UNIVERSIDAD ESAN

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

CARRERA DE DERECHO CORPORATIVO

"La protección de datos personales de los trabajadores frente al uso de tecnologías de monitoreo GPS y videovigilancia en el entorno laboral"

Trabajo de Suficiencia Profesional presentado en satisfacción parcial de los requerimientos para obtener el título profesional de Abogado

AUTORES

Urrutia Zamalloa, Julio Brandon

Valencia Castillo, Rosaluz

ASESOR

Costa Gálvez, Jean Carlo

ORCID N°0000-0001-7831-5959

Lima, Octubre del 2024

VERSIÓN SUSTENTABLE DE TSP 2024.pdf

INFORME DE ORIGINALIDAD

2%	2%	5%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Zamudio Salinas, Maria de Lourdes. "El Derecho a la Proteccion de Datos Personales de los Trabajadores Frente al Control Laboral a Traves del Sistema de Geolocalizacion GPS. Limites y Propuestas", Pontificia Universidad Catolica del Peru - CENTRUM Catolica (Peru) Publicación	1%
2	www.spdtss.org.pe Fuente de Internet	1%
3	revistas.pucp.edu.pe Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

AGRADECIMIENTOS

A nuestra familia, cuya fortaleza y amor incondicional han sido pilares fundamentales en nuestro camino. Agradecemos el constante apoyo y la confianza brindada en cada uno de nuestros proyectos, así como la inspiración que nos motiva a seguir adelante en nuestras metas.

A quienes nos han guiado en nuestra formación, por inculcarnos los valores esenciales de nuestra profesión y proporcionarnos las herramientas necesarias para enfrentar los desafíos académicos y personales. Agradecemos también a nuestro asesor, el docente Jean Carlo Costa Gálvez, quien siempre asumió un rol proactivo y servicial en la construcción de este trabajo.

Su colaboración ha sido crucial para el desarrollo de este trabajo, que busca arrojar luz sobre la protección de datos personales y el uso de medios tecnológicos, resaltando la importancia de garantizar la privacidad y seguridad en un entorno laboral.

ÍNDICE DE CONTENIDOS

RESUMEN

A partir del actual proceso de revolución tecnológica se han originado nuevas formas de trabajar, subordinar y depender. Con relación a esta última, es importante señalar que el empleador tiene la facultad fiscalizadora, por la cual puede ejercer control sobre las actividades de sus trabajadores. El uso de nuevas tecnologías con el propósito de fiscalizar a los trabajadores ya es una realidad, por ello esta investigación está dirigida a establecer límites en el uso y tratamiento de datos personales con relación a la fiscalización mediante nuevas tecnologías, analizando la normativa vigente en dicha materia con la finalidad de demostrar que aquella no contempla varios supuestos en los cuales se incurre en un uso indiscriminado de datos personales, vulnerando el derecho a la privacidad de los trabajadores. En ese sentido, este trabajo propone una aplicación justificada de las nuevas tecnologías en la fiscalización de los trabajadores, garantizando el respeto a sus derechos fundamentales mediante la consideración de diversos principios. Finalmente, realizaremos un análisis para determinar si una medida de fiscalización es válida, además recomendaremos implementar plataformas de fiscalización digital siempre que estas sean razonables y permitan cumplir con objetivos laborales.

Palabras clave: datos personales, datos sensibles, videovigilancia laboral, derecho a la intimidad, derecho al trabajo.

ABSTRACT

From the current process of technological revolution, new ways of working, subordinating and depending have arisen. In relation to the latter, it is important to note that the employer has the supervisory power, through which it can exercise control over the activities of its workers. The use of new technologies for the purpose of supervising workers is already a reality, therefore this research is aimed at establishing limits on the use and processing of personal data in relation to supervision through new technologies, analyzing the regulations in force in said matter with the purpose of demonstrating that it does not contemplate several cases in which there is an indiscriminate use of personal data, violating the right to privacy of workers. In this sense, this work proposes a justified application of new technologies in the supervision of workers, guaranteeing respect for their fundamental rights through the consideration of various principles. Finally, we will carry out an analysis to determine if an inspection measure is valid, and we will also recommend implementing digital inspection platforms as long as they are reasonable and allow work objectives to be met.

Keywords: Protection of personal data, sensitive data, labor video surveillance, right to privacy, right to work.

