empresas pueden identificar áreas que necesitan mejoras. Esto podría incluir, por ejemplo, la detección de cuellos de botella en los procesos de trabajo, la identificación de patrones de comportamiento que puedan evidenciar problemas de productividad, o de necesidades de formación y desarrollo profesional para el personal.

Un segundo objetivo sería la posibilidad de anticiparse a las demandas del mercado; la recopilación y análisis de datos propios del mercado laboral, como pueden ser las tendencias de contratación, las tasas de rotación de empleados o las habilidades más demandadas, pueden ayudar a las empresas a anticiparse a las necesidades futuras de talento y a desarrollar estrategias de contratación y retención de personal más efectivas. Esto les permitiría una mejor preparación para afrontar posibles cambios en el mercado laboral y garantizar que cuentan con el personal y las habilidades adecuados en el momento adecuado.

Como tercer objetivo se plantearía la optimización de procesos internos; mediante el seguimiento y análisis de datos relacionados con los procesos de trabajo y las actividades diarias de los empleados, las empresas pueden identificar áreas de ineficiencia y tomar medidas para optimizar los procesos internos, como puede ser la automatización de tareas repetitivas, la reasignación de recursos para mejorar la carga de trabajo o la implementación de tecnologías que faciliten la colaboración y la comunicación entre los equipos.

En último lugar, este aprovechamiento de la información permitiría maximizar el rendimiento de los recursos; al comprender mejor cómo se utilizan los recursos humanos y materiales en la organización, las empresas pueden tomar decisiones más informadas sobre su asignación y la planificación de proyectos. Esto les permitiría no solo maximizar la utilización de recursos, sino también minimizar los costes asociados al exceso de capacidad o a la falta de estos. Resulta indiscutible que todos estos objetivos contribuirían al éxito de la organización a largo plazo; lo que también debe quedar patente es que igualmente ayudarían al bienestar de sus empleados.

Resulta necesario incidir en el redimensionamiento de la capacidad de las empresas para vigilar y verificar el desarrollo de la actividad laboral. La asequibilidad de muchas de las tecnologías actuales ha facilitado sin duda la generalización de su uso en las empresas, ya sea en el plano específico de la prestación de servicios de mano de algunas herramientas de trabajo (como puede ser el caso de los dispositivos digitales que la empresa facilita a sus trabajadores, del correo electrónico corporativo o de las aplicaciones de mensajería instantánea y redes sociales que pueden utilizar las empresas); ya sea en un plano laboral más amplio a través de mecanismos de control o del tratamiento automatizado de los datos de los que dispone la empresa para la toma de decisiones, entre otros. Y es que estas tecnologías ofrecen a las empresas una inusitada capacidad de seguimiento preciso del trabajo que se está llevando a cabo. Esto es, las actuales tecnologías de la información y la comunicación permiten al empleador contar con una trazabilidad del trabajo sin precedentes como se apuntaba anteriormente. Sirvan de ejemplo, los avances producidos en comunicaciones (5G)

o en dispositivos inteligentes, que no solo han alterado la manera de trabajar o los cauces de comunicación entre la empresa y el trabajador, sino que permiten ubicar geográfica y temporalmente a cualquier empleado con una precisión extraordinaria.

Pero, como hemos visto, esa gran capacidad de obtención de información (datos a todos los efectos) con la que cuentan las empresas en la actualidad, y que les permite llevar a cabo ese control tan exhaustivo de la prestación que realizan sus trabajadores, puede acarrear también una intensa intromisión en la esfera privada de estos si el uso de la tecnología no va acompañado de determinadas garantías. En consonancia, resulta evidente la imbricación entre el actual escenario tecnológico-digital y el aumento del poder de control empresarial, de manera que el avance del primero repercute en el segundo.

#### 4. Necesidad de regulación y control específico

El avance tecnológico ha sido tan vertiginoso que ha superado con creces la capacidad de regulación existente en el ámbito laboral, haciendo patente el distanciamiento temporal entre la norma y la realidad. Y es que, si normalmente el derecho siempre va por detrás del hecho, pues su esencia es dar respuesta al problema que surja, en el caso de la tecnología el abismo temporal se incrementa sensiblemente por la velocidad vertiginosa de su avance. La omnipresencia y accesibilidad de la tecnología han transformado radicalmente las estructuras y normas tradicionales, generando un desfase evidente entre la ley y la realidad laboral. Esta brecha se ha hecho más notoria con el tiempo, ya que las posibilidades que ofrece la tecnología actual en este entorno han evolucionado rápidamente, obligando a una constante

adaptación normativa para mantenerse al día con las demandas cambiantes del mundo laboral.

Las herramientas tecnológicas han revolucionado la forma en que se llevan a cabo las tareas. Desde la comunicación hasta la gestión de proyectos, la tecnología ha optimizado los procesos y aumentado la eficiencia en todos los niveles. Sin embargo, esta rápida evolución tecnológica ha dejado obsoletas muchas de las normativas laborales existentes, que no han sido capaces de adaptarse a las nuevas realidades laborales impulsadas por la tecnología.

Uno de los principales desafíos radica en la necesidad de garantizar los derechos laborales en un entorno cada vez más digitalizado. ¿Cómo se pueden proteger entonces los límites entre la vida laboral y personal cuando la tecnología permite estar conectado de manera permanente? En otras palabras, la regulación sobre el tiempo de trabajo y el derecho a la desconexión digital se enfrenta a nuevos retos con la introducción de tecnologías que permiten el trabajo remoto y la comunicación constante a través de dispositivos móviles. En este sentido, el diseño de procesos colaborativos y de distribución del trabajo, la capacidad de gestión de los recursos humanos, la existencia y claridad de protocolos que regulen el uso de dispositivos y tecnologías, y que determinen los procedimientos de control que podrán llevarse a cabo, resultan, en consecuencia, esenciales.

Además, la tecnología ha cambiado la naturaleza misma del trabajo, creando nuevas formas de empleo, como es el caso del teletrabajo, que desafían las categorías tradicionales de empleo y generan incertidumbre en cuanto a la protección laboral y los derechos de los trabajadores.

Por otro lado, la recopilación y uso de datos en el ámbito laboral plantea importantes cuestiones éticas y legales. ¿Quién tiene

acceso a los datos recopilados sobre el desempeño de los empleados? ¿Cómo se utilizan esos datos y cuál es su impacto en la toma de decisiones laborales, como la contratación, la evaluación del desempeño y la promoción?

En este contexto, la regulación laboral debe adaptarse de manera continua y proactiva no solo para abordar los desafíos emergentes y garantizar que los derechos de los trabajadores estén protegidos en un entorno laboral digital en constante cambio, sino igualmente, y de forma paralela, para permitir que empresas e instituciones puedan conocer qué pueden y qué no pueden implementar por mucho que lo deseen.

Dentro de ese marco legal debe igualmente contemplarse un campo de acuerdo entre empresas y trabajadores, como cauce idóneo de aplicación adaptada a la singularidad de cada entidad. Y es que la negociación colectiva desempeña un papel fundamental en la adaptación de la regulación laboral a los cambios tecnológicos al erigirse en una herramienta poderosa para abordar los desafíos emergentes y garantizar los derechos de los trabajadores. De un lado, la negociación colectiva puede facilitar la incorporación de cláusulas específicas relacionadas con el uso de la tecnología, como sería el caso de disposiciones sobre el derecho a la desconexión digital, el uso de herramientas tecnológicas en el trabajo remoto o la protección de datos personales de los trabajadores. Cláusulas que, además de proporcionar un marco claro y equitativo para regular el uso de la tecnología en el lugar de trabajo, aseguran que se respeten los derechos de los trabajadores y se promueva un entorno laboral saludable y productivo. De otro lado, esta vía puede ser un cauce idóneo para abordar igualmente cuestiones relacionadas con la formación y el desarrollo profesional en el contexto de la

transformación digital. En este sentido, sindicatos y empleadores pueden colaborar para desarrollar programas de capacitación y reciclaje que ayuden a los trabajadores a adquirir las habilidades necesarias para adaptarse a las nuevas tecnologías y mantenerse atractivos en un mercado laboral en constante cambio. Esto no solo beneficiaría a los trabajadores al mejorar su empleabilidad y garantizar su seguridad laboral, sino que también favorecería a las empresas al garantizar que cuentan con una fuerza laboral cualificada y adaptable. En suma, mediante el fomento del diálogo y la colaboración entre los trabajadores y empleadores, la negociación colectiva puede contribuir a construir un futuro del trabajo que beneficie a todos los actores involucrados.

Todo lo anterior requiere una colaboración estrecha entre legisladores, empleadores, trabajadores y expertos en tecnología para desarrollar marcos normativos flexibles y equitativos que promuevan un equilibrio adecuado entre la innovación tecnológica y la protección de los derechos laborales. Solo así podremos asegurar que la tecnología beneficie a todos y no desequilibre la balanza a favor o en contra de alguna de las partes de la relación laboral, amplificando las desigualdades existentes.

## 5. Conclusiones

El análisis recogido aquí revela la imperiosa necesidad de adaptar la regulación laboral a los avances tecnológicos y las nuevas realidades laborales. A medida que la tecnología permea todos los aspectos de nuestras vidas, se plantean preocupaciones sobre la protección de la privacidad y la gestión ética de los datos personales en el ámbito laboral. En particular, la privacidad como derecho fundamental enfrenta desafíos sin precedentes debido al

creciente poder de control empresarial impulsado por las nuevas tecnologías. Desde su primera mención formal en la Declaración Universal de Derechos Humanos de 1948 hasta la proliferación de regulaciones específicas como el Reglamento General de Protección de Datos de la Unión Europea en 2016, se ha sostenido un esfuerzo constante por definir y proteger este derecho.

Por otro lado, las posibilidades y riesgos de la tecnología actual y futura nos sitúan en una encrucijada donde su implementación responsable y ética resulta crucial para maximizar sus beneficios y mitigar sus riesgos.

En el contexto laboral, la tecnología ha redefinido las relaciones entre empleadores y empleados. La digitalización ha permitido una mayor flexibilidad en la organización del trabajo y una optimización de los procesos empresariales, pero también ha dado lugar a nuevos desafíos, como el desempleo tecnológico, la falta de habilidades adecuadas y las condiciones laborales precarias. Es esencial abordar estos desafíos mediante políticas y regulaciones efectivas que protejan los derechos de los trabajadores y promuevan un entorno laboral justo y equitativo.

Ante estos desafíos, es fundamental que la regulación laboral evolucione de manera proactiva para abordar los cambios tecnológicos y garantizar los derechos de los trabajadores. Esto implica establecer normas claras sobre el uso de la tecnología en el lugar de trabajo, proteger la privacidad de los empleados y promover un equilibrio adecuado entre la innovación tecnológica y la protección de los derechos laborales. En este marco, la negociación colectiva emerge como una herramienta poderosa para adaptar con garantías la regulación laboral a los cambios tecnológicos, no solo facilitando la incorporación de cláusulas

específicas relacionadas con el uso de la tecnología, sino igualmente promoviendo la formación y el desarrollo profesional en el contexto de la transformación digital. Dicho de otra forma, la negociación colectiva puede contribuir a construir un futuro del trabajo que beneficie a todos los actores involucrados.

En resumen, la regulación laboral debe evolucionar de manera continua y proactiva para abordar los desafíos emergentes y garantizar que los derechos de los trabajadores estén protegidos en un entorno laboral digital en constante cambio. El avance tecnológico ha planteado nuevos desafíos para la protección de la privacidad y los derechos laborales, pero también ofrece oportunidades para mejorar la eficiencia y la productividad. Para aprovechar al máximo estas oportunidades y mitigar los riesgos asociados, es necesario un enfoque colaborativo y proactivo que involucre tanto a empleadores y trabajadores como a expertos en tecnología y a los poderes públicos en la formulación de políticas y regulaciones adecuadas.

En este contexto, cada rama del poder público desempeña un papel crucial. Hemos visto como el poder legislativo tiene la tarea de crear y aprobar leyes que regulen el uso de nuevas tecnologías en el ámbito laboral y protejan los derechos de los trabajadores. Esto incluye la formulación de leyes de privacidad que aborden los desafíos específicos planteados por las tecnologías avanzadas, así como la creación de marcos regulatorios que aseguren condiciones laborales justas y equitativas en un entorno tecnológico en constante evolución; lo que conduce a la conveniencia de que los legisladores trabajen en estrecha colaboración con expertos en tecnología, trabajadores y empleadores para asegurarse de que las leyes sean pertinentes y efectivas.

Por su parte, el ejecutivo, como responsable de la implementación de políticas y regulaciones, puede, además de establecer agencias o departamentos específicos para supervisar el impacto de las tecnologías emergentes en la privacidad y los derechos laborales, promover la inversión en tecnologías que mejoren la eficiencia y la productividad sin comprometer la privacidad ni los derechos de los trabajadores. Incluso liderar iniciativas para fomentar la colaboración entre el sector público y privado, así como la creación de programas de capacitación y *reskilling* para la fuerza laboral.

En su función de interpretación y aplicación normativa, los tribunales pueden establecer precedentes importantes sobre cómo deben ser protegidos los derechos de privacidad y laborales en este contexto tecnológico.

Este enfoque integrado, donde cada rama del poder público trabaja en sus respectivos roles, es esencial para abordar los desafíos y aprovechar las oportunidades que presenta el avance tecnológico en el ámbito laboral. Solo así será posible garantizar un futuro del trabajo justo, equitativo y sostenible para todos.

**Bibliografía**

Alemán Páez, Francisco, «Especialidades de las facultades de control en el trabajo a distancia. Aspectos materiales, institucionales y valorativos», en *Temas Laborales. Revista Andaluza de Trabajo y Bienestar Social*, núm. 153 (Sevilla: Junta de Andalucía, Consejería de Empleo, Formación y Trabajo Autónomo y Consejo Andaluz de Relaciones Laborales, 2020), pp. 13-60.

Cruz Villalón, Jesús, «Las facultades de control del empleador ante los cambios organizativos y tecnológicos», en *Temas Laborales. Revista Andaluza de Trabajo y Bienestar Social*, núm. 150 (Sevilla: Junta de Andalucía, Consejería de Empleo, Formación y Trabajo Autónomo y Consejo Andaluz de Relaciones Laborales, 2019), pp. 13-44.

Villa Fombuena, María, «La privacidad en el teletrabajo. Un análisis en el contexto de pandemia por covid-19», en *Temas Laborales. Revista Andaluza de Trabajo y Bienestar social*, núm. 15 (Sevilla: Junta de Andalucía, Consejería de Empleo, Formación y Trabajo Autónomo y Consejo Andaluz de Relaciones Laborales, 2021), pp. 193-213.

Warren, Samuel Denis y Louis Dembitz Brandeis, «Right to privacy», en *Harvard Law Review*, vol. IV, núm. 5 (Cambridge, MA: The Harvard Law Review Association, diciembre 15 de 1890), pp. 193-220.

CAPÍTULO III

# La relación laboral y el procesamiento de datos personales

**Stella Vanegas**
Social Partner de Vanegas Morales Consultores

## Introducción

Los datos personales y la información que compartimos y que son recopilados por diversos sistemas y plataformas tecnológicas se han convertido en uno de los activos intangibles más valiosos para empresas, gobiernos y la sociedad en general. Esta nueva era digital ha transformado la manera en que se gestionan los datos, generando una creciente y justificada preocupación por la privacidad y la protección de la información personal. En este sentido, los individuos que son titulares de los datos tienen una serie de derechos, mientras que los responsables y encargados del tratamiento de datos, es decir, las personas físicas o jurídicas, ya sean entidades públicas o privadas, que procesan y tratan esa información, tienen a su vez una serie de obligaciones con respecto a la misma que no pueden pasar por alto. Sin perjuicio de que ambos actores, es decir, titulares y entidades o personas que actúen como responsables y encargados, deban

ser vistos desde una doble perspectiva como sujetos de derechos y obligaciones.

Es importante destacar que los datos son necesarios para una amplia gama de actividades que llevamos a cabo en nuestra vida diaria, desde estudiar, viajar, trabajar, firmar un contrato, gestionar un negocio, emprender, hasta acudir al servicio de salud, entre otros. Tanto las personas titulares de estos datos como las entidades públicas o privadas encargadas de administrarlos necesitan comprender las oportunidades y los riesgos que implica su uso.

Por ejemplo, en Colombia, al igual que en la mayoría de las regulaciones vigentes en la región, existen restricciones específicas para el tratamiento de datos sensibles y de menores de edad. Estas limitaciones se establecieron para prevenir que este tipo de datos se traten con fines discriminatorios o para finalidades no razonables que puedan vulnerar la intimidad del titular sin ningún fundamento válido. En el caso de los menores, el interés del regulador ha sido garantizar que no sean objeto de tratamientos que desconozcan su edad, criterio y capacidad para entender las finalidades y el alcance del tratamiento al que puedan estar sujetos.

A medida que se ha ido adquiriendo conocimiento sobre el derecho a la protección de los datos personales y las leyes que se han promulgado en la región desde 1998, surge la necesidad de examinar el flujo de información que se produce de forma natural al establecer una relación contractual, especialmente en el ámbito laboral, que es el enfoque de este artículo.

¿Se ha preguntado alguna vez qué datos necesita el empleador para establecer el vínculo con el empleado? ¿Ha considerado las facultades que tiene un empleado en relación con el tratamiento de sus datos personales por parte del empleador? La relación

laboral entre empleado y empleador implica un significativo intercambio de información personal, desde datos básicos, como el nombre y la dirección, hasta información más sensible, como la historia clínica ocupacional y los datos de los hijos menores de edad, entre otros. En este contexto, es crucial examinar cómo se manejan y protegen estos datos en el entorno laboral, así como los derechos y responsabilidades que surgen para ambas partes: empleadores y empleados.

Para abordar esta cuestión, el texto se dividirá en las siguientes cuatro partes: primero, se realizará una síntesis de los principios relevantes del tratamiento de datos personales; segundo, se analizarán estos principios en el contexto de la relación laboral en Colombia; tercero, se ofrecerán algunas recomendaciones para incluir en el programa integral de gestión de datos personales que debe desarrollar cada entidad que procese datos personales; y, para cerrar, se presentará un análisis de dos casos relevantes relacionados con la gestión de datos personales, resumiendo lo discutido en el capítulo y destacando las principales conclusiones y sugerencias para futuras investigaciones o prácticas.

### 1. La importancia de los datos personales en el contexto actual

El tratamiento, el procesamiento y el almacenamiento de datos personales han facilitado significativamente la vida cotidiana. Un ejemplo claro es que, anteriormente, todos los trámites debían realizarse de forma presencial, mientras que ahora, gracias a la tecnología y a los factores de autenticación establecidos en los dispositivos móviles, las personas pueden interactuar con diversos servicios sin necesidad de acudir físicamente a sus instalaciones ni de presentar documentos de identidad para confirmar su

identidad. Por ejemplo, las transacciones bancarias que ahora se pueden realizar sin salir de casa, utilizando usuario, contraseña y autenticación biométrica (datos personales), solían requerir una visita presencial. Este sencillo ejemplo ilustra el valor que los datos personales tienen para cada individuo y cómo su uso adecuado o inadecuado puede afectarlos seriamente.

Considérese, por ejemplo, el papel fundamental de los datos personales en el sector público para la toma de decisiones, la implementación de políticas públicas y su seguimiento. En Colombia, se creó el Sistema de Identificación y Clasificación de Potenciales Beneficiarios de Programas Sociales (Sisbén) como un mecanismo técnico, objetivo, equitativo y uniforme para seleccionar a los beneficiarios de los gastos sociales. Este sistema consiste en «una encuesta que permite conocer las condiciones socioeconómicas de los hogares y los clasifica en función de su capacidad para generar ingresos y calidad de vida» (Departamento Nacional de Planeación, s.f., p. 3). La encuesta incluye datos personales como información sobre la vivienda, servicios públicos disponibles, antecedentes educativos, sociodemográficos, ocupacionales, ingresos, salud y fecundidad, entre otros. Estos datos los utiliza el gobierno nacional para determinar la inclusión de personas en el Sisbén, lo que pone de relieve la importancia crucial de la información personal en este proceso y su potencial impacto positivo en los beneficiarios del gasto social.

En el ámbito laboral, tanto en las entidades públicas como en las privadas, es habitual la recopilación, el procesamiento y el almacenamiento de datos personales de los trabajadores, junto con el uso de tecnología, para facilitar diversos procesos cruciales. Estos incluyen la selección y reclutamiento de personal, el monitoreo y la supervisión del desempeño laboral y la gestión integral del personal.

En la misma línea, también es necesario señalar que, en términos de transparencia, es importante procurar que la información de los empleados públicos permita generar herramientas para la rendición de cuentas sin dejar de proteger su privacidad. Esto supone un importante reto en materia de equilibrio para conseguir de manera armónica ambos fines.

El uso efectivo de los datos personales permite a una entidad pública optimizar la eficiencia operativa y mejorar la toma de decisiones estratégicas. Sin embargo, es fundamental que todas estas actividades cumplan con la normativa de protección de datos personales vigente y garanticen la intimidad y privacidad de los empleados. El cumplimiento de estas normativas no solo es una obligación legal, sino también un imperativo ético que fortalece la confianza y la seguridad dentro del entorno laboral. De esta manera, se garantiza que el manejo de la información personal se realice de manera responsable y respetuosa, protegiendo los derechos y libertades de los trabajadores.

En relación con esto, los datos personales pueden utilizarse para distintos fines asociados al desarrollo del objeto social de una empresa:

> Para unas es el bien que comercializan en desarrollo de su objeto social principal, ofreciendo a terceros el suministro de la información que reposa en sus bases de datos. Para otras, se convierte en el insumo cardinal para fijar estrategias de publicidad, emprender tácticas de fidelización de los clientes, evaluar el riesgo crediticio de las personas, prestar servicios o vender bienes ajustados a la medida del «perfil virtual» de cada cliente, etc. En el mundo laboral los datos también son la fuente para realizar

> un proceso de selección de personas para proveer un cargo. Finalmente, los datos personales son información necesaria para cumplir obligaciones legales y que por tanto deben enviarse a las autoridades y terceros para fines de, entre otras, seguridad social, impuestos, investigaciones, judiciales, etc. (Remolina, 2013, p. 23).

De este modo, en el ámbito laboral, es posible identificar aplicaciones o finalidades principales en las que los datos personales juegan un papel fundamental, las cuales no son excluyentes, son legítimas y pueden ser implementadas válidamente por los empleadores. Estas aplicaciones corresponden al uso de los datos personales en procesos de selección de personal, inclusión en beneficios o programas de bienestar, cumplimiento de deberes legales, adopción de medidas de seguridad física en las instalaciones a través de la videovigilancia, el análisis de métricas y patrones en el desempeño de los trabajadores, con mayor razón cuando se ha convertido en algo habitual que el trabajo se preste de manera híbrida o remota. Es importante destacar que estas finalidades no pretenden ser exhaustivas y que simplemente sirven como lista ilustrativa de las aplicaciones de los datos personales en el ámbito laboral.

### 2. Tensión entre los intereses del empleador y los datos personales de los empleados

A partir de lo anterior, surge naturalmente una tensión entre los intereses del empleador y los intereses del empleado en el tratamiento de los datos personales. Por un lado, el derecho a la libertad de empresa del empleador, consagrado en el artículo 333 de la Constitución Política de 1991, establece que:

> La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común [...]. La ley delimitará el alcance de la libertad económica cuando así lo exijan el interés social, el ambiente y el patrimonio cultural de la Nación.

Por lo tanto, los empleadores tienen la libertad de realizar su actividad económica dentro de los límites del bien común y conforme a las normativas vigentes, incluido el tratamiento de datos personales de sus empleados para ciertas aplicaciones.

Por otro lado, el derecho de *habeas data* está relacionado con el derecho a la intimidad y se encuentra consagrado en el artículo 15 de la Constitución Política de 1991 en los siguientes términos:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Así, los empleados tienen derecho a la protección de su intimidad y a la posibilidad de acceder, actualizar y corregir cualquier información que se tenga sobre ellos, sin importar si se encuentra en entidades públicas o privadas.

Como materialización de la tensión descrita, la Sentencia T768 de 2008 de la Corte Constitucional resolvió un caso en el que un trabajador de un banco fue despedido por un incidente captado por una cámara de vigilancia durante su hora de descanso. El trabajador

argumentó que no había autorizado la grabación y que el incidente no estaba relacionado con su desempeño laboral, sino que constituía un acto de espionaje de la entidad bancaria sobre los empleados solicitando el amparo de sus derechos a la intimidad, la dignidad humana, el debido proceso y el trabajo en condiciones dignas y justas.

En este contexto, la Corte Constitucional determinó que:

> La facultad de instalar mecanismos de vigilancia y control no puede ser ejercida de manera absoluta, aparejando una injerencia arbitraria en la esfera íntima de los trabajadores, y por tanto, en eventos en los cuales se encuentren en pugna el derecho a la intimidad del trabajador y el derecho del empleador a dirigir su actividad laboral, se deberá determinar las circunstancias específicas del caso en concreto, para ponderar los mismos en razón de la finalidad, proporcionalidad, necesidad e idoneidad de la medida, y por tanto determinar su razonabilidad, que deben encontrarse fundamentadas según el desarrollo inherente de la relación laboral (Sentencia T768, 2008).

Por fuera del debate laboral sobre la legitimidad o ilegitimidad que tenía el empleador para desvincular al trabajador, este caso ilustra cómo el derecho a la libertad de empresa del empleador y el derecho a la intimidad del empleado pueden entrar en conflicto. Por un lado, los empleadores necesitan vigilar sus instalaciones para garantizar la seguridad y la eficiencia en el lugar de trabajo, monitorizando áreas con cámaras de videovigilancia. Por otro lado, aunque los empleados están sujetos a supervisión durante el trabajo, esta no debe extenderse a su esfera íntima, ni a espacios personales, como áreas de descanso, baños o vestuarios.

Finalmente, esta situación invita a reflexionar sobre aspectos clave como el objetivo, la proporcionalidad, la necesidad y la idoneidad de las medidas adoptadas. Siempre será fundamental considerar si existen alternativas menos intrusivas para alcanzar los mismos fines legítimos, minimizar los posibles perjuicios y asegurar que las medidas no constituyan tratos inhumanos, degradantes o que afecten de manera irrazonable o ilegítima a la intimidad de las personas. En este escenario, donde deben ponderarse los derechos en juego, una vez se tiene la certeza de que las acciones a implementar responden a la necesidad legítima de la empresa y se ha realizado la ponderación adecuada entre esta y los derechos del empleado, debe facilitarse el paso a la aplicación del principio de transparencia. Esto implica informar adecuadamente a los empleados y, cuando sea necesario, obtener previamente su consentimiento para el tratamiento de sus datos personales en el contexto planteado. Este tema se desarrollará con mayor profundidad en las siguientes secciones de este artículo.

### 3. Generalidades de la protección de datos personales en Colombia

Hablar de principios en la protección de datos personales, tanto en Colombia como en el mundo, implica reconocer que estas normativas, destinadas a desarrollar derechos fundamentales como el derecho al *habeas data*, están diseñadas para adaptarse a entornos que evolucionan con mucha rapidez. Su objetivo es proporcionar elementos que orienten de manera continua a los sujetos receptores de estas normas y faciliten el cumplimiento, al brindar claridad sobre los pilares que deben respetarse a lo largo del procesamiento de la información personal.

En Colombia, existen dos leyes de protección de datos personales: la primera es la Ley Sectorial 1266 de 2008, que regula el *habeas data* financiero, y la segunda es la Ley General de Protección de Datos, conocida como la Ley 1581 de 2012. Esta última, en su artículo 4, establece los principios que deben regir el tratamiento de datos, los cuales deben complementarse con los establecidos por la Corte Constitucional en la Sentencia C-748 de 2011. En este artículo, nos centraremos en aquellos principios que, en nuestra opinión, tienen mayor relevancia para el tratamiento de datos en una relación laboral.

En primer lugar, el principio de libertad, consagrado en el literal c) del artículo 4 de la Ley General, estipula que «el tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán obtenerse o divulgarse sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento». La Sentencia C-748 de 2011 de la Corte Constitucional estableció que este principio es fundamental en la administración de datos, ya que permite al titular decidir de manera voluntaria si desea que su información pueda ser objeto de tratamiento. Asimismo, este principio limita el tratamiento de datos personales únicamente a los casos en los que se cuente con la aquiescencia del titular, o en los que se cumpla con un mandato legal o judicial que releve la necesidad de dicha aprobación.

Partiendo del hecho de que hasta la fecha el consentimiento es la única base legítima para el tratamiento de datos, a menos que exista un mandato legal o judicial que lo releve, es crucial considerar el artículo 10 de la Ley General, que enumera los casos en los que no se requiere la autorización del titular para el tratamiento de sus datos personales: (i) cuando la información es solicitada

por una entidad pública o administrativa en el ejercicio de sus funciones legales o por orden judicial; (ii) cuando los datos son de naturaleza pública; (iii) en casos de urgencia médica o sanitaria; (iv) cuando el tratamiento de la información está autorizado por ley para fines históricos, estadísticos o científicos; y (v) cuando se trate de datos relacionados con el registro civil de las personas.

Una vez mencionadas las excepciones al consentimiento establecidas por la Ley General, se observa que en las relaciones laborales ordinarias es poco frecuente que los empleadores se encuentren en alguna de dichas situaciones excepcionales. Por lo tanto, como norma general, los empleadores deben obtener la autorización de sus empleados para tratar sus datos personales.

Esta situación es característica de los países cuyas regulaciones no contemplan otras bases legítimas para el tratamiento, y suele corresponder a regulaciones anteriores a la entrada en vigor del Reglamento General de Protección de Datos de la Unión Europea (RGPD). Colombia es uno de estos países y actualmente está revisando su ley, un trámite legislativo que esperamos produzca resultados en el futuro cercano.

Como se mencionó al principio de esta sección, en Colombia la autorización para el tratamiento de datos personales debe cumplir con los requisitos de ser previa, expresa e informada. En cuanto al carácter previo, la autorización debe ser otorgada por el titular antes de la recolección de los datos o, a más tardar, en ese momento. En relación con el carácter expreso, la autorización debe reflejar la voluntad libre del titular, ser inequívoca, explícita, concreta y no tácita, de modo que su silencio no pueda interpretarse como una forma de aquiescencia para el tratamiento de su información. Por último, en relación con el carácter informado, el titular debe

aceptar el tratamiento de sus datos y ser plenamente consciente de los efectos de su autorización (Resolución 68753 de 2023).

En segundo lugar, el principio de finalidad, establecido en el apartado b) del artículo 4 de la Ley General, establece que «el tratamiento de datos personales debe tener una finalidad legítima de acuerdo con la Constitución o la ley». Esta finalidad debe ser comunicada al titular antes de que otorgue su autorización, o simultáneamente con este acto. La Corte Constitucional, en la Sentencia C-748 de 2011, aclaró que este principio debe entenderse atendiendo a dos aspectos fundamentales: en primer lugar, bajo el principio de necesidad, los datos deben conservarse durante un período no superior al necesario para los fines para los que fueron recopilados. Esto implica que toda finalidad tiene un término y, una vez vencido, se debe cesar en el tratamiento. En segundo lugar, los datos deben ser estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos, prohibiéndose el tratamiento de datos que no estén estrechamente relacionados con el objetivo de la misma. En este sentido, está claro que cuando una entidad requiera datos personales, se debe limitar el procesamiento de datos al mínimo necesario y solo deben tratarse los datos adecuados, pertinentes y acordes con las finalidades para las que se previeron.

En términos prácticos, solamente se deben solicitar y obtener aquellos datos necesarios para desarrollar la relación contractual, cumplir con los deberes que como empleados tienen aquellas personas que desempeñen funciones asociadas al procesamiento de datos y permitir a la empresa conocer, medir y tener trazabilidad de la ejecución de las labores encomendadas a los empleados, así como proteger la seguridad y la confidencialidad de la información.

En relación con lo anterior, el literal c) del artículo 17 de la Ley General establece como un deber fundamental de los responsables del tratamiento de datos «informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada». Además, el artículo 12 de la misma ley establece que el responsable debe informar al titular sobre los siguientes aspectos: el tratamiento al que se someterán sus datos personales y la finalidad del mismo, el carácter facultativo de la respuesta a las preguntas que le sean hechas cuando estas versen sobre datos sensibles, los derechos que le asisten como titular y la identificación, dirección física o electrónica y teléfono del responsable del tratamiento. Por lo tanto, entre otras cosas, el responsable debe informar al titular sobre el tratamiento al que se someterán sus datos, la finalidad del mismo, los derechos que le asisten y debe actuar en concordancia con esta finalidad y autorización, evitando extralimitarse o realizar un tratamiento diferente a las finalidades informadas.

Por último, el principio de transparencia, regulado en el literal e) del artículo 4 de la Ley General, dispone que «en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan». Este principio consagra el derecho que tiene cualquier titular a solicitar información a un responsable o encargado sobre sus datos personales. De acuerdo con la Sentencia C-748 de 2011, los responsables o encargados deben suministrar, como mínimo, la siguiente información: datos sobre la identidad del controlador de datos, el propósito del procesamiento de los datos personales, qué datos se podrán revelar, cómo

la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos y toda otra información necesaria para el procesamiento justo de los datos.

En relación con lo anterior, el literal k) del artículo 17 de la Ley 1581 de 2012 establece como deber de los responsables del tratamiento «adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos». Del mismo modo, el artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015 dispone que los responsables deben elaborar políticas para el tratamiento de los datos personales, implementarlas en formato físico o electrónico, en un lenguaje claro y sencillo, y ponerlas en conocimiento de los titulares. Estas políticas deben contener, como mínimo, la siguiente información:

- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable.
- Tratamiento al que se someterán los datos y su finalidad.
- Derechos que le asisten al titular.
- Persona o área responsable de la atención de peticiones, consultas, reclamaciones y ante la cual el titular puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato, así como revocar la autorización.
- Procedimiento para que los titulares de la información puedan ejercer los derechos anteriormente mencionados.
- Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

Tras revisar el alcance de los tres principios mencionados anteriormente, se crea el ambiente propicio para reflexionar sobre la aplicación de estos principios en la realidad del contexto labo-

ral y preguntarse, en función de su rol, si ese contexto laboral ha desarrollado las herramientas que le permitan cumplir efectivamente con ellos como empleador o si, invirtiendo el punto de vista, el empleado ha recibido esta información y ha entendido las razones por las cuales ha de suministrar sus datos personales.

Considerando el principio de libertad, surgen interrogantes respecto a ambos roles:

Como empleador:

- ¿Ha analizado el tipo de datos que necesita recopilar?
- ¿Tiene claridad sobre la pertinencia de las finalidades?
- ¿Ha previsto mecanismos adicionales al formato de autorización para comunicar y explicar al empleado la relevancia de la solicitud de los datos requeridos?
- ¿Ha establecido un canal eficiente que permita resolver las dudas o inquietudes que puedan tener los empleados respecto de la información que está siendo tratada o que se busca tratar?

Como empleado:

- ¿Qué acciones considera que le permitirían tener un mejor conocimiento sobre el tratamiento de sus datos?
- ¿Qué mecanismos le facilitarían entender su autorización?
- ¿Conoce la importancia de cumplir con los deberes que establece la ley de protección de datos cuando usted debe tratarlos?
- ¿En qué casos considera que, en la relación laboral, el empleado tendría la capacidad de elegir libremente si desea que su información pueda ser o no objeto de tratamiento?

En respuesta, es posible que el empleado se sienta implícitamente obligado a proporcionar todos los datos personales que le

solicite o requiera el empleador debido a la naturaleza de la relación laboral y a la asimetría de poder existente. Esta dinámica puede dar lugar a una situación en la que el empleado sienta que no tiene verdadera opción para negarse a proporcionar ciertos datos, por miedo a posibles represalias o consecuencias negativas en su contratación o empleo.

Para disipar esta preocupación del empleado, es importante aplicar el principio de transparencia establecido en el literal e) del artículo 4 de la Ley General en los siguientes términos. El uso de un lenguaje sencillo y preciso fortalece la relación de confianza y contribuye a evitar malas interpretaciones por parte de los empleados.

Otro elemento a considerar es que, en el desarrollo de una relación laboral, los empleadores deben poder llevar a cabo todos los tratamientos derivados de esta, lo cual les obliga a anticiparse y dejar cubiertos los escenarios posibles. Si durante la relación laboral surge la necesidad de aplicar nuevos tratamientos, se puede actualizar la autorización u obtener autorizaciones individuales para los nuevos fines. Dada esta casuística y la realidad de que algunos datos son necesarios para las finalidades imprescindibles de una relación laboral, es necesario debatir si en la relación laboral debería tratarse datos personales de los empleados exclusivamente basados en su autorización o si podría implementarse otra base legitimadora que tenga en cuenta los derechos y deberes tanto del empleador como del empleado, como bien sería el desarrollo de una relación contractual, establecida en el artículo 6 del Reglamento General de Protección de Datos (RGPD).

Ahora bien, considerando los principios de finalidad y transparencia, es pertinente reflexionar sobre los siguientes puntos:

- ¿Cómo comunicar de manera suficiente y oportuna al empleado las finalidades que se persiguen con la recolección de sus datos personales?
- ¿Qué análisis realizó el empleador para determinar la necesidad y la razonabilidad de la información solicitada?
- Los empleados, como titulares de los datos, ¿dónde pueden informarse y formarse para entender mejor las razones de la recolección y el procesamiento?

Las relaciones laborales deben fomentar la existencia de confianza y cooperación; ambas partes están llamadas a informarse mejor y a hacer más comprensible lo que sucede con los datos personales. Un programa de gestión de datos personales debe considerar al grupo de empleados como uno de sus principales grupos de interés, y los empleados deben esforzarse por informarse y colaborar ante solicitudes razonables de información. Además, tienen derecho a preguntar y a solicitar explicaciones cuando los tratamientos y/o las finalidades puedan resultar excesivos o improvisados.

#### 4. Datos sensibles

Probablemente, usted, como lector, ya haya anticipado que existen varios tipos de datos personales y que no todos deben ser custodiados o tratados de la misma forma. A este respecto, tanto la Ley Sectorial como la Ley General prevén las siguientes categorías de datos:

- Dato personal: cualquier información vinculada a una o más personas físicas o jurídicas determinadas o determinables.
- Dato público: aquel que califica como tal la ley o la

Constitución política y que no sea semiprivado o privado. Por ejemplo, las sentencias judiciales debidamente ejecutoriadas o el estado civil de las personas.