CAPÍTULO I: INTRODUCCIÓN

1.1. Descripción de la realidad problemática

Las nuevas tecnologías han reformulado completamente el estilo de vida del mundo como sociedad, llevándonos a transformar incluso nuestra forma de producir y trabajar. De esta manera, el uso de estas herramientas ha originado el planteamiento de nuevos escenarios, en los que se encuentran en disputa derechos fundamentales y se hace necesaria su regulación. En efecto, la implementación de nuevas tecnologías en diversos aspectos de nuestra vida cotidiana ocasiona muchas veces la colisión de derechos, lo cual lleva a la necesidad de delimitar y/o restringir ciertas tecnologías en el uso de diferentes ámbitos, siendo uno de ellos el ámbito laboral.

Dentro del ámbito laboral tenemos al derecho laboral como la rama del derecho que tiene como propósito la tutela de los derechos del trabajador dentro de su vínculo contractual con el empleador. Así las cosas, el derecho laboral contiene *per se* una serie de preceptos y principios que se inclinan a la tutela del empleado como la parte menos favorecida dentro del vínculo laboral, esto debido a que es el empleador (la empresa), quien ostenta el poder y tiene atribuciones para dirigir la fuerza de trabajo del colaborador (rol de fiscalización). La falta de regulación específica nos lleva a reflexionar sobre el papel fiscalizador del empleador y el uso de la tecnología en el marco de un vínculo laboral. Es el caso que nuestra legislación aún no ha delimitado a través de norma específica el poder que tiene el empleador para fiscalizar las funciones del trabajador haciendo uso de nuevas tecnologías.

En consecuencia, al no tener un esquema legal claro para el uso de las nuevas tecnologías para el monitoreo o fiscalización de los trabajadores, se generan sendos vacíos en los límites que debieran existir con relación a los derechos de los trabajadores, uno de estos límites está orientado al derecho de protección de datos personales frente al control que puede ejercer el empleador en el marco de una relación laboral. Esta carencia regulatoria dificulta la delimitación precisa de la actuación del empleador y el manejo de la información de carácter privado de los operarios, lo que favorece la vulneración de derechos fundamentales, especialmente considerando que el trabajador está en una situación desventajosa dentro del vínculo laboral.

A partir de esta problemática, analizaremos la necesidad de interpretar correctamente los principios fundamentales de la protección de datos personales en el manejo de información de los trabajadores por parte de la empresa, estableciendo límites tanto para casos en los que dicho uso se hace obligatorio, como para los que son de carácter consensual.

1.2. Problemas de investigación

1.2.1. Problema General

¿El acceso a datos personales obtenidos mediante el uso de nuevas tecnologías para el control y fiscalización laboral-, como el GPS y la videovigilancia-, vulnera el derecho a la protección de datos personales del trabajador?

1.2.2. Problemas específicos

1. ¿Qué criterios se deben emplear para acceder a datos de geolocalización o videovigilancia como mecanismos de fiscalización laboral en el marco de una relación de trabajo?
2. ¿En el Perú contamos con un ordenamiento jurídico que regule eficazmente el uso de datos personales obtenidos por mecanismos de fiscalización laboral como el GPS y la videovigilancia dentro de una relación de trabajo?

1.3. Objetivos de investigación

1.3.1. Objetivo general

Analizar si el acceso a datos personales obtenidos mediante el uso de nuevas tecnologías para el control y fiscalización laboral- como el GPS y la videovigilancia- vulnera el derecho a la protección de datos personales del trabajador.

1.3.2. Objetivos específicos

1. Determinar los criterios que deben aplicarse para acceder a datos de geolocalización o videovigilancia como mecanismos de fiscalización laboral en el marco de una relación de trabajo.

2. Evaluar si en el Perú contamos con un ordenamiento jurídico que regule eficazmente el uso de datos personales obtenidos por mecanismos de fiscalización laboral como el GPS y la videovigilancia dentro de una relación de trabajo.

1.4. Justificación de la investigación

La presente investigación reviste una particular importancia dentro de la protección de datos personales y establece lineamientos de mayor claridad para la aplicación de mecanismos de fiscalización laboral mediante el uso de nuevas tecnologías como el rastreo satelital por GPS y el registro de imágenes por videovigilancia.

En esa línea, el estudio realizado pretende evidenciar la ausencia de regulación con respecto al manejo de los datos personales frente a su inadecuada protección cuando se trata del uso de dispositivos tecnologías como mecanismos de control laboral por parte de la empresa hacia sus trabajadores, dicha problemática se agrava en la medida que no existen pronunciamientos legislativos, judiciales ni administrativos en esta materia, lo cual dificulta aún más establecer una guía jurídica para delimitar el uso de los señalados datos personales en torno a una relación de trabajo.

De tal manera, nuestra investigación contribuye a delimitar los criterios aplicables para el uso adecuado de los datos personales a los que el empleador tiene acceso cuando ejerce su rol de fiscalización mediante nuevas tecnologías como rastreo GPS y videovigilancia.