- Dato semiprivado: aquel que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar al titular y a otro grupo de personas o a la sociedad en general. Por ejemplo, los datos financieros y crediticios de actividad comercial.
- Dato privado: aquel que, por su naturaleza íntima o reservada, solo es relevante para el titular. Por ejemplo, la historia clínica.
- Dato sensible: aquel que afecta a la intimidad del titular o cuyo uso indebido puede generar discriminación. Por ejemplo, la pertenencia a sindicatos, los datos relativos a la salud y los datos biométricos. También forman parte de esta categoría los datos de los menores de edad.

Como se puede inferir, en una relación de carácter laboral hay lugar para conocer y tratar datos de diferente naturaleza. En países como Colombia, donde la única base legal para el procesamiento de datos es el consentimiento, es necesario obtener la autorización del titular de manera previa, expresa e informada. Si se trata de datos sensibles, dicha aprobación debe ser explícita y se debe indicar que no se está obligado a suministrarlos, dado el carácter facultativo que establece la ley.

El tratamiento de datos sensibles se puede realizar cuando el titular haya dado su autorización explícita, cuando sea necesario para salvaguardar el interés vital del titular, cuando el tratamiento se realice en el curso de actividades legítimas por parte de una fundación, ONG, asociación u otro organismo sin ánimo de lucro

(como una asociación sindical), cuando se refiera a datos necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y cuando el tratamiento tenga una finalidad histórica, estadística o científica (Ley 1581, 2012, artículo 6).

Sin embargo, la pandemia del COVID-19 volvió a poner de manifiesto la tensión entre los intereses de los empleados y los empleadores en lo que respecta al tratamiento de datos sensibles y la salud pública. Es importante recordar que, ante el brote de esta pandemia, se implementaron diversas medidas para hacerle frente, entre las que se destaca la vacunación contra el COVID-19. La vacunación de una persona se considera un dato relacionado con su estado de salud y, por tanto, un dato sensible sujeto a protección.

En este contexto, surge la pregunta: ¿podría el empleador requerir de manera obligatoria la aplicación de la vacuna? ¿Sería válido solicitar la información sobre la vacunación de sus empleados en la medida en que fuese necesaria para salvaguardar la salud de los demás trabajadores? Para responder a estas preguntas, cabe recordar que la vacunación es libre y voluntaria, y los ciudadanos pueden disentir y no aceptarla, tal y como establece el literal d) del artículo 10 de la Ley 1751 de 2015 en los siguientes términos: «Ninguna persona podrá ser obligada, contra su voluntad, a recibir un tratamiento de salud».

Por lo tanto, según nuestro criterio, no es posible obligar a los empleados a vacunarse contra el coronavirus. Sin embargo, como medida para hacer frente a una negativa, se podría generar un entorno que proteja a los empleados que sí han consentido en ser vacunados. Si se generan espacios específicos para unos y otros, no se podrá considerar una acción discriminatoria, ya que, ante la tensión entre derechos fundamentales, hay que hacer un adecua-

do juicio de ponderación que permita cumplir de manera razonable con la protección demandada por ambos.

Ahora bien, frente a la necesidad de obtener información sobre la fecha y el lugar de la vacunación, la respuesta se encuentra en el artículo 10 de la Ley General, según el cual no se requiere la autorización del titular para el tratamiento de sus datos personales cuando se trate de casos de urgencia médica o sanitaria. Por lo tanto, el empleador sí puede requerir información sobre la vacunación de sus empleados para salvaguardar la salud de los demás trabajadores. Esto no impide que, en el ejercicio de esta excepción, el empleador, aunque no requiera la autorización de su empleado para tratar esta información, deba cumplir con los demás principios y deberes establecidos en la norma, de tal manera que debe conservarla bajo condiciones de confidencialidad y seguridad, garantizando la reserva de la información en todo momento. Un mal uso de estos datos podría generar condiciones de discriminación o malos tratos para los empleados que decidieron no vacunarse.

### 5. Recomendaciones frente al PIGDP

A continuación, se presentarán una serie de recomendaciones prácticas que pueden ayudar a los empleadores en la construcción y la revisión del Programa Integral de Gestión de Datos Personales (PIGDP). Para garantizar un adecuado tratamiento de los datos personales en el entorno laboral, es fundamental seguir una serie de medidas que cumplan con la normativa y protejan la privacidad de la información.

En primer lugar, es fundamental que todas las entidades, tanto públicas como privadas, que manejen información personal en sus procesos de gestión de recursos humanos inclu-

yan procedimientos claros en sus manuales internos. Estos procedimientos deben abordar desde la vinculación inicial de los empleados hasta aspectos como la contratación a través de agencias temporales o la obtención de datos de portales de empleo en línea.

En segundo lugar, se deben identificar y asignar roles específicos para el cumplimiento de estas normativas, junto con la implementación de controles efectivos para preservar la integridad y confidencialidad de los datos.

En tercer lugar, es fundamental establecer un proceso robusto para la atención de consultas y reclamaciones, de modo que los colaboradores se sientan respaldados en el ejercicio de sus derechos sobre sus datos personales.

Es necesario incorporar programas de capacitación continua para el personal en relación con sus derechos y responsabilidades en materia de protección de datos. Está comprobado que la inversión en la formación de los empleados produce resultados positivos y beneficios tangibles para los empleadores. Es especialmente importante diseñar entrenamientos y campañas que respondan a las necesidades específicas de cada área. Las áreas encargadas de diseñar productos y servicios, generar estrategias de recolección de datos o establecer los canales para ello deben ser las primeras en recibir este entrenamiento, junto con las áreas que procesan datos sensibles y de menores de edad. También es fundamental incluir a las áreas que atienden peticiones, quejas y reclamaciones, ya que deben estar preparadas para explicar claramente las finalidades de la recolección y las políticas de tratamiento de datos a los empleados y a los candidatos que formen parte de los procesos de selección.

Este enfoque proactivo no solo contribuye al cumplimiento de la normativa, sino que también fortalece la confianza y el compromiso entre la empresa y su equipo humano.

### 6. Casos relevantes

A continuación, se destacarán dos casos relevantes relacionados con el tratamiento de datos sensibles y el cumplimiento de deberes por parte de los empleadores. El caso descrito en la Resolución 18848 de 2019 trata de una pareja de esposos que contrataron a un fotógrafo para que tomara fotos de su evento. Posteriormente, el hotel utilizó estas fotografías con fines publicitarios sin la debida autorización de la pareja.

Ante estos hechos, el hotel argumentó que el fotógrafo no tenía ningún vínculo contractual con él y les compartió las imágenes bajo una autorización de cesión de uso de propiedad intelectual en la que el fotógrafo se comprometía a asumir toda la responsabilidad y a salir en defensa del hotel ante un reclamo de un tercero por derechos de autor. Asimismo, el hotel argumentó que no tenía la calidad de responsable y que había compartido las imágenes con una revista para su publicación, confiando en que el fotógrafo había obtenido la autorización por parte de los esposos.

Sin embargo, el hotel, a pesar de no tener un vínculo contractual con el fotógrafo, omitió obtener la autorización previa, expresa e informada de los titulares para el tratamiento de sus datos personales. El tratamiento en cuestión consistió en el uso y entrega de las fotografías a una revista para su publicación en un anuncio publicitario.

La autoridad colombiana de protección de datos personales (Superintendencia de Industria y Comercio, SIC) indicó que la

autorización de cesión de derechos de propiedad intelectual no recae sobre el tratamiento de datos personales y no es aplicable. Igualmente, tanto el fotógrafo como el hotel tuvieron la condición de responsables del tratamiento en distintos momentos, ya que ambos definieron el uso que se le dio a las fotografías y las finalidades de esos usos.

Finalmente, se debe destacar que las fotografías en las que aparece el rostro o el cuerpo completo de una persona se consideran datos personales, dado que pueden asociarse con una persona determinada o determinable. Sin embargo, en este caso, las fotografías no se pueden clasificar como datos biométricos, ya que no se han procesado con medios técnicos que posibiliten la identificación o autenticación unívoca de sus titulares.

En las relaciones laborales, es posible que se traten datos que fueron recolectados por otra empresa o por un tercero. Sin embargo, los empleadores sí pueden ser responsables del tratamiento de estos datos, por lo que siempre deben cumplir con los deberes correspondientes y asegurarse de contar con la autorización de los titulares para su tratamiento. Asimismo, se resalta la importancia de comunicar las finalidades a los titulares y de no extralimitarse ni realizar tratamientos fuera de lo autorizado. Por ejemplo, como empleador, si contrato a una persona, no puedo utilizar sus datos con fines comerciales a menos que le comunique esta finalidad.

La Resolución 101695 de 2015 describe el caso de un ciudadano que manifestó su interés en participar en un proceso de selección para un puesto de trabajo en una empresa, enviando su currículum al correo que esta había habilitado. Sin embargo, tras pasar varios días, el solicitante no recibió ninguna respues-

ta por parte de la empresa respecto a su proceso de selección. Por lo tanto, decidió consultar el estado de su trámite, bajo el entendido de que la empresa es responsable del tratamiento de sus datos personales al recoger su currículum. En esta misma solicitud, el ciudadano preguntó sobre el tratamiento de sus datos personales para este proceso, pero no recibió respuesta hasta cuatro meses después.

Ante estos hechos, la SIC investigó a la empresa por dos cargos. En primer lugar, porque la empresa no contaba con la autorización previa, expresa e informada del titular para el procesamiento de sus datos personales. Como se anticipó previamente, conforme al principio de libertad, los datos no pueden ser obtenidos sin la autorización previa, expresa e informada del titular. En este sentido, la Corte Constitucional, en la Sentencia C-748 de 2011, estableció que no está permitido el consentimiento tácito del titular del dato y que nunca se podrá inferir el silencio del titular como una autorización para el uso de su información. En el mismo sentido, indicó que dentro de este principio se entiende la posibilidad de retirar el consentimiento y de limitar el plazo de su validez por parte del titular.

En este análisis, la SIC también hizo hincapié en la importancia de que los titulares comprendan de manera clara, suficiente y previa las finalidades de la información proporcionada, así como de los efectos de su autorización (Sentencia C-748 de 2011). Por lo tanto, para garantizar el principio de libertad, las empresas deben informar sobre las condiciones en las que se llevará a cabo el tratamiento de los datos. Además, la SIC reprocha en este caso la falta de información previa, explícita, precisa e inequívoca al titular sobre las finalidades de la recolección, sus derechos como titular, quién

posee su información y dónde puede ejercer esos derechos. Es importante recordar que, de acuerdo con el artículo 2.2.2.25.2.2 del Decreto 1074 de 2015, el responsable debe solicitar la autorización del titular para el tratamiento de los datos, a más tardar en el momento de la recolección de estos, e informarle sobre las finalidades específicas del tratamiento de su información.

La SIC reprueba que no se le informara al titular de manera expresa, clara, previa e inequívoca sobre el tratamiento al que se someterían sus datos, las finalidades, sus derechos y la identificación del responsable. Por ello, se concluye que el consentimiento del titular no fue informado, lo cual debió cumplir la empresa a más tardar en el momento en que recolectó la información.

En segundo lugar, la SIC investigó a la empresa por incumplir su deber de informarle sobre el uso que ha hecho de sus datos personales. En relación con ello, la empresa respondió a la consulta del titular cuatro meses después de presentarla, indicándole que no había sido preseleccionado. Es importante recordar que el derecho de *habeas data* permite a cualquier persona conocer, actualizar y rectificar la información que se tiene de sí misma en una base de datos. Con este propósito, el artículo 14 de la Ley General estipula que las consultas deben atenderse en un plazo máximo de diez días hábiles contados a partir de su presentación. En caso de necesitar más tiempo, se debe informar al titular sobre la razón de la demora y la fecha en que se resolverá su consulta, la cual no puede superar los cinco días hábiles siguientes al vencimiento del primer plazo. Por lo tanto, aunque la empresa respondió de manera clara, precisa y detallada a la consulta del titular, lo hizo fuera del plazo establecido por la ley para los responsables del tratamiento.

No obstante, la empresa apeló esta decisión y, en la Resolución 1908 de 2017, al reevaluar el caso, la SIC determinó que el hecho de que el mismo titular remitiera su hoja de vida para el proceso de selección habilitaba a la empresa para usar la información del titular con esta finalidad, lo cual constituía una conducta que demostraba su interés en participar en el proceso de selección de manera libre y voluntaria. También indicó que se había cumplido parcialmente el deber de informar al titular sobre las finalidades de la recolección de sus datos y los derechos que le asistían, ya que su aplicación se había realizado a través de una plataforma. Al enviar su currículum a la empresa, el titular sabía que lo hacía para participar en un proceso de selección para un puesto de trabajo y el tratamiento que se le iba a dar a su currículum vitae. Sin embargo, no se podían inferir de esta situación los derechos que le asisten a los titulares ni la política de tratamiento de datos por los que se rige. Por lo tanto, se concluye que existe un incumplimiento parcial frente al deber de informar al titular sobre la finalidad y los derechos que le asisten. La resolución también confirma el incumplimiento por parte de la empresa de contestar las consultas, peticiones y reclamaciones dentro del plazo establecido.

Este caso ilustra la importancia que tiene para los empleadores cumplir con sus deberes como responsables, entre otros: (i) informar al titular sobre el tratamiento al que se someterán los datos y las finalidades de la recolección; (ii) atender de manera oportuna las peticiones, quejas y reclamos; (iii) definir procesos de retención de datos; (iv) aportar la mayor claridad posible sobre los fines del tratamiento y los canales ante los cuales pueden elevar sus consultas y reclamos.

Lo anterior se aplica no solo a los datos de los aspirantes, como en este caso, sino también a la recopilación de datos personales de empleados, proveedores, colaboradores, accionistas, clientes y demás personas relacionadas con la empresa.

**7. Conclusiones**

Es esencial que tanto empleados como empleadores estén plenamente conscientes de sus derechos y obligaciones en relación con los datos personales. Por un lado, aunque los empleados puedan ser considerados la parte más vulnerable de la relación laboral, esto no implica que estén desprovistos de protección legal ni que puedan ser objeto de tratamientos que infrinjan la ley. Por otro lado, los empleadores, en su papel de responsables del tratamiento de datos y al ser considerados la parte más fuerte de la relación laboral, tienen el deber de cumplir con todas las obligaciones y principios establecidos para garantizar un tratamiento adecuado de esta información. El objetivo debe ser cumplir no solo formalmente, sino también de manera sustantiva. El área de recursos humanos debe organizar el trabajo para identificar qué finalidades y con qué alcance se deben cumplir según las funciones, el tipo de procesos, la ubicación de los empleados, su movilidad, la posibilidad de compartir la información con entidades vinculadas, la naturaleza de los datos y el grado de impacto que puede tener el tratamiento en la intimidad de las personas, entre otros.

En este sentido, es importante destacar el principio de libertad y la facultad que tienen los titulares de autorizar de manera previa, expresa e informada el tratamiento de sus datos personales o de optar por no autorizarlo. Asimismo, se debe tener en cuenta que, en Colombia, los empleadores no suelen estar amparados

por las excepciones establecidas en la Ley General de Protección de Datos y, por lo tanto, deben obtener siempre autorización para realizar cualquier tipo de tratamiento. Además, es indispensable que los empleadores cumplan con el principio de finalidad e informen a los empleados sobre las finalidades para las que serán tratados sus datos y que recojan únicamente los datos necesarios y adecuados para cumplir con dicha finalidad.

Por su parte, los casos relevantes destacan la importancia de que los empleadores cumplan con sus obligaciones como responsables del tratamiento de datos, incluyendo la recopilación de datos personales de aspirantes, proveedores, colaboradores, accionistas, clientes y otras personas relacionadas con la empresa. Los casos destacan la importancia de responder a las consultas dentro de los plazos establecidos por la ley y de garantizar el ejercicio efectivo del derecho de *habeas data* en todo momento.

Aunque no ha sido tema de este capítulo y seguramente podremos abordar el tema en una futura entrega, los empleadores deben fomentar una cultura sólida de prevención de incidentes y protección de datos personales dentro de sus organizaciones. Esto no solo beneficia a las empresas al cuidar los datos de sus empleados, sino que también contribuye a proteger los datos de todas las personas que se relacionen con la empresa. Es crucial seguir avanzando en el desarrollo e implementación de herramientas que promuevan la seguridad de la información.

Por último, es importante considerar cómo debería regularse el uso de la inteligencia artificial en las empresas, asegurando que se utilice de manera segura y que no se exponga información confidencial de la compañía ni se asuman riesgos innecesarios, sino que se generen los elementos de gobernanza que hagan de

su uso una práctica que promueva la eficiencia empresarial y el respeto a los derechos humanos.

**Bibliografía**


Congreso de la República de Colombia, *Ley 1266 de 2008* (expedida el 31 de diciembre de 2008). Recuperada de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

----------, *Ley 1581 de 2012* (expedida el 17 de octubre de 2012). Recuperada de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

----------, *Ley 1751 de 2015* (expedida el 16 de febrero de 2015). Recuperada de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1751_2015.html

Constitución Política de Colombia [C.P.] (expedida en 1991). Artículo 15 [Título II]. (49ª ed.). Legis.

----------, Artículo 333 [Título XII]. (49ª ed.). Legis.

Corte Constitucional, Sala Novena de Revisión, *Sentencia T768 de 2008* (La magistrada ponente fue Clara Inés Vargas Hernández y se aprobó el 31 de julio de 2008).

Corte Constitucional, Sala Plena, *Sentencia C-748 de 2011* (El magistrado ponente fue Jorge Ignacio Pretelt Chaljub y se aprobó el 6 de octubre de 2011).

Departamento Nacional de Planeación, *Abecé* (Bogotá: Departamento Nacional de Planeación, s. f.). Recuperado de: https://colaboracion.dnp.gov.co/CDT/Prensa/Sisben-Abece.pdf

Parlamento Europeo, *General Data Protection Regulation de 2016* (expedida el 27 de abril de 2016). Recuperada de: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Presidencia de la República de Colombia, *Decreto Único Reglamentario 1074 de 2015* (Expedido el 26 de mayo de 2015). Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608

Remolina Angarita, Nelson, «Tratamiento de datos personales en el contexto laboral», en *Revista Actualidad Laboral*, núm. 175 (Bogotá: Editorial Legis, 2013), pp. 1924. Recuperado de https://xperta.legis.co/visor/rlaboral/rlaboral_d6cac6ef1ad80028e0430a0101510028

Superintendencia de Industria y Comercio, *Resolución 101695 de 2015* (expedida el 28 de diciembre de 2015).

----------, *Resolución 18848 de 2019* (expedida el 31 de mayo de 2019).

----------, *Resolución 1908 de 2017* (expedida el 24 de enero de 2017).

----------, *Resolución 68753 de 2023* (expedida el 1 de noviembre de 2023).

----------, *Los datos personales y la propiedad industrial*. Recuperado de https://www.sic.gov.co/content/los-datos-personales-y-la-propiedad-industrial#:~:text=¿Qué%20son%20los%20datos%20biométricos,datos%20sensibles%20de%20la%20persona.

CAPÍTULO IV

# Protección de la intimidad en el trabajo y negociación colectiva

**Gilberth Díaz Vásquez**
Dirigente sindical del Magisterio Nacional de Costa Rica

> El hecho de que […] al empresario le son atribuibles los poderes de control y vigilancia con el fin principal de alcanzar los objetivos de la organización, no lo facultan para accesar indiscriminadamente el correo electrónico de los trabajadores […] Las potestades o poderes de los empresarios subsisten, siempre y cuando no se limiten o restrinjan los derechos de los dependientes […] Cabe reiterar que los derechos a la intimidad, al secreto de las comunicaciones y a la autodeterminación informática son derechos inherentes a la persona del trabajador, a quien se le han de garantizar esos derechos, independientemente de que se desenvuelva dentro de la esfera personal o laboral. Se trata de derechos personalísimos, los cuales no se le pueden tutelar a la persona en su vida privada y ser excluidos dentro del ámbito laboral. Es inaceptable que, cuando el trabajador se desenvuelve en la empresa, no tenga garantizados los derechos a la intimidad y al secreto de las comunicaciones y que con o sin su consentimiento el empresario pueda accesar a su correo electrónico (Garro y Meseguer, 2004).

> Artículo 4: Deberán adoptarse medidas adecuadas a las condiciones nacionales, cuando ello sea necesario, para estimular y fomentar entre los empleadores y las organizaciones de empleadores, por una parte, y las organizaciones de trabajadores, por otra, el pleno desarrollo y uso de procedimientos de negociación voluntaria, con objeto de reglamentar, por medio de contratos colectivos, las condiciones de empleo (OIT, Convenio sobre el Derecho de Sindicación y de Negociación Colectiva, 1949, núm. 98).

## Introducción

Como se establece en la Constitución Política de Costa Rica, en la jurisprudencia de la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica y en el Código de Trabajo de este país, tanto el derecho a la intimidad de las personas trabajadoras como el poder de dirección y control del empleador

son derechos y libertades fundamentales reconocidos constitucionalmente, así como en las convenciones regionales comunes a todos los países de la región latinoamericana. Estos derechos de las personas trabajadoras y de los empresarios también han sido reconocidos por la Corte Interamericana de Derechos Humanos, de modo que no existen dudas ni sobre su vigencia como derechos y libertades fundamentales en América Latina ni sobre su valor normativo al más alto nivel jurídico. Sin embargo, surge una tensión insalvable cuando estos derechos —de idéntica jerarquía y resistencia— se enfrentan en el ámbito laboral de la empresa o en la relación contractual del contrato de trabajo.

Hasta la fecha, en Costa Rica, al igual que en la mayoría de los países de la región, los empleadores ejercen su facultad de dirección y control del trabajo y de la persona trabajadora como un poder absoluto, derivado del poder de dirección empresarial. Este poder está respaldado por la legislación laboral y el contrato de trabajo, los cuales establecen el elemento de subordinación jurídica al que está sujeta la persona trabajadora. Esta situación solo se atenúa por la jurisprudencia emitida por los órganos de la jurisdicción laboral.[1]

---

[1] Ver por ejemplo un caso que, ante la falta de normativa regulatoria, fue resuelto por la Sala Segunda de Casación Laboral. Sentencia n.º 00172-2011 de las 11:05 horas del 18 de febrero del 2011: «… DESPIDO INJUSTIFICADO POR PÉRDIDA DE CONFIANZA. GRABACIÓN DE CONVERSACIONES TELEFÓNICAS Y DERECHO A LA INTIMIDAD. PRUEBA OBTENIDA DE MANERA ILEGAL. Con respecto al derecho a la intimidad se cita el voto de la Sala Segunda núm. 124-10 y el voto de la Sala Constitucional núm. 6552-03. El empleador tiene la potestad de vigilar y comprobar el fiel desempeño de las labores pactadas por medio del contrato de trabajo. No obstante, ese poder debe ejercerse de manera afín con las garantías fundamentales del empleado, de modo que los sistemas de monitoreo aplicados deben estar originados en una nece-

Por el contrario, los trabajadores y las trabajadoras tienen muy poca capacidad para oponerse a este tipo de control y defender su derecho —también fundamental— a la intimidad y la privacidad. Esta situación es aún más evidente en países como Costa Rica, donde la afiliación sindical es muy baja y escasa la negociación colectiva, lo que deja al poder del empleador sin oposición por parte de una fuerza organizada de sus trabajadores.[2]

Además del aspecto de fuerza y poder dentro de la empresa, existe un elemento histórico que respalda el reconocimiento de amplias facultades de control empresarial en el ámbito laboral. Como señala el juez costarricense Fabián Arrieta Segleau: «Históricamente se ha

---

sidad objetiva y ser proporcionales con el fin para el que están dispuestos. Ello con el objeto de descartar que se conviertan en un ambiente de acoso, que amenace con coartar el derecho de intimidad. Se indicó que la actora fue despedida por pérdida de confianza, por irrespeto en el uso de las herramientas de la empresa y el abuso en la forma de emplear el tiempo laboral, que utilizaba para hacer comentarios que deterioraban las relaciones interpersonales con sus compañeros. Como prueba se aportaron las grabaciones de sus conversaciones telefónicas. Sin embargo, consta que la empresa no tenía ningún interés real y objetivo que justificara esas grabaciones, pues la actora no fungía como operadora del servicio de *call center* que esa compañía daba, y no consta que hubiera habido advertencia alguna en ese sentido. Así, ese monitoreo no solo constituyó un ejercicio abusivo de la potestad de control y dirección de la empleadora, sino también un flagrante quebrantamiento del derecho de intimidad de la actora…».

[2] Sobre el modelo de representación laboral colectiva en Costa Rica, Mauricio Castro Méndez señala: «…la tasa de sindicalización es baja y los sindicatos son sistemáticamente sustituidos por órganos unitarios no sindicales (comités permanentes de trabajadores) y predominan los medios impositivos de determinación de condiciones de trabajo. Su historia es de acciones y reacciones, ya que las tres etapas de construcción del derecho laboral colectivo, son seguidas por reacciones conservadoras a partir de la deslegitimación sindical y el rechazo del conflicto, así como la prevalencia de la armonización de intereses a través del canal no sindical» (Castro, 2022, p. 286).

reconocido a quien posee los medios de producción amplios poderes, tanto para organizarlos como para controlar a quienes ponen a su disposición su capacidad de trabajo, estableciéndose dentro de la empresa un sistema de poder absolutamente jerárquico que requeriría una serie de contrapesos que garanticen el respeto de la dignidad de los trabajadores» (Arrieta, 2023, p. 123).

Según la doctrina laboral y constitucional, el hecho de que el poder de dirección y control se deriven del contenido esencial de la libertad de empresa no otorga al empleador facultades absolutas o ilimitadas respecto a la posición subordinada del trabajador. Por el contrario, estos poderes empresariales de dirección y control, aunque tengan fundamento constitucional, están limitados por el derecho constitucional y laboral a la intimidad y la privacidad de las personas trabajadoras en el centro de trabajo y en la relación laboral. En la práctica, sin embargo, no existe normativa interna en los países ni en las empresas que establezca los límites naturales de cada uno de esos dos derechos fundamentales que, en el mundo laboral, entran en colisión.

Por lo tanto, razones históricas del desarrollo político y económico de la sociedad capitalista, así como la falta de fuerza organizativa entre los trabajadores en la empresa (debido a la ausencia de sindicatos) y la carencia de normas positivas (leyes, convenciones colectivas, reglamentos o acuerdos) que establezcan límites naturales al poder de dirección y control del empleador, hacen que el derecho a la intimidad y privacidad de las personas trabajadoras quede injustamente relegado frente a este. La situación se vuelve particularmente peligrosa para el personal subordinado debido al desarrollo vertiginoso de las tecnologías de la información y la comunicación, de la ciencia informática

y biométrica, de la universalización de las redes sociales, del uso del correo electrónico y de las plataformas de mensajería como herramientas de trabajo suministradas por el empleador. Estos avances modernos amplifican la capacidad de control empresarial al facilitar el rastreo, la recolección y el almacenamiento de información sensible de los trabajadores.

Conviene insistir en el punto: el derecho a la intimidad y privacidad de las personas trabajadoras en el entorno laboral debe estar en equilibrio con el interés legítimo de las empresas. La protección de los derechos y la responsabilidad en esta materia incluye, desde la perspectiva laboral y sindical, el cuidado de la información personal del trabajador en su vida cotidiana, la concienciación sobre el uso de su información personal en el ámbito laboral, la negociación colectiva de cláusulas que protejan el derecho a la intimidad y privacidad en el marco de un trabajo digno, así como el ejercicio del consentimiento libre e informado para aceptar estas regulaciones. Desde la perspectiva del trabajador, la protección contra arbitrariedades y usos inadecuados de la información está directamente relacionada con la estabilidad en el empleo, el ejercicio efectivo de la libertad sindical, la protección contra el acoso laboral, la discriminación de género y la protección contra abusos patronales en general.

El objetivo general de este capítulo es presentar alternativas para la negociación colectiva de cláusulas sobre la protección de la intimidad y privacidad de las personas trabajadoras en la empresa, que sirvan para establecer límites al «derecho irrestricto» de las empresas, amparado en la potestad de dirección y control, para documentar, conservar en forma permanente y utilizar la información privada o sensible de sus empleados, incluso en per-

juicio de sus derechos de acceso al empleo, a la estabilidad laboral, a la no discriminación y al ejercicio de la libertad sindical. Los objetivos específicos de este trabajo son los siguientes:

- Analizar las tensiones entre la vigilancia y el control laboral ejercido por el empleador y la protección de datos personales, el derecho a la intimidad y a la privacidad de las personas trabajadoras.
- Identificar las principales amenazas a la intimidad y privacidad de las personas trabajadoras en el lugar de trabajo desde la perspectiva sindical.
- Formular recomendaciones de política pública para lograr un mejor equilibrio entre estos derechos desde la visión de los sindicatos.
- Encontrar alternativas para la negociación colectiva de cláusulas que protejan el derecho a la intimidad y privacidad frente al tratamiento de los datos personales del trabajador en el ámbito laboral.

Para cumplir con dichos objetivos generales y particulares, el presente capítulo se organiza en cuatro secciones: Tensiones entre la privacidad y la intimidad como derecho humano de la persona trabajadora y la libertad de empresa; Protección contra arbitrariedades patronales y usos inadecuados de la información, incluyendo el acoso laboral; Consentimiento libre e informado, y Negociación colectiva y cláusulas de protección del derecho a la privacidad en el marco de un trabajo digno.

## 2. Tensiones entre la privacidad y la intimidad como derecho humano de la persona trabajadora y la libertad de empresa

Es habitual que las empresas, especialmente las de mayor tamaño,

implementen mecanismos de vigilancia y control del personal a la entrada y salida del trabajo. Esto puede incluir la revisión de pertenencias personales, cacheos generales o selectivos y otras medidas de seguridad destinadas a prevenir robos de propiedad del empleador o la sustracción de información confidencial de la empresa. Además, cada vez es más frecuente exigir exámenes médicos para detectar el consumo de ciertos fármacos o drogas, así como pruebas de embarazo o evaluaciones psicológicas. Con el avance tecnológico, también se ha vuelto normal la instalación de cámaras de vigilancia en el interior de las empresas, así como el registro de la hora de entrada y salida mediante mecanismos biométricos como la huella dactilar, el reconocimiento facial, la geometría de la mano, el reconocimiento de voz y el escaneo de retina. Estos procedimientos, que a menudo vulneran la intimidad y privacidad de los trabajadores, permiten al empleador acceder a información sensible de su personal en tiempo real y almacenarla en archivos electrónicos permanentes.

Desde la entrevista de trabajo, el empleador recopila información privada y sensible de los candidatos, la cual conserva en sus registros. Suministrar esta información se convierte en una obligación para el aspirante al puesto de trabajo, ya que, si se niega a proporcionar algún tipo de información solicitada en la entrevista, es descartado como candidato.

Con la popularización de las redes sociales (como Facebook, Twitter[3], Instagram, entre otras) y la adopción del correo electrónico y plataformas de mensajería instantánea como WhatsApp por parte de los empleadores como herramientas de trabajo

[3] Desde el 24 de julio de 2023, Twitter pasó a llamarse X.

obligatorias para su personal, han surgido nuevas posibilidades tecnológicas para el rastreo, la localización, la grabación y el almacenamiento de información privada o sensible de las personas trabajadoras. Esta información se almacena y queda a disposición del empleador, y en ocasiones, el personal no tiene conocimiento de que dicha información está en poder de quienes los contratan.

El desarrollo avanzado del software y hardware en el ámbito de la informática permite al empleador acceder a información personal del trabajador que va más allá de lo necesario para conocer sus competencias y habilidades laborales o profesionales, pudiendo incursionar en áreas muy sensibles de su intimidad. Por ejemplo, filiación política y sindical, credo religioso, vínculos sociales, estado de salud, condiciones de discapacidad, uso de medicamentos o drogas, antecedentes penales, informes crediticios, preferencias sexuales, opiniones personales sobre el trabajo, la empresa empleadora o sus representantes, y sobre las autoridades públicas, entre otros aspectos.

Otras situaciones incluyen, por ejemplo, la prohibición de citas interinstitucionales o relaciones de pareja entre empleados, así como la obligación de cumplir o abstenerse de ciertas conductas o comportamientos fuera del horario laboral, como el uso de herramientas de trabajo propiedad del empleador (computadoras, teléfonos, bíper…) o el acceso a redes o plataformas de mensajería fuera del horario laboral.

Finalmente, es importante destacar los temas relacionados con la seguridad de la información privada de las personas trabajadoras, que la empresa gestiona y custodia en diversos formatos. Aunque esta información sea recopilada de forma legítima por la empresa, no siempre es de dominio público y un descuido por

parte del empleador o actos delictivos de sus representantes podrían comprometer gravemente la privacidad de los trabajadores.

Todo este poder empresarial, que legalmente no está delimitado y que se ve magnificado por el uso de las nuevas tecnologías, genera una tensión constante con el derecho humano o fundamental del trabajador a preservar su intimidad y privacidad frente a las intromisiones ilegítimas de la empresa o institución empleadora.

En sí mismo, el poder de dirección empresarial, en sus dos dimensiones (organizar la empresa en general y ordenar las prestaciones de los trabajadores individualmente), no es inherentemente negativo para el personal. La empresa, como entidad responsable, posibilita el empleo digno y el salario justo, que son fundamentales para el sustento familiar de los trabajadores. Sin embargo, para su funcionamiento adecuado, la empresa requiere recursos humanos, económicos y técnicos, así como organización y control, responsabilidades y funciones que corresponden al empresario, quien asume el riesgo de invertir el capital necesario para organizar la empresa y garantizar su funcionamiento y sostenibilidad a largo plazo.

Lo verdaderamente pernicioso es el ejercicio arbitrario, abusivo o malintencionado de esa autoridad patronal. Cuando el empleador utiliza la información privada de los trabajadores o invade su intimidad de manera no ética, o contraviniendo abiertamente la buena fe que debería imperar en las relaciones laborales, pone en peligro los derechos fundamentales de cada individuo que forma parte de su personal y afecta negativamente al ambiente laboral.

Ante estas tensiones, es crucial buscar puntos de equilibrio que consideren todos los intereses y derechos en juego. La inti-

midad y privacidad del trabajador deben protegerse en la medida en que no socaven injustificadamente la capacidad de gestión de la empresa ni constituyan un abuso de este derecho.

Por ejemplo, se consideran legítimos algunos controles empresariales sobre correos electrónicos o navegación web con fines laborales, siempre que se haya informado debidamente, pero no así la lectura indiscriminada de comunicaciones personales. Del mismo modo, se admite la videovigilancia con garantías contra posibles abusos, pero no se justifican los exámenes médicos invasivos que no estén relacionados con las funciones del puesto de trabajo.

En última instancia, se requiere un equilibrio prudente y razonable entre estos derechos e intereses contrapuestos. En cada caso, se debe evaluar si las medidas empresariales que puedan afectar a los derechos fundamentales, como la privacidad o la intimidad del trabajador, están debidamente justificadas. Solo de esta manera se garantizará un entorno laboral en el que se protejan adecuadamente la dignidad y la libertad de los trabajadores, así como la capacidad organizativa de las empresas.

### 3. Protección contra arbitrariedades patronales y usos inadecuados de la información, incluido el acoso laboral

No existen normativas o principios generales que establezcan límites claros al poder de dirección empresarial, lo que dificulta la prevención generalizada de la arbitrariedad patronal y el abuso contra los trabajadores por el uso indebido de su información sensible o privada, que es recopilada y custodiada por la empresa.

En aquellas organizaciones empresariales donde no hay presencia sindical ni negociación colectiva, el poder del empleador

se muestra como una autoridad unilateral y robusta, que, al carecer de límites, puede ser proclive al abuso.

Algunas manifestaciones de este uso indebido de la información privada de los trabajadores se producen cuando se utiliza para discriminar, negando la contratación, elaborando «listas negras» para impedir el reingreso de los trabajadores a la empresa o para coartar la libertad sindical, entre otras acciones similares. Esta información también se emplea para disciplinar o sancionar a los trabajadores.

En la práctica laboral actual, es frecuente el uso de esta información privada para acosar laboralmente a los trabajadores que se desea expulsar de la empresa.

Según Rosario Peña Pérez, al intentar definir el acoso laboral, existen tres corrientes doctrinales desde el punto de vista jurídico. La primera, defendida por Velázquez, entiende que el acoso constituye un ataque a la dignidad y a la salud laboral del trabajador. La segunda, propuesta por Molina Navarrete, considera que es un acto pluriofensivo que afecta a un conjunto de derechos fundamentales, todos ellos relacionados con la dignidad. La tercera, definida por Sagardoy, sostiene que es un ataque a la dignidad del trabajador entendida como dignidad profesional.[4] Sin embargo, una definición que refleja de manera acertada la vivencia personal es la que dio el juez Ramón Gimeno Lahoz hace diez años: «Es la presión laboral tendente a la autoelimi-

---

[4] María José Blanco Barea y Javier López Parada, «La dignidad y el *mobbing* en un estado social y democrático de derecho», en *Preventionworld.com* (entrada del 19 de mayo del 2002). Recuperado de: https://prevention-world.com/actualidad/articulos-tecnicos/dignidad-y-mobbing-estado-social-y-democratico-derecho/

nación de un trabajador mediante su denigración» (Peña Pérez, 2013, p. 40).

El núcleo central del acoso laboral descrito consiste en un ataque a la dignidad del trabajador mediante su denigración. Para lograr este objetivo, se requiere información relativa a la intimidad y privacidad de la persona trabajadora, siendo los bancos de datos privados del personal custodiados por el empleador un elemento central en este proceso.

Estas arbitrariedades o abusos patronales son posibles gracias a la posición de poder del empleador frente a sus empleados subordinados. Además, el desarrollo tecnológico y las ciencias informáticas han permitido la creación de lo que se conoce como «empresa panóptica», un concepto derivado de la arquitectura carcelaria ideada por el filósofo Jeremy Bentham y desarrollado por Michel Foucault. En este modelo, desde un punto central se ejerce vigilancia, control y corrección sobre todos los espacios y sujetos dentro de la empresa. Este panoptismo moderno se realiza mediante la tecnología y las ciencias informáticas aplicadas al control empresarial (Ávila-Fuenmayor, 2016, pp. 215-234).

En el contexto laboral moderno, una empresa panóptica se caracteriza por lo siguiente:

- Monitoreo constante de los empleados: los empleados sienten que son observados y evaluados constantemente a través de cámaras de seguridad, software de monitoreo de computadoras, control de acceso biométrico, etc.
- Recopilación masiva de datos: las empresas recopilan grandes cantidades de datos sobre el desempeño, las actividades, la ubicación y el comportamiento de los empleados.

- Estructura jerárquica rígida: existe una clara separación entre quienes controlan y monitorizan (gerentes) y quienes son controlados y monitorizados (empleados).
- Disciplina y normalización: se busca que los empleados se ajusten a ciertas normas y estándares de comportamiento y productividad mediante mecanismos de vigilancia y posibles sanciones.
- Poder asimétrico: la dirección tiene un gran poder de control y toma de decisiones, mientras que los empleados tienen poca autonomía.