Por otro lado, el presente trabajo supone una especial relevancia en las ramas del Derecho de protección de datos, nuevas tecnologías, laboral y constitucional, puesto que el uso indiscriminado de los medios tecnológicos por parte del empleador, mediante plataformas de control y monitoreo laboral, trae como consecuencia una vulneración de los derechos del trabajador, siendo que pueden quedar expuestos incluso derechos fundamentales como el derecho a la intimidad y dignidad de la persona humana.

En ese sentido, nuestro trabajo propone establecer los límites legales en el uso y tratamiento válido de los datos personales, cuya recepción se configura al momento de emplear mecanismos de control y fiscalización laboral dentro de una relación de trabajo.

Para ello, consideramos que se deberían aplicar preceptos constitucionales, principios generales del Derecho, la Ley de Datos Personales y su Reglamento, así como diversos pronunciamientos judiciales y administrativos, incluyendo aquellos provenientes de ordenamientos jurídicos extranjeros.

1.5. Hipótesis

1.5.1. Hipótesis general

El acceso a datos personales obtenidos mediante el uso de nuevas tecnologías de fiscalización laboral como el GPS y la videovigilancia sí supone una vulneración a la protección de datos personales del trabajador cuando se realiza un indebido uso de dichos datos personales.

1.5.2. Hipótesis específicas

1. Los criterios que deben aplicarse para acceder a datos de geolocalización o videovigilancia como mecanismos de fiscalización laboral en el marco de una relación de trabajo, tales como la proporcionalidad y finalidad, para garantizar el respeto a la protección de datos personales del trabajador.

2. El ordenamiento jurídico peruano no regula de manera eficaz el uso de datos personales obtenidos por mecanismos de fiscalización laboral como el GPS y la videovigilancia dentro de una relación de trabajo.

1.6. Marco metodológico

La presente tesis emplea el método cualitativo con una estructura jurídico dogmática, todo a su vez que tiene por objeto el estudio central del acceso a datos personales obtenidos mediante el uso de nuevas tecnologías para la gestión y fiscalización laboral como el GPS y la videovigilancia que vulnera el derecho a la protección de datos personales del trabajador. En este sentido, se llevará a cabo una exhaustiva recopilación de información para responder adecuadamente las preguntas antes planteadas.

CAPÍTULO II: ANÁLISIS CRÍTICO

2.1. El derecho a la protección de datos

2.1.1. Antecedentes

En este acápite se ofrecerán nociones sobre la Ley de Protección de Datos Personales, cuya promulgación fue tardía en comparación con las legislaciones de otros países. Un ejemplo es Alemania, que en 1977 aprobó su Ley Federal de Protección de Datos, o conocida como el *Bundesdatenschutzgesetz*, basada en fundamentos constitucionales y estudios doctrinarios sobre la privacidad. De manera similar, países como Italia desarrollaron leyes inspiradas en normas previas, como el Estatuto de los Trabajadores de 1970, que prohíbe ciertas formas de monitoreo a distancia. Por otro lado, en Estados Unidos, el *Privacy Act* de 1974 que estableció las bases para la protección de la información personal[1].

El *Privacy Act* surgió como una ley independiente, diseñada como un régimen de excepción al *Freedom of Information Act* (en adelante FOIA). Este último permitía a todos los ciudadanos acceder a la información de entidades públicas, promoviendo la transparencia. *El Privacy Act*, en cambio, estableció restricciones para proteger los datos personales, equilibrando el derecho a la privacidad con el acceso a la información pública.

El FOIA exige a las agencias difundir 04 actos administrativos clave, como lo son: el primero, el establecimiento en los cuales los interesados podrán solicitar las informaciones; el segundo, los procedimientos imprescindibles para la colaboración y participación en los procedimientos; la tercera, las disposiciones legales emitidas por el Poder Legislativo; y la cuarto, las distintas formas de publicación de los actos que facultan a los ciudadanos para que de forma particular o grupal tengan conocimiento de las decisiones tomadas por las *agencies*[2].

---

[1] Juan Espinoza Espinoza, *"*La tutela jurídica del tratamiento de los datos personales frente a los avances de la información. Propuesta para un redimensionamiento del denominado derecho general de la personalidad y para una definición común del denominado hábeas data", *IUS VERITAS 10,* no.20 (2000): 89.

[2] Espinoza, *"La tutela jurídica del tratamiento de los datos personales frente a los avances de la información. Propuesta para un redimensionamiento del denominado derecho general de la personalidad y para una definición común del denominado hábeas data"*, 89.