Estas características evidencian una forma de control empresarial excesivo y una violación de la privacidad de los trabajadores y las trabajadoras, que es necesario limitar para que el derecho a la intimidad y a la privacidad de cada individuo empleado prevalezca y no sea anulado por la potestad de dirección y control del empleador.

Para equilibrar los derechos fundamentales a la intimidad y privacidad que corresponden a la persona trabajadora con la libertad de empresa y su potestad de dirección y control del empleador en el mundo de las relaciones laborales, es necesario desarrollar sindicatos fuertes, garantizar el ejercicio pleno de la libertad sindical y consolidar el derecho a la negociación colectiva.

Además, es necesario desarrollar reglas claras de proporcionalidad y ponderación que permitan determinar en cada caso concreto qué derecho tiene preponderancia y cuál de los dos derechos debe ceder para no romper el esquema de equidad y justicia, consustancial a toda idea de derecho y, más aún, al derecho propio de una sociedad democrática.

Otra norma importante para proteger a las personas trabajadoras de las intromisiones de los empleadores en su intimidad y

privacidad es la exigencia del consentimiento libre e informado, lo cual se desarrollará en el siguiente apartado.

#### 4. Consentimiento previo, libre e informado

El principio del consentimiento previo, libre e informado es fundamental en el ámbito del derecho a la intimidad y la privacidad de los trabajadores. Básicamente, implica que cualquier acción que afecte la privacidad de un individuo en el contexto laboral debe basarse en su consentimiento voluntario, otorgado después de recibir información completa y comprensible sobre las implicaciones de dicha acción. Desde la perspectiva legal, el consentimiento previo, libre e informado implica dos elementos clave: voluntariedad e información completa, comprensión y capacidad de retirar consentimiento.

- Voluntariedad: el trabajador o la trabajadora deben otorgar su consentimiento de manera voluntaria, sin coerción, amenaza o presión indebida por parte del empleador u otras partes involucradas.
- Información completa: el trabajador o la trabajadora debe recibir información detallada y clara sobre qué datos personales se recopilarán, cómo se utilizarán, quién tendrá acceso a ellos y cualquier otro aspecto relevante relacionado con la privacidad.
- Comprensión: el trabajador o la trabajadora debe comprender completamente la información proporcionada, incluidas las implicaciones legales y prácticas de otorgar su consentimiento.
- Capacidad de retirar el consentimiento: el trabajador o la trabajadora debe tener la opción de retirar su

consentimiento en cualquier momento, sin sufrir consecuencias adversas en el ámbito laboral.

El resultado de una correcta aplicación del consentimiento previo, libre e informado es que ninguna información del trabajador o de la trabajadora que esté en poder del empleador se podrá utilizar en su contra si no se le ha informado de manera amplia y comprensible sobre la existencia de esa información, el medio en que está grabada y los alcances de su autorización expresa al empleador para utilizarla.

Si no se cumple con lo anterior, la información privada del trabajador que afecte el derecho a la intimidad no podrá ser utilizada por el empleador para ningún fin, mucho menos para sancionar o disciplinar.

### 5. La negociación colectiva y las cláusulas de protección del derecho a la intimidad y a la privacidad en el marco de un trabajo digno

La legislación moderna de casi todos los países cuenta con normas y sanciones para las personas responsables de bases de datos físicas o electrónicas, ya sean públicas o privadas, que accedan, registren o conserven información personal. Esta información puede ser de dos tipos: datos personales de uso restringido, que, aunque formen parte de registros de acceso público, no son de acceso irrestricto ya que son de interés solo para su titular o para la administración pública; y datos personales sensibles, que revelan aspectos íntimos de la persona, como el origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros. Por ejemplo, en Costa Rica, la Ley de Protección de la Persona frente al Tratamiento

de sus Datos Personales (n.º 8968, del 7 de julio de 2011) aborda este tema.

Sin embargo, esta legislación no está diseñada para proteger a la persona trabajadora del uso que pueda hacer su empleador de la información a la que accede, almacena o custodia en la empresa. Esta información puede permanecer en poder del empleador incluso después de finalizada la relación laboral.

Esta situación, nueva en cuanto a su intensidad y alcance, carece de un control normativo específico, o al menos no se han creado aún disposiciones legales que limiten el poder del empleador y garanticen el pleno reconocimiento del derecho a la intimidad y privacidad de la persona trabajadora dentro de la empresa.

Es aquí donde surgen la acción sindical y la negociación colectiva como medios idóneos para establecer límites al poder del empleador y proteger así los derechos fundamentales a la intimidad y privacidad de las personas trabajadoras en un mundo laboral cambiante y en permanente evolución tecnológica. La negociación colectiva se convierte en el principal instrumento sindical y de los trabajadores para proteger sus datos personales en el ámbito de la empresa y frente a su empleador.

La negociación colectiva es un proceso mediante el cual los empleadores y los representantes del sindicato, en representación de los empleados, negocian los términos y condiciones de empleo. Una vez se llega a un acuerdo, este puede formalizarse en una convención colectiva de trabajo, que establece los derechos y obligaciones de ambas partes durante un período de tiempo determinado. La negociación colectiva es fundamental para garantizar relaciones laborales justas y equilibradas, y promover la estabilidad laboral y el bienestar tanto de los trabajadores

como de los empleadores. Esto incluye aspectos como salarios, horarios, beneficios y cláusulas de protección de la intimidad y privacidad frente al uso no autorizado de la información personal o reservada de la persona trabajadora.

La convención colectiva de trabajo tiene la virtud de ser adaptativa y de revisión periódica, lo que hace posible ajustarla al mismo tiempo que se introducen nuevos cambios tecnológicos o en la organización de la empresa y su entorno. Más específicamente, la negociación colectiva del trabajo puede desempeñar un papel importante en la protección de los derechos a la intimidad y a la privacidad de los trabajadores en los siguientes ámbitos:

- *Inclusión de cláusulas de privacidad en los contratos individuales de trabajo*: las partes pueden negociar en la convención colectiva de trabajo la inclusión de disposiciones específicas en los contratos individuales de trabajo que protejan la privacidad de los trabajadores. Esto puede incluir regulaciones sobre el uso de datos personales, supervisión en el lugar de trabajo y acceso a información confidencial, como parte del establecimiento de relaciones laborales compatibles con los criterios del trabajo digno.
- *Cláusulas que garanticen el consentimiento previo informado y políticas de concienciación sobre el uso responsable de la información personal*: a través de la negociación colectiva, se puede hacer obligatorio el consentimiento previo informado, sin el cual no se puede utilizar la información privada del trabajador. Igualmente, el empleador debe comprometerse a facilitar espacios de información y capacitación sobre el uso de las redes sociales y otras plataformas, sin riesgo de filtración, robo o abuso de la información privada de los trabajadores.

- *Establecimiento de procedimientos justos para la vigilancia en el lugar de trabajo*: a través de la negociación colectiva, se pueden acordar políticas y procedimientos claros y transparentes sobre el monitoreo electrónico, el uso de cámaras de seguridad y otras formas de vigilancia en el lugar de trabajo, asegurando que se respeten los derechos de privacidad de los trabajadores.
- *Definición de límites en la divulgación de la información personal*: las partes pueden acordar restricciones sobre la divulgación de información personal de los trabajadores a terceros, garantizando que los datos personales se traten de manera confidencial, se utilicen únicamente para fines legítimos relacionados con el empleo y se destruyan o devuelvan al trabajador una vez que concluya la relación laboral.
- *Protección contra la discriminación, el acoso laboral y sexual, así como la persecución sindical*: a través de la negociación colectiva, se pueden establecer políticas y procedimientos para prevenir y abordar todo tipo de discriminación, el acoso laboral y sexual en el lugar de trabajo, y todo tipo de persecución sindical, lo que contribuye a proteger la privacidad y la dignidad de los trabajadores.
- *Cláusulas de protección contra acciones invasivas*: la negociación colectiva permite establecer cláusulas que prohíban al empleador realizar acciones de control invasivas en la salud o el cuerpo de sus trabajadores, como exámenes de embarazo o de control de consumo de drogas, así como pruebas psicológicas.
- *Prohibición del uso de la información personal de las personas trabajadoras en su perjuicio*: las convenciones colectivas de trabajo pueden

establecer políticas que prohíban utilizar la información personal del trabajador que circula en redes sociales en su perjuicio en procedimientos disciplinarios o judiciales. También se puede prohibir al empleador que abra los mensajes personales del correo electrónico, aunque este forme parte de una plataforma empresarial.

- *Cláusulas para garantizar la autonomía informativa de la persona trabajadora*: la negociación colectiva debe crear normas que permitan a la persona trabajadora decidir sobre el uso que da a su información personal, por ejemplo, respecto a su imagen personal y sus preferencias religiosas, políticas o sexuales.
- *Cláusulas convencionales para utilizar el principio de proporcionalidad en caso de duda*: cuando, para lograr un objetivo legítimo derivado de un derecho fundamental, es indispensable limitar otro derecho fundamental de tal manera que la satisfacción de uno solo pueda realizarse a costa del otro, debe aplicarse el juicio de proporcionalidad en sentido estricto.[5] En estos casos, es necesario establecer en los convenios colectivos de trabajo, al menos, los parámetros mediante los cuales estas cuestiones serán interpretadas y resueltas en caso de duda. El principio de proporcionalidad se presenta como el mecanismo más idóneo para este fin, entendido como el triple juicio de proporcionalidad o subprincipios desarrollados en el proceso constitucional.

---

[5] José Luis Ugarte Cataldo, «Privacidad, trabajo y derechos fundamentales», en *Estudios Constitucionales*, año 9, núm. 1 (Santiago de Chile: Centro de Estudios Constituciones, 2011), pp. 13-36. Recuperado de: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002011000100002

Estos subprincipios son: el juicio de idoneidad, el juicio de necesidad y el de proporcionalidad en sentido estricto.[6]

La negociación colectiva es una herramienta eficaz para mitigar la ausencia de límites a la potestad del empresario de dirección y control en la empresa. Si se utiliza correctamente, puede convertirse en un medio eficiente para que los sindicatos y los trabajadores fortalezcan la protección de los derechos a la intimidad y a la privacidad en la empresa, permitiendo la creación de normas y procedimientos que respeten y salvaguarden estos derechos fundamentales.

## 6. Conclusión

Una revisión del estado del arte en materia de protección del derecho a la intimidad y privacidad de la persona trabajadora en el ámbito empresarial nos lleva a las siguientes conclusiones.

Históricamente, los derechos a la intimidad y privacidad de los trabajadores han sido considerados fundamentales, aunque, en la era capitalista de las democracias liberales, los derechos

---

[6] El juicio de idoneidad exige que la restricción al derecho fundamental de que se trate permita alcanzar efectivamente un fin legítimo, entendiendo por tal un fin o interés de naturaleza constitucional. La idea relevante en este subprincipio es rechazar, por desproporcionadas, las medidas o conductas inidóneas del empleador. Al juicio de necesidad, por su parte, le importa que la medida o restricción del derecho fundamental sea indispensable para lograr el fin legítimo, no existiendo una alternativa más benigna con el derecho fundamental en cuestión. En ese sentido, será necesaria y proporcionada la conducta del empleador que restringe derechos fundamentales del trabajador solo cuando no exista un medio menos gravoso de obtener el objetivo perseguido. Por último, se utiliza el juicio de proporcionalidad en sentido estricto. Solo si la restricción es considerada idónea y necesaria, corresponde, y solo en ese caso, revisar si, además, es proporcional en sentido estricto (Ver José Luis Ugarte Cataldo, *op. cit.*)

empresariales, como el de propiedad privada y la libertad de empresa, han prevalecido. Esto ha llevado a una situación en la que los empleadores han tenido un control prácticamente absoluto sobre sus empleados en el ámbito laboral, menoscabando así la autonomía de la intimidad y privacidad de los trabajadores, reconocida plenamente solo fuera del entorno laboral.

En países como Costa Rica, donde la sindicalización es baja y la regulación unilateral de las condiciones laborales prevalece sobre la negociación colectiva, el poder político e ideológico de los empleadores se ve fortalecido, ya que los trabajadores carecen de la capacidad de actuar en conjunto a través de sindicatos para defender sus intereses.

Estas tensiones históricas entre los derechos a la intimidad y privacidad y las potestades de dirección y control del empleador se han agravado con la irrupción de las nuevas tecnologías de la información y la comunicación. La empresa ahora tiene acceso a información privada de los trabajadores a través de diversas herramientas, lo que ha generado preocupaciones sobre el uso abusivo de dicha información y la implementación de medidas invasivas de control.

La normativa nacional, tanto laboral como civil o administrativa, se muestra insuficiente para establecer límites claros a la potestad patronal y proteger a los trabajadores en sus derechos fundamentales a la intimidad y privacidad. Es en el ámbito constitucional y en las decisiones jurídicas internacionales donde se ha desarrollado jurisprudencia vinculante, aunque aún es insuficiente para proteger de manera efectiva a los trabajadores contra el abuso de sus datos personales por parte de las empresas.

La negociación colectiva, especialmente la suscripción de convenciones colectivas de trabajo, es el medio más idóneo para

establecer límites a la potestad del empleador y proteger la intimidad de los trabajadores. A través de esta, se pueden introducir cláusulas generales de protección de la intimidad y la privacidad de las personas trabajadoras, así como prohibiciones concretas sobre el uso abusivo de su información personal por parte de los empleadores. También se puede garantizar el consentimiento previo e informado para cualquier uso de la información privada del personal y prohibir su uso para fines discriminatorios, acosos laborales, persecuciones sindicales o disciplina dentro de la empresa o en procesos judiciales.

En resumen, la negociación colectiva es fundamental para establecer un equilibrio entre los derechos del empleador y los derechos fundamentales de los trabajadores a la intimidad y privacidad en el entorno laboral.

**Bibliografía**

Abogados con Experiencia (bufete jurídico), *Comprendiendo las causas clave de las preocupaciones sobre la privacidad en el lugar de trabajo*. Recuperado de: https://abogadosconexperiencia.com/laboral-y-empleo-blog/comprendiendo-las-causas-clave-de-las-preocupaciones-sobre-la-privacidad-en-el-lugar-de-trabajo

Asamblea Legislativa de Costa Rica, Proyecto de ley, expediente núm. 16919: *Reforma de los artículos 69 inciso c), 70 y 83 del código de trabajo, ley núm. 2 de 27 de agosto de 1943*. 2008. (Para introducir protección expresa al derecho a la intimidad de la persona trabajadora)

----------, Ley N.º 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales. (Se aprobó el 7 de julio del 2011).

Arrieta Segleau, Fabián, «Los poderes del empleador y sus límites», en *Curso de Derecho Laboral*, tomo IV (San José de Costa Rica: Editorial Jurídica Continental, 2023), pp. 117-220.

Ávila-Fuenmayor, Francisco, «El concepto de poder en Michel Foucault», en *Telos*, vol. 8, núm. 2 (Maracaibo: Universidad Privada Dr. Rafael Belloso Chacín, 2006), pp. 215-234.

Carro H., Rocío y Gabriel Espinoza C., «Equilibrio entre la privacidad del trabajador y poderes empresariales», en *Revista Judicial de la Corte Suprema de Justicia*, núm. 108 (San José de Costa Rica: Corte Suprema de Justicia, 2013), pp. 23-45.

Castro Méndez, Mauricio, *Legitimación, conflicto y disciplinamiento laboral: modelos iberoamericanos y de representación colectiva* (Montevideo: Ediciones Fundación de Cultura Universitaria, 2022). Disponible en:
https://legalaidatwork.org/es/factsheet/privacy-in-the-workplace/

Garro Morales, Ángela María y Ana Luisa Meseguer Monge, *El correo electrónico de los trabajadores*. Tesis de Maestría en Derecho del Trabajo y Seguridad Social de la UNED, 2004.

Legal Aid at Work, *Privacidad en el lugar de trabajo*. Disponible en:
https://legalaidatwork.org/es/factsheet/privacy-in-the-workplace/

Legálitas, *Los límites de la empresa para controlar a sus trabajadores*. Disponible en:
https://www.legalitas.com/actualidad/que-puede-hacer-y-que-no-la-empresa-en-relacion-a-datos-personales-de-empleados

LegalShield, *Leyes de privacidad de los empleados*. Disponible en:
https://www.legalshield.com/blog/es-blog/derechos-de-los-trabajadores/leyes-de-privacidad-de-los-empleados/

Organización Internacional del Trabajo (OIT), *Protección de los datos personales de los trabajadores. Repertorio de recomendaciones prácticas de la OIT* (Ginebra: Oficina Internacional del Trabajo, 1997).

----------, *Convenio sobre la discriminación (empleo y ocupación), 1958 (núm. 111)*, aprobado por Costa Rica mediante la Ley 2848 del 26 de octubre de 1961.

Peña Pérez, Rosario, *El acoso laboral* (Bogotá: Ediciones la U, 2013).

Toscani Gimenes, Daniel, «El derecho a la libertad de expresión de los trabajadores», en *Linkedin* (Fecha de publicación: 20 de mayo de 2021). Recuperado de: https://es.linkedin.com/pulse/el-derecho-la-ibertad-de-expresi%C3%B3n-los-trabajadores-toscani-gimenez

Varela Arroyo, Julia, «El impacto de las redes sociales en los derechos de los trabajadores y en los derechos laborales del siglo XXI», en *Curso de Derecho Laboral*, tomo IV (San José de Costa Rica: Editorial Jurídica Continental, 2023), pp. 221 a 368.

CAPÍTULO V

# Manejo de la privacidad en el trabajo

**Federico Anaya Ojeda**
Presidente Ejecutivo del Instituto Latinoamericano del Derecho del Trabajo y Seguridad Social

## Introducción

En el mundo actual, donde la información y la tecnología desempeñan y desempeñarán papeles fundamentales en todas las esferas de la vida, la protección de los datos personales y la privacidad se han convertido en temas de máxima relevancia. El ámbito laboral no es una excepción a esta regla; tanto los trabajadores como los empleadores, sin menoscabar el papel del Estado y las autoridades, deben establecer conjuntamente políticas claras y éticas que protejan de manera precisa y rápida la información confidencial de las personas involucradas en una relación laboral, garantizando el respeto de los derechos individuales de cada uno.

En el desarrollo de esta obra se abordan diversos aspectos relacionados con la privacidad y la protección de datos en el ámbito laboral, tanto de los trabajadores como de los empleadores. Se destaca la importancia de establecer políticas de privacidad y adaptarse a las tecnologías emergentes. Se subraya la necesidad de obtener el consentimiento de los trabajadores y de recopilar

los datos de manera transparente y ética. Asimismo, se examina la manera de supervisar y monitorear responsablemente a los empleados durante la jornada laboral. También se enfatiza la relevancia de las auditorías y del cumplimiento normativo en los procesos de mejora continua, así como la retención y eliminación de los datos personales. Por último, se explora la privacidad en el futuro con la implementación de nuevas tecnologías.

A través del análisis de estos temas, se explora cómo las empresas pueden gestionar de manera efectiva la protección de datos y la privacidad, asegurando el cumplimiento normativo y promoviendo una cultura de respeto a la privacidad mediante la adopción de medidas adecuadas para enfrentar los desafíos que plantea la evolución tecnológica.

### 1. Políticas de privacidad empresarial

El desarrollo de políticas claras de privacidad es fundamental dentro de la empresa para respetar los derechos individuales y colectivos de los trabajadores, además de para establecer un ambiente de trabajo confiable y ético. Estas políticas deben basarse en principios estrictamente apegados a la ley y a la ética, proteger la privacidad y la información personal de las personas, y regular el uso de esta información por parte del empleador.[1]

Para empezar, estas políticas de privacidad deben identificar los tipos de datos personales que la empresa va a recopilar, procesar, almacenar y destruir, y los propósitos legítimos en los que estos datos se van a basar. Esta información incluye, además del

---

1 Roberto Massa, *Planeación estratégica de los datos personales: del diagnóstico al plan de trabajo* (Ciudad de México: Aldo Mauricio Massa y Amazon Publishing, 2021).

nombre de la persona, su domicilio, los números de identificación, cuentas bancarias, datos financieros, datos de la seguridad social, registros médicos y cualquier otra referencia que pudiera identificar a la persona.

Estas políticas también deben definir de manera clara y precisa las medidas de protección y seguridad que la empresa debe implementar para evitar accesos no autorizados, pérdida de información, filtraciones o hackeo de los datos personales. Estas medidas pueden incluir el uso de sistemas restringidos o cifrados, un acceso controlado a datos sensibles, así como procedimientos de eliminación segura de información que ya no se utilice o que se considere obsoleta.

Por último, estas políticas deben establecer las responsabilidades y obligaciones de los trabajadores en relación con la privacidad de los datos. Esto puede incluir instrucciones para el manejo adecuado de la información confidencial, prohibiciones expresas de compartir datos personales sin autorización y la notificación inmediata por parte del empleador de las posibles brechas de seguridad o incidentes de privacidad que pongan en riesgo la información de los trabajadores.[2]

La comunicación efectiva de las políticas de privacidad por parte de la empresa a los empleados es fundamental para asegurar su comprensión y, en consecuencia, su cumplimiento. Las estrategias empleadas deben ser transparentes, específicas y accesibles, y garantizar que todos los trabajadores conozcan sus derechos y responsabilidades en relación con el manejo y utilización de datos personales.

---

2 Massa, *op. cit.*

Una de las formas más efectivas de comunicar estas políticas es a través de manuales. Estos documentos formales describen con detalle las políticas y procedimientos relacionados con la privacidad de datos. Deben ser accesibles para los trabajadores, ya sea en formato físico o virtual, y actualizarse constantemente cuando haya cambios en las políticas.

Una comunicación efectiva de las políticas de privacidad debe complementarse con la obligación del empleador de proporcionar capacitación a los trabajadores, en particular, sesiones informativas sobre las políticas de privacidad, sus implicaciones y cómo aplicarlas en el día a día. El objetivo de esta formación es fomentar una cultura de privacidad en toda la organización para garantizar que los empleados comprendan la importancia de proteger la información confidencial.

La comunicación efectiva también implica establecer canales de contacto y mecanismos de consulta, como la línea roja, la voz con valor, que son medios de comunicación que utilizan las empresas con sus trabajadores para establecer un diálogo directo. También se pueden usar buzones anónimos u otros medios similares para que los empleados tengan una vía institucional para plantear sus interrogantes y preocupaciones o reportar posibles violaciones a la privacidad de manera confidencial y segura.

Es de suma importancia que estas políticas se integren en la cultura de la empresa, ya que de lo contrario no serían efectivas ni serían aceptadas por los empleados. Para lograrlo, es necesario alinear las políticas de privacidad con los valores, principios, objetivos, misión, visión y planificación estratégica de la empresa, asegurando la congruencia en las prácticas relacionadas con la privacidad de datos.

Como en todas las grandes decisiones empresariales, es indispensable que los líderes de la empresa se involucren y respalden activamente las políticas de privacidad. Esto puede incluir comunicaciones internas que destaquen la importancia de la privacidad y su inclusión como un tema relevante en las actividades de formación y desarrollo profesional. Con el respaldo de los líderes, será más fácil promover una cultura de respeto a la privacidad de los empleados.

Las políticas de privacidad deben reflejarse en las prácticas operativas y en las decisiones empresariales diarias. Hay que considerar e integrar las políticas de privacidad en las prácticas operativas, en las decisiones cotidianas de la empresa, en el diseño de productos y servicios, en la administración de los datos de los clientes y proveedores y, por supuesto, en la implementación de las tecnologías de la información y la comunicación.

La cultura organizacional debe valorar y proteger la privacidad de los datos en el entorno laboral, desarrollando políticas claras a ese respecto, comunicándolas de manera efectiva a los empleados e integrándolas en la cultura empresarial. Todo ello en conjunto, valga la insistencia, promoverá la confianza, el compromiso y el bienestar de los trabajadores.

Un modelo de lo anterior en México son los esquemas de autorregulación de datos personales emitidos por el Instituto Nacional de Acceso a la Información y Protección de Datos Personales.[3] El cumplimiento irrestricto de estos esquemas permite obtener una certificación en privacidad. Cada país debería tener

---

[3] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *Guía de autorregulación*. Recuperado de https://inicio.inai.org.mx/CalendarioCapacitacion/GUIA%20AUTORREGULACION.pdf

su propia entidad reguladora, como ocurre en Argentina con la Agencia de Acceso a la Información Pública (AAIP), en Brasil con la Autoridad Nacional de Protección de Datos (ANPD) y en Perú con la Autoridad Nacional de Protección de Datos Personales (ANPDP), por citar algunos ejemplos.

### 2. Consentimiento y obtención de datos

A medida que el derecho a la privacidad en el ámbito laboral adquiere una relevancia creciente en el mundo de la tecnología, la recopilación de datos se vuelve cada día más necesaria e intrusiva. Uno de los pilares fundamentales para respetar este derecho es obtener el consentimiento de los empleados para la recopilación y el uso de sus datos personales. Este proceso debe realizarse de manera ética y legal para garantizar el derecho a la privacidad de los trabajadores y favorecer el cumplimiento normativo (o *compliance*) necesario para el buen funcionamiento de la empresa.

Pero este consentimiento no es de cualquier tipo; por parte del empleado, implica que debe estar informado sobre los datos que se van a recopilar, la manera en que se van a utilizar y cómo se van a proteger. No basta con obtener su firma en el documento, sino que es necesario que los empleados comprendan totalmente las implicaciones de dar su consentimiento y que puedan revocarlo en cualquier momento.[4]

La recopilación y el uso de la información personal en el trabajo deben regirse por principios éticos y jurídicos que, por supuesto, respeten, guarden y protejan los derechos de los trabajadores.

---

[4] Reglamento General (UE) 2016/679, de 27 de abril, de protección de datos. Parlamento Europeo, Consejo de la Unión Europea. https://gdpr-info.eu/

Las empresas deben transparentar en todo momento los datos que se recopilan, la manera en que se recopilan y la forma en que se utilizarán en el futuro, con información precisa y comprensible, incluso antes de solicitar el consentimiento del trabajador.

Además, la recopilación de datos debe ser proporcional al propósito legítimo para el que se está recabando la información y evitar en todo momento una recopilación innecesaria, irrelevante o excesiva de información personal. De la misma forma, es indispensable que el empleador implemente medidas de seguridad adecuadas para proteger la información de los trabajadores contra accesos no autorizados, piratería de la información, pérdidas o filtraciones. El consentimiento informado debe ser informado, valga la redundancia. Debe ser otorgado de manera voluntaria por el trabajador, sin presión ni condicionamiento alguno. Asimismo, los empleados deben poder retirar su consentimiento, como se ha mencionado anteriormente.

En algunos países, este consentimiento se obtiene a través del aviso de privacidad. Este documento es una herramienta esencial para obtener el consentimiento informado y, al mismo tiempo, explicar a los empleados la manera en que se gestionan sus datos personales en el ámbito laboral. Este aviso de privacidad debe ser claro y comprensible, y proporcionar información sobre aspectos importantes, como la identidad del responsable, las finalidades del tratamiento de los datos personales, los datos recopilados, los fundamentos jurídicos para la obtención y el tratamiento de los datos, los derechos de los empleados en relación con sus datos, las medidas de seguridad que aplicará el empleador y la posibilidad de transferir los datos a terceros, asegurando la protección de la información en esas transferencias.

La finalidad principal de la recopilación de datos es utilizarlos para prestar servicios y cumplir con las obligaciones jurídicas de la empresa, como el pago de salarios y la identificación de los trabajadores ante las autoridades gubernamentales. Secundariamente, estos datos pueden utilizarse para el análisis, el estudio y la mejora de los procesos o servicios, siempre con el consentimiento explícito del trabajador.

En Estados Unidos, la Unión Europea, Canadá, México, Brasil y Australia, el aviso de privacidad se emplea activamente y su eso está regulado por las leyes internas.[5]

| **Tabla 1. Leyes del derecho a la privacidad** | |
|---|---|
| **País** | **Ley/Regulación** |
| Estados Unidos | Ley de protección de la Privacidad en Línea los Niños (COPPA), Ley de Privacidad del Consumidor de California (CCPA) |
| Unión Europea | Reglamento General de Datos (GDPR) |
| Canadá | Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA) |
| México | Ley Federal de Protección de Datos Personales en Posesión de Particulares |
| Brasil | Ley de Protección de Datos (LGPD) |
| Australia | Ley de Privacidad de la Información (Privacy Act) |
| Fuente: OpenAI, ChatGPT (versión del 14 de marzo) Lenguaje amplio. https://chat.openai.com/chat | |

En conclusión, el aviso de privacidad es una herramienta decisiva para informar a los empleados sobre cómo se recopilan, utili-

[5] Ley Federal de Protección de Datos Personales en Posesión de los Particulares del 4 de octubre de 2023.

zan, guardan y protegen sus datos personales en el ámbito laboral. Además, permite que el empleador obtenga el consentimiento del trabajador de manera transparente, informada y ética.

Este aviso debe ser comprensible para todos los empleados y proporcionar información sobre los siguientes aspectos:

- Identidad del responsable.
- Finalidad del tratamiento de los datos.
- Tipo de datos recopilados.
- Fundamentos legales del tratamiento de los datos.
- Derechos de los trabajadores en relación con sus datos personales, incluyendo los derechos ARCO (acceso, rectificación, cancelación y oposición).
- Medidas de seguridad implementadas para la protección de los datos personales.
- Mención, en su caso, de la transferencia de los datos personales a terceros.

Con esta información, los empleados pueden comprender adecuadamente el tratamiento de sus datos personales y ejercer sus derechos de manera apropiada.

**3. Monitoreo y vigilancia razonable**

Las prácticas de supervisión y vigilancia en el entorno laboral son habituales y sirven para garantizar la seguridad, mejorar la eficiencia de los procesos productivos y de servicios, y asegurar el cumplimiento normativo de las regulaciones vigentes. Sin embargo, es indispensable establecer un equilibrio entre la seguridad empresarial y el respeto al derecho de privacidad de los trabajadores.

Para empezar, como se ha mencionado anteriormente en este artículo, existe una diferencia sutil pero significativa entre privaci-

dad e intimidad. La privacidad se refiere al derecho de una persona a controlar quién tiene acceso a su información personal y cómo se utiliza; la intimidad, por otro lado, se refiere al ámbito más privado de la vida de una persona, incluyendo sus pensamientos, sentimientos, relaciones personales y actividades privadas. La privacidad se centra en el control sobre la información personal, mientras que la intimidad abarca aspectos más profundos y privados.

Una de las formas de lograr este equilibrio es utilizar técnicas de monitoreo para fines legítimos del trabajo contratado, establecer límites y fronteras en la vigilancia y mantener una cultura empresarial que proteja la privacidad de los trabajadores.

El uso de técnicas de monitorización como cámaras de seguridad, sistemas de seguimiento de computadores, análisis de comunicaciones electrónicas, geolocalización en teléfonos móviles y cualquier otra forma de monitorización o seguimiento debe estar justificado para fines legítimos y específicos. No obstante, en ocasiones, es justificable buscar alguna garantía de seguridad en el lugar de trabajo y la prevención del uso indebido de los recursos que ha proporcionado la empresa, el cumplimiento de los requisitos jurídicos y normativos, así como el control y la mejora de la productividad y la eficiencia. Algunos de estos controles son necesarios para medir la cantidad, la calidad y los tiempos de las tareas encomendadas.

Sin embargo, a pesar de la importancia del monitoreo para estos fines, también es indispensable establecer los límites y las restricciones necesarias para proteger la privacidad, la dignidad y la intimidad de las personas trabajadoras y garantizar que estas herramientas se utilicen de manera ética y responsable.

Entre las restricciones y límites de la vigilancia empresarial, se deben observar principios fundamentales, como el de pro-

porcionalidad. Del mismo modo que los datos privados que se solicitan al trabajador deben ser proporcionales al servicio contratado, las medidas de vigilancia también deben ser adecuadas al propósito perseguido, sin ser excesivas o intrusivas. Las empresas deben evitar, siempre que sea posible, el monitoreo constante y generalizado que no esté justificado para la mejor prestación del servicio. Los empleadores tienen la obligación de ser transparentes e informar a los trabajadores que están siendo monitoreados sobre la forma y el tiempo en que se realiza el monitoreo y la manera en que se utilizarán los datos recopilados.

Además, los trabajadores deben tener derecho a acceder a la información recopilada y la posibilidad de corregir o aclarar cualquier inexactitud en esos datos. Es trascendental evitar el monitoreo en áreas o actividades que puedan considerarse privadas, íntimas o sensibles, como conversaciones personales, actividades de aseo personal o hechos que ocurran fuera del horario laboral.

Es indispensable mantener el equilibrio entre la seguridad empresarial, el control de la productividad y el respeto a la privacidad. El ambiente laboral se beneficiará enormemente del cumplimiento de este equilibrio. Para lograrlo, las empresas deben implementar medidas de seguridad eficaces, como políticas de acceso y uso de datos, controles de seguridad en sistemas informáticos y formación en seguridad para los trabajadores, sin comprometer la privacidad de ninguno de ellos.

Una cultura empresarial que valore y proteja la privacidad de los empleados, que fomente la confianza y el respeto mutuo, tiende a crear círculos virtuosos. Por ese motivo, es necesario involucrar a los trabajadores en la creación y el desarrollo de políticas de privacidad, sensibilizándolos y estableciendo canales de comuni-

cación pertinentes para que puedan plantear sus inquietudes y denunciar violaciones a su privacidad de manera confidencial.

**4. Auditorías y cumplimiento normativo**

La realización de auditorías, ya sean externas o internas, para evaluar el cumplimiento legal en materia de privacidad laboral es una práctica común y también es fundamental para garantizar que las empresas operen dentro del marco de la ley, con ética y transparencia, y de acuerdo con lo dispuesto por las diferentes leyes aplicables.

Las auditorías en materia de privacidad laboral se enfocan en considerar diferentes aspectos, como la elaboración de las políticas de privacidad, los procedimientos que de ellas emanen y las implicaciones prácticas según la normativa jurídica establecida para los empleadores y en protección de los trabajadores.

Las auditorías suelen incluir, dentro de su desarrollo, una evaluación de políticas. Estas se revisan para asegurarse de que, en materia de privacidad y seguridad de datos, se encuentran debidamente alineadas con las leyes, las normas y los reglamentos. Las auditorías también suelen incluir un análisis de procedimientos en el que se verifica la recolección, el uso, el almacenamiento y, en su caso, la eliminación de los datos personales, asegurándose, por supuesto, de que se lleve a cabo conforme a derecho. De la misma manera, las auditorías deben revisar los controles de seguridad que se impongan y verificar que los controles de seguridad tecnológica y organizativa aplicados para proteger la información personal de los trabajadores sean eficaces y no hayan sido vulnerados. Por último, las auditorías pueden hacerse en relación con el cumplimiento de las normativas de privacidad laboral establecidas por las autoridades encargadas de inspeccionar estos aspectos.

Cuando las realizan entidades independientes, estas auditorías se consideran externas y aportan una perspectiva imparcial, objetiva y experta sobre el cumplimiento normativo. Pueden ser requeridas por regulaciones específicas o porque los clientes así lo exijan y buscan garantizar la protección de los datos. Existen organizaciones en las que los sindicatos cumplen un papel importante en todo el proceso de obtención, consentimiento y auditoría de los datos personales de los trabajadores.

El proceso de mejora continua, basado en los resultados de las auditorías, es uno de los principales beneficios que se obtienen, dada su contribución a la optimización de las políticas y prácticas de privacidad de una empresa. Los resultados de las auditorías proporcionan información muy valiosa sobre las áreas de mejora, las oportunidades, las amenazas, las debilidades y las fortalezas en el manejo de los datos personales.

Basándose en estos resultados, las empresas pueden implementar correcciones y medidas preventivas, lo cual puede incluir actualizaciones en las políticas empresariales, una mayor capacitación para los trabajadores y mejoras en el hardware o software utilizado.

Para garantizar un manejo efectiva de la privacidad laboral, las empresas deben desarrollar un sistema integral de gestión de la privacidad que abarque:

- Políticas y procedimientos claros.
- Formación y sensibilización continuadas.
- Monitoreo y evaluación constantes.
- Gestión de incidentes.
- Revisión y actualización periódicas del sistema de gestión de la privacidad.

La implementación adecuada de este sistema no solo facilita el cumplimiento normativo, sino que también promueve una cultura de respeto y protección de la privacidad en toda la organización.

**5. Retención y eliminación de datos personales**

Dentro de las políticas de protección de datos personales, es muy útil incluir un apartado específico que aborde la retención de datos, la implementación de procedimientos para la eliminación de información personal y el cumplimiento de las regulaciones regionales e internacionales.

Las políticas de retención de datos deben establecer los periodos de tiempo durante los cuales la información personal de los empleados permanecerá almacenada y segura antes de ser eliminada. Estas políticas deben basarse en factores como la naturaleza de la información, su relevancia para los fines operativos de la empresa y para el cumplimiento de aspectos legales y fiscales de acuerdo con las leyes aplicables.

Al desarrollar estas políticas, las empresas deben considerar aspectos críticos, como el tipo de datos que van a tratar, identificando con precisión los que se recopilan y determinando el tiempo de retención según su utilidad y propósito. También es necesario tener en cuenta los aspectos legales, identificando los requisitos que deben cumplirse según las regulaciones locales y globales que establecen periodos específicos para la retención de ciertos tipos de información, como datos médicos, fiscales y laborales.

Adicionalmente, se debe evaluar el riesgo asociado a la retención prolongada de datos personales y adaptarlo a las necesidades operativas y legales de la empresa. Es de suma importancia considerar el consentimiento y los derechos de los empleados, y

garantizar que estén al corriente de los períodos de retención de sus datos personales, así como respetar sus derechos de acceso y rectificación.

En el proceso de eliminación segura de información personal, cuando los datos ya no son necesarios para los fines para los que fueron recopilados, se deben seguir los siguientes pasos:

En primer lugar, se deben identificar los datos obsoletos que ya no sean necesarios o relevantes para los fines operativos o legales de la empresa. Luego, se deben emplear métodos de eliminación seguros y efectivos, como la destrucción física de documentos o la eliminación irreversible de archivos digitales mediante programas especializados. Al finalizar el proceso, se debe mantener un registro detallado de los datos eliminados cuando sea necesario, garantizando la confidencialidad de la información recabada.

Por último, pero no menos importante, se debe notificar al empleado la eliminación de sus datos, respetando escrupulosamente sus derechos laborales y de confidencialidad de la información.

El cumplimiento de la normativa nacional e internacional sobre retención y eliminación de datos personales es un requisito ineludible para garantizar la privacidad de los trabajadores y evitar posibles consecuencias económicas sancionadoras. Algunas de estas regulaciones incluyen:

- El Reglamento General de Protección de Datos en la Unión Europea.
- La Ley de Protección de Datos Personales en Estados Unidos.
- La Ley Federal de Protección de Datos Personales en Posesión de Particulares en México.

Es esencial respetar tanto las regulaciones laborales que establecen periodos específicos para la retención de ciertos tipos de información de los empleados, como los registros de pago de salarios, contratos, solicitudes de empleo, capacitaciones o evaluaciones del desempeño, así como cualquier otro documento que deba conservar el empleador.[6] También se debe tener en cuenta lo pactado en los convenios o contratos colectivos laborales que pudieran estar en vigor.

Por ejemplo, según la jurisprudencia expresada en la tesis aislada de la Suprema Corte de Justicia de la Nación en México, titulada «Estipulaciones que debe contener el Contrato Colectivo de Trabajo», se permite que en el contrato colectivo se establezcan otras disposiciones acordadas por las partes, independientemente de las obligatorias.

El artículo 47 de la Ley Federal del Trabajo establece las estipulaciones que deben contener los contratos colectivos de trabajo, fijándose, en las cuatro primeras fracciones, las condiciones necesarias que en todo contrato colectivo deben establecerse, que son el monto de los salarios, las horas de trabajo, la intensidad y calidad del trabajo, así como los descansos y vacaciones; es decir, las obligaciones especificadas anteriormente deben formar parte indispensable de todo contrato colectivo. La fracción V del artículo mencionado establece que en el contrato colectivo se fijarán las demás estipulaciones que convengan las partes. Esta disposición debe interpretarse en el sentido de que, independientemente de las obligaciones contenidas en

---

6 Federico Anaya, *Ley Federal del Trabajo comentada* (Ciudad de México: Editorial Valdepeña, 2024).

las primeras fracciones, que son de carácter obligatorio, a nadie puede imponerse obligación alguna con la que no esté de acuerdo voluntariamente, siempre que no esté fijada en la ley o establecida consuetudinariamente en la empresa.

### 6. Privacidad y tecnología del futuro en el trabajo

El rápido avance de la tecnología en el ámbito laboral plantea todo un conjunto de retos en cuanto a la protección de la privacidad de los trabajadores.

Las tecnologías emergentes, como la inteligencia artificial, el internet de las cosas (IoT), la analítica de datos y la biometría, los algoritmos artificiales (entendidos como un conjunto de instrucciones u operaciones que permiten procesar datos para ofrecer resultados), los robots, los programas informáticos, las plataformas digitales y las nuevas tecnologías de la información y la comunicación han transformado radicalmente la forma en que se llevan a cabo las actividades laborales. Estas tecnologías ofrecen grandes beneficios en términos de modernización, productividad, eficiencia, personalización de servicios y reducción de tiempos, pero también plantean desafíos significativos en cuanto a la privacidad y la seguridad de los datos personales de las personas y, en concreto, de los trabajadores.

Las tecnologías emergentes pueden suponer un desafío importante para la privacidad laboral. Los programas espía y las cookies, que son archivos que almacenan información en nuestros dispositivos y que el 99.99 % de las páginas web utilizan con fines de mercadotecnia, suponen una preocupación importante. Por ello, es necesario adaptar las políticas a las tendencias tecnológicas y a las consideraciones éticas que deben guiar la imple-

mentación de nuevas tecnologías. Este aspecto es fundamental y debe observarse con detenimiento.[7]

Un aspecto en el que se nota el impacto de estas tecnologías es la recopilación masiva de datos. Las tecnologías emergentes permiten compendiar con un solo clic grandes cantidades de datos personales de los trabajadores, entre ellos, el lugar de residencia, los patrones de comportamiento y los datos biométricos. El uso de algoritmos de inteligencia artificial para analizar datos también permite crear perfiles detallados de los empleados, lo que podría dar lugar a discriminaciones en el proceso de contratación basadas en características como el color de la piel, la edad o el lugar donde realizaron sus estudios.

En el Internet de las Cosas (IoT), los dispositivos físicos integrados con sensores, sistemas ciberfísicos, software y otras tecnologías conectadas a través de Internet permiten el monitoreo constante de las actividades laborales. Esta característica podría generar muchísimo estrés laboral debido a la invasión de la privacidad y la vigilancia excesiva. Estos dispositivos pueden ser objetos cotidianos como electrodomésticos (lavadoras, neveras, licuadoras, aspiradoras), dispositivos de entretenimiento (teléfonos, altavoces), dispositivos de seguridad (puertas, focos), vehículos, drones, dispositivos médicos o componentes de edificios inteligentes. Todos estos artefactos pueden comunicarse entre sí y vienen provistos de sistemas informáticos para realizar funciones específicas.[8]

---

7 Roberto Arenas Lara, *Privacidad personal vs. transparencia de datos* (Ciudad de México: Universo de Letras, 2023).

8 Redacción de Oracle, «¿Qué es el IoT?». Recuperado de: *https://www.oracle.com/*

Por último, la proliferación de dispositivos conectados y la transferencia de datos a través de redes exponen a las empresas a riesgos de ciberseguridad, que podrían afectar la privacidad de los empleados. De igual manera, los trabajadores se enfrentan a riesgos cibernéticos que podrían comprometer la privacidad de la empresa.[9]

Ante estos desafíos, las empresas deben adaptar sus políticas de privacidad y seguridad a las tecnologías emergentes. Esto implica evaluar los riesgos asociados con la adopción de nuevos conocimientos, así como revisar y actualizar constantemente las políticas de privacidad y seguridad para abordar los últimos cambios tecnológicos y los riesgos inminentes que puedan surgir. En definitiva, es necesario proporcionar formación y capacitación continua a los trabajadores sobre el uso responsable de las tecnologías.

Además, es importante implementar mecanismos efectivos para obtener el consentimiento informado de los empleados cuando se introduzcan nuevas tecnologías. También se debe priorizar la protección de datos sensibles mediante el establecimiento de medidas adicionales de seguridad, como en el caso de los datos médicos o biométricos, así como los datos de preferencias, geolocalización y comportamiento, antes de que se recopilen y procesen los datos personales.[10]

---

*mx/internet-of-things/what-is-iot/*

[9] Flavio Suárez-Muñoz (comp.), *Internet de las cosas e inteligencia artificial: los retos regulatorios y éticos del extractivismo de datos, la privacidad y los derechos humanos* (Morelia: IoT CiberSec, 2024).

[10] Future of Privacy Forum, *Privacy and Emerging Technologies*. Recuperado de: https://fpf.org/issues/privacy-emerging-technologies/ Última consulta: 3 de abril de 2024.

## 7. Conclusiones

El rápido avance de la tecnología en el ámbito laboral plantea numerosos retos en cuanto a la protección de la privacidad de los trabajadores. Por esta razón, es indispensable implementar políticas transparentes que garanticen no solo el derecho individual y colectivo del trabajador, sino también los del empleador, así como la construcción de un clima laboral eficiente y adecuado.

Las políticas de privacidad deben estar fundamentadas en la ley, la ética, la moral y las buenas costumbres para así garantizar la protección de los datos personales. Esto implica definir los datos que se van a tratar, recopilar, procesar y, en su caso, destruir. Dentro de estas políticas, se deben establecer mecanismos para proteger la confidencialidad de los datos, negar el acceso a personas no autorizadas y prevenir la pérdida o robo de información.

Las políticas de privacidad deben definir claramente los derechos y obligaciones de los trabajadores. Al mismo tiempo, es fundamental proporcionar a los empleados los elementos imprescindibles para gestionar esos datos, lo que implica ofrecer capacitación e instrucciones específicas sobre la información que se va a facilitar. Además, es necesario establecer la prohibición de intercambiar datos personales sin autorización del empleador, con el fin de evitar posibles brechas de seguridad que puedan poner en riesgo la información tanto de la empresa como de los empleados.

En el contexto de las tecnologías emergentes, la protección de los datos de los trabajadores en posesión de los empleadores debe adaptarse constantemente para hacer frente a los retos de un mundo cada vez más tecnológico. Hay que evaluar tanto los riesgos evidentes como los ocultos asociados con la adopción de estas nuevas tecnologías para garantizar la privacidad de los empleados.

La protección de los datos personales es y seguirá siendo tan crucial como la innovación tecnológica.

**Bibliografía**


Anaya, Federico, *Ley Federal del Trabajo comentada* (Ciudad de México: Editorial Valdepeña, 2024).

Arenas Lara, Roberto, *Privacidad personal vs. transparencia de datos* (Ciudad de México: Universo de Letras, 2023).

Davara F. de Marcos, Isabel (coord..), *GPS. Protección de datos personales en el sector privado* (Ciudad de México: Editorial Tirant Lo Blanch y Davara Abogados), 2020.

Massa, Roberto, *Planeación estratégica de los datos personales: del diagnóstico al plan de trabajo* (Ciudad de México: Aldo Mauricio Massa y Amazon Publishing, 2021).

Parra Noriega, Luis Gustavo, *Hacia una nueva autoridad especializada en protección de datos personales en México* (Ciudad de México: Editorial Tirant Lo Blanch, 2022).

Piñar Mañas, José y Lina Ornelas Núñez (coords.), *La protección de datos personales en México* (Ciudad de México: Editorial Tirant Lo Blanch, 2013).

Rosales, Mariano Carlos, *Prontuario de protección de datos personales* (Ciudad de México: Aqua Ediciones, 2016).

**Reglamentos y Leyes**

Reglamento General (UE) 2016/679, de 27 de abril, de protección de datos. Parlamento Europeo, Consejo de la Unión Europea. https://gdpr-info.eu/

Ley Federal 2023, de 04 de octubre, de Protección de Datos Personales en Posesión de los Particulares.

**Páginas de Internet**

Future of Privacy Forum, *Privacy and Emerging Technologies.* Recuperado de: https://fpf.org/issues/privacy-emerging-technologies/ Consultada el 14 de marzo de 2024.

Information Commissioner's Office (ICO), *Understanding Consent in Data Protection.* Recuperado de: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/understanding-consent/

OpenAI. (2024, marzo 14). [Conversación con ChatGPT]. (ChatGPT es el nombre del autor en este caso, y la fecha es la fecha en que se realizó la conversación).

Privacy Rights Clearinghouse, *Employee Monitoring: Is There Privacy in the Workplace?* Disponible en: https://privacyrights.org/resources/employee-monitoring-there-privacy-workplace

Privacy Rights Clearinghouse, *The Growing Importance of Corporate Privacy Policies*. Disponible en: https://privacyrights.org/resources/growing-importance-corporate-privacy-policies

Redacción de Oracle, «¿Qué es el IoT?». Recuperado de: https://www.oracle.com/mx/internet-of-things/what-is-iot/

Suárez-Muñoz, Flavio (comp.), *Internet de las cosas e inteligencia artificial: los retos regulatorios y éticos del extractivismo de datos, la privacidad y los derechos humanos* (Morelia: IoT CiberSec, 2024).

TrustArc, *Data Privacy Audits: Best Practices and Compliance Tips*. Disponible en: https://www.trustarc.com/resources/data-privacy-audits-best-practices-compliance-tips/

U.S. National Archives and Records Administration, *Data Retention Policies and Procedures*. Disponible en: https://www.archives.gov/records-mgmt/policy/data-retention.html

CAPÍTULO VI

# Una agenda para el futuro: algunas conclusiones

**Luz Angela Cardona Acuña**
Coordinadora de especialistas de las Comisiones Americanas de Seguridad Social
Conferencia Interamericana de Seguridad Social

La privacidad es un derecho fundamental e inherente a la dignidad humana que protege la esfera íntima de las personas. Desde su aparición, refleja la preocupación por la injerencia en la vida privada por parte de diversos actores sociales. A pesar de su reconocimiento pleno en la era digital, se vuelve a debatir sobre su realización, especialmente en el contexto laboral, tema central de *Privacidad y trabajo*.

Los instrumentos internacionales de ámbito universal, americano y europeo han reconocido este derecho, ya sea como derecho a la intimidad o como privacidad, y cada región utiliza un énfasis diferenciado para definirlo. La Organización Internacional del Trabajo (OIT) lo ha incluido como parte de los derechos de las personas trabajadoras y del trabajo digno. Sin embargo, a pesar del desarrollo del derecho internacional de los derechos humanos, no todos los países de las Américas cuentan con políticas adecuadas para su regulación. Muchas de las legislaciones no definen adecuadamente las restricciones legítimas,

proporcionales y ajustadas a objetivos justificados, ni la finalidad y necesidad de dichas restricciones, lo que se traduce en una preocupante falta de estabilidad jurídica.

Ante esta realidad, queda en evidencia que el catálogo de derechos laborales no contempla la vida privada (privacidad e intimidad). Por este motivo, es importante que se establezcan instancias de queja y solución de controversias, así como mecanismos efectivos de protección, vigilancia y fiscalización de datos personales. La privacidad en el lugar de trabajo es un aspecto fundamental de la dignidad humana y debe abordarse desde la perspectiva de los derechos humanos. Si bien los derechos laborales abarcan diversas protecciones para las personas trabajadoras, la cuestión de la privacidad a menudo requiere un enfoque matizado. En el panorama tecnológico actual, que cambia rápidamente y donde el teletrabajo se ha vuelto cada vez más común, los límites entre la vida personal y la profesional pueden difuminarse con facilidad. Cuando se trata de privacidad en el lugar de trabajo, entran en juego consideraciones de intimidad. Las personas tienen derecho a mantener un nivel de discreción en su vida personal que los empleadores deben respetar. Esto incluye proteger la información personal, garantizar la confidencialidad y proteger contra vigilancia o monitoreo injustificados.

En la actualidad, las nuevas tecnologías tienen una gran capacidad para recolectar y almacenar información personal, lo que pone en riesgo el derecho a la privacidad. Esta información ha adquirido un valor significativo para las empresas a la hora de tomar decisiones. El volumen de datos que se genera a diario por persona excede la capacidad de vigilancia y regulación de los Estados y las empresas. Los cambios tecnológicos han trans-

formado la relación laboral con la aparición del teletrabajo y el trabajo en plataformas, así como la capacidad y los tipos de control que un empleador puede ejercer sobre sus trabajadores en términos de procesos, rutinas y productividad.

A medida que los avances tecnológicos continúan remodelando la forma en que trabajamos, es esencial que las leyes laborales se adapten a estos cambios. El teletrabajo, por ejemplo, plantea desafíos únicos en términos de privacidad. Los empleadores pueden tener acceso a información personal y confidencial cuando los empleados trabajan de forma remota, lo que genera preocupaciones sobre la seguridad de los datos y las transgresiones de la privacidad. En este contexto, resulta cada vez más importante establecer directrices para proteger los derechos de privacidad en las modalidades de teletrabajo. Esta premisa va de la mano de la implementación de medidas de comunicación segura. La necesidad de que las empresas cuenten con una debida trazabilidad del teletrabajo no debe ser una condición que comprometa el respeto a la vida privada de las personas. Se requiere responsabilidad y ética en la implementación de cualquier tecnología de monitoreo.

La garantía del derecho a la privacidad en el entorno laboral debe estar en equilibrio con el interés legítimo de las empresas en manejar información relevante para el desarrollo de sus actividades. Las empresas e instituciones necesitan contar con normas que delimiten su ámbito de actuación. En el mismo sentido, deben desarrollar capacidades para implementar acciones que protejan al trabajador y hagan uso de información que contribuya a su actividad. La rendición de cuentas empresarial, o *accountability* en inglés, es un pilar fundamental para diseñar y adoptar políticas sobre protección de datos personales.

Desde otra perspectiva, las empresas deben disponer de información que les permita cumplir con los estándares de prevención y erradicación de la corrupción, gran parte de la cual deriva del acceso a datos personales de las personas trabajadoras. Asimismo, en cuanto al acceso a las tecnologías, las empresas deben conocer a fondo las cláusulas y los términos de uso. Enfrentar los desafíos tecnológicos mediante políticas y regulaciones efectivas es una forma de generar entornos laborales justos y equitativos.

La responsabilidad de las personas trabajadoras en este marco incluye: cuidar su información personal en la vida cotidiana; concienciarse sobre el uso de su información personal en el ámbito laboral; negociar colectivamente cláusulas de protección del derecho a la privacidad en el marco de un trabajo digno; y dar su consentimiento libre e informado para aceptar estas regulaciones. Desde la perspectiva del trabajador, la protección contra arbitrariedades y el uso inadecuado de la información está directamente relacionada con la estabilidad en el empleo, la ayuda contra el acoso laboral y la tutela contra los abusos patronales.

En este contexto, se hace evidente la necesidad de establecer protocolos que regulen la relación entre el derecho al trabajo y la privacidad. Estas normativas deben tomar en consideración diversos factores, como el tamaño, el sector y la actividad económica de las empresas, así como los distintos procesos inherentes al mundo laboral. Entre estos figuran:

a) La prestación de servicios laborales.
b) Los mecanismos de control de las personas trabajadoras, como el uso de tecnologías biométricas, dispositivos móviles, vehículos o correos electrónicos institucionales.
c) El uso de información personal en sistemas automatizados.

d) La clasificación de datos personales, como registros médicos, financieros o familiares.
e) El uso de redes sociales para el control o sanción de los empleados.
f) El reconocimiento de la relación entre estos aspectos y la promoción de entornos laborales saludables y seguros.

Estas normativas deben diseñarse de manera que protejan los derechos de los trabajadores y de las empresas, fomentando un equilibrio justo y respetuoso en el ámbito laboral.

Se reconoce la necesidad de establecer elementos de gobernanza en el seno de las empresas e instituciones para asegurar los derechos humanos de las personas trabajadoras, al tiempo que se equilibran con políticas destinadas a salvaguardar la seguridad de la información en los lugares de trabajo. Hay que subrayar la importancia de contar con mecanismos que atiendan quejas y resuelvan disputas en caso de violaciones de las normas y directrices de privacidad. Por ese motivo, debe prestarse especial atención a la transparencia en la recopilación y el almacenamiento de datos, así como a la clarificación de los propósitos de dicha información y, llegado el caso, a la destrucción o eliminación de ese acervo. La implementación y comunicación efectiva de estos procesos no solo protege los derechos individuales y colectivos de los trabajadores en el entorno laboral, sino que también garantiza la continuidad operativa de las empresas e instituciones en lo referente a datos personales.

El respeto a la privacidad, el adecuado tratamiento de los datos personales y la protección de la información empresarial o institucional son fundamentales para mantener la confianza entre empleadores y trabajadores. La violación de la privacidad puede minar la confianza en el lugar de trabajo y generar una ruptura

en la comunicación y la colaboración. Por el contrario, el respeto a la privacidad puede fomentar un ambiente laboral positivo en el que los empleados se sientan valorados y respetados.

Cuando los empleados perciben que su privacidad está protegida, es más probable que se comprometan activamente con su trabajo y contribuyan al éxito general de la empresa. Esto, a su vez, puede impulsar la moral y la productividad de los empleados, lo que beneficia tanto al personal como a la compañía.

Las empresas deben ser completamente transparentes en cuanto a sus prácticas de recopilación de datos. La información que proporcionen debe ser adecuada para abordar las preocupaciones sobre privacidad. Al ser claras sobre los tipos de datos que recopilan y los propósitos para los que se utilizan, las empresas garantizan que las personas estén plenamente informadas sobre el manejo de sus datos. Esta transparencia permite a los empleados tomar decisiones informadas sobre su privacidad y otorgar su consentimiento a las prácticas de recopilación de datos.

Además, la transparencia no solo contribuye a crear una cultura sólida de prevención de incidentes y protección de datos, sino que también fomenta la reciprocidad y la corresponsabilidad en el uso de la información institucional. Todo esto, combinado, ayuda a reducir el riesgo de filtración o uso indebido de los datos por parte de los propios trabajadores.

Aunque esta obra aborda las reflexiones más actuales sobre el tema, quedan pendientes otros aspectos que requieren una mayor consideración, tales como:

a) La evidencia del cumplimiento de la responsabilidad proactiva.
b) El uso de herramientas como los Project Impact Assessment.

c) El uso de herramientas de privacidad, seguridad y ética por diseño.
d) El uso y la regulación de los correos electrónicos institucionales.
e) La regulación de la privacidad en el campo del teletrabajo.
f) El uso de plataformas digitales basadas en geolocalización.
g) Las comunicaciones por WhatsApp, Telegram y el hackeo de perfiles.
h) Las tecnologías emergentes.
i) La vigilancia en el lugar de trabajo y la ciberseguridad.
j) La responsabilidad social corporativa.
k) La regulación internacional de empresas transnacionales.
l) La cultura de la privacidad y el respeto mutuo en el trabajo.
m) La resolución de conflictos sobre estos temas.
n) Las medidas de reparación y sanción cuando se produce daño.
o) Las regulaciones diferenciadas para los sectores público y privado.

Uno de los aportes más significativos de esta obra para el público interesado en la seguridad social en general, y para su membresía en particular, es el reconocimiento de que el derecho a la vida privada debe formar parte integral del catálogo de derechos laborales. La privacidad y la intimidad deben ser garantizadas tanto por el Estado como por particulares, en sus respectivos ámbitos de competencia como sujetos obligados en el marco de esta interrelación de derechos. Este principio es especialmente relevante en un contexto de aparición de nuevas tecnologías y su creciente uso en el ámbito laboral.

La interdependencia entre los derechos a la privacidad y los derechos laborales exige regulaciones adecuadas y actualizadas. Estas deben establecer normas fundamentadas, cuyas bases se encuentren en los principios del derecho internacional de los derechos humanos.

Ante la expansión de las tecnologías y las nuevas realidades laborales asociadas a este avance, surgen desafíos y oportunidades en el uso de la tecnología en el ámbito laboral, con implicaciones directas en la privacidad de los trabajadores. La relación laboral se está redefiniendo en múltiples aspectos debido a la digitalización, la deslocalización de la relación laboral y la implementación de tecnologías de monitorización del trabajo. El reto consiste en que el derecho laboral se adapte a estos cambios y a la consiguiente aparición de nuevos eventos y fenómenos que requieran su intervención.

Sin duda, ante cualquier implementación tecnológica, se debe prestar atención a los riesgos de gobernanza a los que se enfrentan las empresas y las instituciones. La privacidad de los trabajadores no es el único aspecto en peligro. También se deben considerar la ciberseguridad, la manipulación de información, la brecha digital, la dependencia tecnológica, el desempleo generado por la tecnología, la falta de habilidades y las condiciones laborales precarias, así como la discriminación algorítmica.

Quienes son responsables de la gobernanza deben promover la atención a estos riesgos y ser proactivos en la actualización de la normativa interna, así como en la capacitación continua del personal. Se debe poner un énfasis especial en las áreas de recursos humanos, ya que, dentro de la cultura de la organización, son los principales responsables del manejo de la información, la formación y el reclutamiento del personal.

Por otro lado, aunque puede haber ciertos puntos de acuerdo entre los empleadores y las personas trabajadoras sobre el tema, también se revelan diferentes posturas que deben tenerse en cuenta para elaborar y actualizar normativas, protocolos nacionales o corporativos y para negociar contratos colectivos de trabajo. En la actualidad, gran parte de las relaciones laborales comienzan con el intercambio y el almacenamiento de información personal de los trabajadores.

En los procesos de las empresas e instituciones, mucha de esta información recopilada se utiliza para orientar negocios, contratar proveedores y personal. De esta manera, la información se ha convertido en uno de los recursos más importantes para las empresas y la sociedad en general.

El derecho a la privacidad en el ámbito laboral es una cuestión sumamente compleja y multidimensional que requiere una cuidadosa consideración desde diversas perspectivas. Esta obra ofrece una visión de los derechos humanos, fundamentada en la corresponsabilidad y respaldada por sólidas medidas de gobernanza. Si bien es innegable la importancia de la privacidad para la autonomía individual, la dignidad y la protección de los datos personales, las empresas también deben equilibrar estas preocupaciones con la necesidad de seguridad, transparencia y cumplimiento normativo.

Encontrar un punto medio que respete los derechos individuales y, al mismo tiempo, satisfaga las necesidades operativas de las empresas es esencial para fomentar un entorno laboral seguro, saludable y ético. En última instancia, el debate sobre el derecho a la privacidad en el contexto empresarial continuará evolucionando a medida que avance la tecnología y cambien los valores sociales.

CAPÍTULO VII

# Recomendaciones para la acción

**María Teresa González Nava**
Especialista de la Comisión Americana Jurídico Social
Conferencia Interamericana de Seguridad Social

Una contribución significativa de esta obra, al provenir del ámbito técnico de las Comisiones Americanas de Seguridad Social, es la propuesta de una serie de recomendaciones que establezcan un marco modelo para los países de habla hispana miembros de la Conferencia Interamericana de Seguridad Social. Este marco deberá abarcar los derechos tanto de las personas trabajadoras como de las empresas, basándose en una información común que ambas partes deben poseer para mantener un equilibrio adecuado entre la privacidad y el trabajo.

Es importante destacar que este documento marco deberá ser revisado y complementado a medida que se analicen los temas pendientes de reflexión presentados en esta misma obra y, por supuesto, los nuevos elementos que puedan surgir en esta *era* de la digitalización, tal como han señalado los distintos autores.

No se puede pasar por alto que las instituciones de naturaleza pública también pueden adoptar las recomendaciones presentadas aquí, teniendo en cuenta la legislación específica aplicable

a los trabajadores del Estado y a las entidades gubernamentales. Como se ha visto, es esencial mantener en todos los ámbitos una perspectiva de derechos humanos y una gobernanza que fomente entornos laborales seguros y productivos.

**Establecimiento de una política de privacidad**

- Todas las empresas e instituciones deben contar con una política de privacidad que establezca el tratamiento de datos personales. Esta política debe ser aplicable tanto a su personal como a proveedores y terceros relacionados. El área responsable de estos datos debe recabar el consentimiento correspondiente.
- La política de privacidad también debe justificar la necesidad de recabar determinados datos, en función del tipo de relación que se establezca. La transparencia de dicha política es indispensable. Uno de los componentes clave de una política eficaz de privacidad y protección es tener prácticas claras de recopilación de datos. Esto implica describir qué datos se recopilan de las personas y con qué propósito se utilizarán. Por ejemplo, una empresa puede especificar que recopila nombres de clientes y direcciones de correo electrónico con el fin de enviar ofertas promocionales y boletines informativos. Además, la política debe ofrecer transparencia sobre cómo se almacenan y comparten los datos, ya sea en servidores seguros o se compartan con terceros para fines específicos.
- Las políticas de privacidad deben garantizar un ambiente laboral y una cultura organizacional basados en la

confianza, el equilibrio y la cooperación, que favorezcan un ambiente adecuado de productividad laboral.

- A partir de la política de privacidad, se sugiere establecer mecanismos y protocolos que prevengan el abuso de poder por parte de los empleadores, incluyendo la justificación y fundamentación de las posibles restricciones o intervenciones en correos, cámaras, dispositivos, entre otros.

**Disposiciones laborales y contractuales específicas**

- Para garantizar la integridad de la información empresarial o institucional, las personas trabajadoras deberán suscribir un acuerdo específico de confidencialidad, que tendrá efecto incluso después de finalizar la relación laboral.
- Es esencial capacitar a las personas trabajadoras en protección de datos y ciberseguridad para evitar que se afecte el flujo de información dentro de la empresa, pero debe llevarse a cabo con las suficientes medidas de seguridad. Las organizaciones deben realizar sesiones de formación periódicas sobre las prácticas de protección de datos, resaltando la importancia de proteger la información confidencial y de seguir los protocolos de manejo. Al fomentar una cultura de privacidad de datos dentro de la organización, los empleados son más conscientes a la hora de salvaguardar los datos y están mejor preparados para identificar y responder a posibles amenazas a la seguridad. Por ejemplo, se les puede capacitar sobre cómo reconocer intentos de *phishing* o la

forma adecuada de manejar los datos de los clientes y/o usuarios para evitar el acceso no autorizado.

- La participación de las personas trabajadoras en el diseño de los procesos de la empresa o institución garantiza que cada uno identifique su responsabilidad con respecto a la información que maneje.
- Además, se debe fomentar el conocimiento, la aplicación y el monitoreo de la adopción de los estándares de protección de datos personales, basados en un equilibrio entre la empresa, las personas trabajadoras y proveedores.
- Las condiciones de teletrabajo y su trazabilidad deben estar establecidas en el contrato laboral y la normativa interna correspondiente. Cualquier medida adicional de supervisión y supervisión laboral debe ser comunicada de inmediato y con toda claridad.

**Medidas de seguridad de la información**

- Los sistemas de información utilizados en las empresas e instituciones, ya sean propios o contratados a terceros, deben someterse a evaluaciones de seguridad y auditorías periódicas para identificar vulnerabilidades y abordarlas con prontitud.
- Se recomienda el uso de técnicas de cifrado para el almacenamiento y la transmisión de datos. El cifrado convierte la información confidencial en un código que solo puede descifrarse con una clave, lo que proporciona una capa adicional de seguridad.
- Capacitar al personal encargado, especialmente al de Recursos Humanos, en el tratamiento y la protección de los datos personales.

- Identificar a los aliados y las estrategias de trazabilidad de procesos con las contrapartes internas y externas de la empresa.
- Definir directrices sobre el manejo de *cookies* durante la navegación, dado su alcance para la recopilación de datos personales.
- Proteger los derechos de los empleadores en relación con la seguridad de sus intereses, inversiones y patrimonio.

**Mecanismos de atención de quejas y solución de controversias**

- El documento de política de privacidad debe especificar el área responsable de atender las quejas relacionadas con el manejo de datos personales y el uso indebido de información institucional.
- El personal encargado de las instancias de queja y solución de controversias debe analizar la situación conforme a la normatividad interna, la legislación laboral vigente y con una perspectiva de derechos humanos.
- Estos mecanismos deben prever medidas sancionadoras y garantías de no repetición ante un posible uso indebido de información o filtración.

**Actualización constante de normatividad y políticas de privacidad**

- Realizar análisis del impacto de la adopción de nuevas tecnologías en el trabajo y la privacidad, e involucrar a los empleados en la toma de decisiones relacionadas con esos temas.
- Realizar estudios de derecho comparado sobre diferentes regulaciones para conocer diversas experiencias en la materia.

- Identificar y aplicar los mecanismos ya existentes para la regulación de la privacidad en el trabajo:
- Reglamento General de Protección de Datos de la Unión Europea (RGPD) de 2018.
- Guía de protección de datos por defecto de la Agencia Española de Protección de Datos (AEPD).
- Red Iberoamericana de Protección de Datos.
- Recomendaciones sobre la protección de los datos personales de las personas trabajadoras de la Organización Internacional del Trabajo (OIT).
- Observación General n.º 16. Comentarios generales adoptados por el Comité de los Derechos Humanos, artículo 17, Derecho a la intimidad.
- Principios rectores sobre las empresas y los derechos humanos.

## SOBRE LAS Y LOS AUTORES

### Federico Anaya Ojeda

Es un destacado abogado laboralista, administrador de empresas, maestro, doctor y doctorante, con una carrera multifacética y una sólida trayectoria en el ámbito jurídico y académico. Tiene una licenciatura en Derecho, un máster en Administración, un máster en Alta Dirección por la Universidad Europea de Madrid, es candidato a doctor en Derecho por la Universidad Anáhuac y la Universidad Complutense de Madrid, y ha sido reconocido como Doctor Honoris Causa por el Claustro Nacional de Doctores. Preside el bufete de abogados Anaya Valdepeña, fundado en 1932, y ocupa el cargo de presidente ejecutivo del Instituto Latinoamericano de Derecho del Trabajo y de la Seguridad Social (ILTRAS). Además, es asesor laboral de diversas cámaras. Es coordinador de la Comisión de Derecho de la Empresa en el Ilustre y Nacional Colegio de Abogados de México. Es profesor de posgrado en la Escuela Libre de Derecho y en el Instituto de Posgrado en Derecho. Ha sido conferenciante, catedrático y ponente en numerosas instituciones educativas, tanto nacionales como internacionales. Actualmente, es director general de la *Revista Laboral* y ha escrito diversas obras jurídicas. Su influencia se extiende a la dirección de EVA Editorial y la presidencia del consejo. Ha formado parte del sínodo para concursos de oposición para jueces de distrito y locales especializados en materia de trabajo.

### Luz Angela Cardona Acuña

Doctora en Investigación en Ciencias Sociales con mención en Sociología y maestra en Población y Desarrollo por la Facultad La-

tinoamericana de Ciencias Sociales (FLACSO) de México. Es especialista en Métodos de Análisis Demográfico por la Universidad Externado de Colombia y en Psicología por la Pontificia Universidad Javeriana de Colombia. De noviembre de 2019 a agosto de 2020, fue investigadora visitante en el Center for Cultural Sociology de la Universidad de Yale. En la actualidad, es coordinadora de especialistas de las CASS en la CISS. Anteriormente, ha trabajado en la Comisión de Derechos Humanos de la Ciudad de México y en el Programa Presidencial de Derechos Humanos y Derecho Internacional Humanitario de Colombia. Su experiencia incluye consultorías para la Unión Europea, el Instituto Interamericano de Derechos Humanos, la Agencia de Cooperación CIVIS y el Institute for Economics and Peace. Ha sido docente en programas de posgrado en la Universidad Autónoma de Guerrero, la Universidad Autónoma de Coahuila, el Centro de Investigaciones y Estudios de Género de la Universidad Nacional Autónoma de México, la Escuela Federal de Formación Judicial de México y FLACSO-México. Es miembro del Sistema Nacional de Investigadores e Investigadoras de México nivel I.

**Jorge Ulises Carmona Tinoco**

Abogado y académico mexicano, es doctor, maestro y licenciado en derecho en la UNAM, maestro en Derecho (LLM) con especialidad en Derecho Internacional de los Derechos Humanos por la Universidad de Essex (Inglaterra), especialista y maestro en Argumentación Jurídica por la Universidad de Alicante (España) y maestro en la misma disciplina por la Universidad de Palermo (Italia), diplomado en Amparo por la Universidad Iberoamericana y la Suprema Corte de Justicia de la Nación. Durante quin-

ce años colaboró en labores de protección interna e internacional de los derechos humanos en la Comisión Nacional de los Derechos Humanos (CNHD), la entonces Procuraduría General de la República y la Secretaría de Relaciones Exteriores. Desde 2002 es investigador en el Instituto de Investigaciones Jurídicas de la UNAM e investigador nacional nivel II por el Conacyt, así como profesor en el nivel de licenciatura y posgrado en la Facultad de Derecho de la UNAM. Es autor de más de 140 trabajos publicados sobre protección interna e internacional de los derechos humanos, argumentación e interpretación jurídicas. Fue defensor universitario en la UNAM (2012-2015) y sexto visitador general en la CNHD, a cargo de la promoción y protección de los DESCA (2015-2019).

**Gilbert Díaz Vásquez**

Es educador, dirigente sindical del Magisterio Nacional de Costa Rica, abogado y notario. Es licenciado en Derecho y en Gestión Educativa, y profesor de Educación General Básica. Ocupa la presidencia del Sindicato de Trabajadoras y Trabajadores de la Educación Costarricense (SEC); se ha desempeñado como representante laboral en la Junta Directiva y en la Asamblea de los Trabajadores del Banco Popular, así como en organismos corporativos y de la economía social solidaria en representación de los profesionales de la educación de Costa Rica, como la Junta de Pensiones y Jubilaciones del Magisterio Nacional (JUPEMA) y la Operadora de Pensiones Vida Plena. Es miembro de número y ha presidido la Junta Paritaria de Relaciones Laborales del Ministerio de Educación Pública de Costa Rica (JPRL-MEP). A nivel internacional, ha representado a los y las profesionales de la

educación de Costa Rica y Centroamérica en la Internacional de la Educación (IE) y en la Federación de Organizaciones Magisteriales de Centroamérica (FOMCA).

**María Teresa González Nava**

Es licenciada en Derecho, especialista en Derecho de Amparo y maestra en Gobierno y Políticas Públicas por la Universidad Panamericana. En el sector público, ha trabajado en derecho administrativo y presupuestario, siendo directora de Asuntos Financieros y subdirectora de Asuntos Jurídicos en la Secretaría de Hacienda y Crédito Público. Participó en la elaboración, ejecución y seguimiento de los Planes Nacionales de Desarrollo 2013-2018 y 2019-2024. Además, coordinó agendas legislativas en el Congreso de la Unión y en las legislaturas locales. En seguridad pública, fue jefa de Oficina de la Coordinación del Sistema de Desarrollo Policial de la Comisión Nacional de Seguridad, gestionando recursos humanos, financieros y materiales. En el sector privado, tiene experiencia en derecho fiscal, financiero y corporativo; planeación estratégica; resolución de conflictos y prevención de riesgos; transparencia y protección de datos personales; control interno; anticorrupción y *compliance* en general. Ha trabajado en Sesma, Sesma & McNeese y Legalance. Además, ha colaborado en informes y acciones de derechos humanos en México con la organización Red TDT «Todos los derechos para todas y todos».

**Stella Vanegas**

Abogada por la Universidad Javeriana, especialista en Legislación Financiera por la Universidad de los Andes, especialista en Derecho Comunitario por la Universidad de Alcalá y LLM en Leyes por

la Universidad de Lovaina. Socia fundadora de Vanegas Morales Consultores desde el año 2013 y profesora de la especialización en Derecho Comercial de la materia «Datos personales». Desde 2015 es miembro de IAPP (International Association of Privacy Professionals) Co-Chair del Knowledge Net Chapter de IAPP para Colombia para el periodo 2020-2021 y 2023-2024, y es Chair del Capítulo LATAM de Privacy Rules desde 2020, así como se desempeñó como directora de ADAPRI (Asociación Colombiana de Datos y Privacidad) y en la actualidad es miembro de su Comité Directivo.

**María Villa Fombuena**

Doctora en Derecho por la Universidad de Sevilla. Es profesora titular de Derecho del Trabajo y de la Seguridad Social del Centro Cardenal Spínola CEU, adscrito a la Universidad de Sevilla, institución en la que también ejerce como profesora adscrita al Departamento de Derecho del Trabajo y de la Seguridad Social. Es coordinadora del Máster en Big Data & Business Analytics de la Universidad Pablo de Olavide desde el año 2015, en el que igualmente es la responsable de la materia relativa a la protección de datos; y delegada de Protección de Datos desde el año 2018. En 2023 fue nombrada miembro colaborador de la ELA (European Labour Authority). Asimismo, la profesora Villa es autora de diversas publicaciones de alto impacto y evaluadora externa de varias revistas nacionales e internacionales.

Este libro se terminó de imprimir en los talleres de Grupo Fogra SA de CV, el mes de noviembre de 2024. Se tiraron 278 ejemplares, más sobrantes para reposición. Cuidaron de la edición: Luz Angela Cardona Acuña y María Teresa González Nava, eds.