Aunque, el FOIA aportó la introducción del derecho a conocer, también establece las siguientes excepciones de conocer información que de ser divulgada podría colocar en peligro a la seguridad nacional, el funcionamiento del *agencie,* secretos comerciales, información médica y personal e investigaciones de las *agencies* que tutelen la seguridad interna del país. En ese sistema americano, la clasificación de los datos se construye bajo una pirámide de jerarquía, dentro de la cual prima la información considerada como *National Security Council*, es así que no todas las *agencies* pueden liberar y difundir información perteneciente a otra *agencie;* por ello, existe un *Counsil* que tiene la asistencia del *Interagency Classificatión Review Commitee,* el cual recibe las sugerencias y pedidos[3].

Por otro lado, tenemos el modelo francés, con la *Loi relative á informatique* del 17 de enero del 1978, el valor de su aporte consistió en darle una tutela al sujeto en su vida privada, incluido en el campo de las informaciones, adquiriendo así la informática una dimensión de ser un servicio público y en consecuencia, sujeto al control del Estado. Habiendo realizado un breve recorrido por los antecedentes universales de la materia que nos atañe, procederemos a analizar ello en nuestra normativa precedente y actual[4].

2.1.2. En la Constitución del 1979

La Constitución Política del Perú es una de las normas más relevantes del país y constituye la base de todo el ordenamiento jurídico. Dentro de la jerarquía normativa peruana, la Constitución ocupa el lugar más alto. A diferencia del modelo propuesto por Kelsen, el sistema legal peruano reconoce la importancia de la ética, la moral, los derechos fundamentales y otras disciplinas como elementos esenciales de la Constitución.

En este contexto, la Constitución de 1979 representa un claro ejemplo de cómo la norma suprema del país refleja estos principios fundamentales.

---

[3] Espinoza, *"La tutela jurídica del tratamiento de los datos personales frente a los avances de la información. Propuesta para un redimensionamiento del denominado derecho general de la personalidad y para una definición común del denominado hábeas data"*, 89.

[4] Espinoza, *"La tutela jurídica del tratamiento de los datos personales frente a los avances de la información. Propuesta para un redimensionamiento del denominado derecho general de la personalidad y para una definición común del denominado hábeas data"*, 89.

A través de este documento, se dio mayor importancia a los derechos fundamentales, los cuales se consolidaron como pilares esenciales dentro del marco constitucional peruano. Estos derechos, que hoy se reconocen como inherentes a todas las personas por su condición humana, reflejan un avance significativo en su protección[5].

La Constitución de 1979 brindó un enfoque más amplio y detallado al tema laboral en comparación con las constituciones de 1920 y 1933, que lo trataron de manera más general. En este marco, se destacó el trabajo no solo como una fuente de riqueza, sino también como un elemento fundamental para la realización personal y para contribuir al bienestar de toda la sociedad[6].

Podemos observar que la Constitución política de 1979 sólo reconoce el derecho de la intimidad personal y familiar. Aunque, los derechos a la intimidad y la protección de datos personales son distintos, es común reconocer que los primeros están relacionados con los segundos, como se puede observar en las Constituciones del Reino de España, los Estados Unidos Mexicanos, Colombia, la República de Chile y el Perú.

Aunque la Constitución de 1979 otorgó relevancia a varios derechos fundamentales, como la integridad y la dignidad, no incluyó una protección específica de los datos personales. Este tema comenzó a ganar mayor importancia con la Constitución de 1993, que abordó de manera más clara la protección de la intimidad y abrió el camino para el desarrollo de normativas especializadas. A partir de este marco, surgió la Ley de Protección de Datos Personales, creada para responder a las nuevas preocupaciones sociales y a los avances tecnológicos que hicieron necesaria una regulación más detallada en esta materia.

En resumen, la Constitución de 1979 respondió a la necesidad de crear un marco legal que colocara a la persona en el centro del orden jurídico, asegurando su dignidad, sus derechos y libertades, y reconociendo su papel fundamental en la sociedad[7].

---

[5] Sessarego, *"Las personas, el personalismo y la constitución peruana de 1979"*, 81-95.
[6] Bustamante, *"La Constitución de 1979 y el derecho del trabajo"*, 7.
[7] Sessarego, *"Las personas, el personalismo y la constitución peruana de 1979"*, 81-95.

2.1.3. En la Constitución vigente

La Constitución de 1993 constituye el primer instrumento jurídico en introducir uno de los hitos más relevantes, en cuanto a derechos fundamentales, al reconocer que toda persona puede decidir cómo se manejan sus datos personales. Coincidiendo con lo sostenido por Eguiguren quien refiere que a través del numeral 6 del art. 2 de la presente carta magna se reconoce la facultad de disposición de los ciudadanos sobre sus datos[8].

Años más tarde, el Tribunal Constitucional (en adelante TC), a través de diversos fallos y con base en el inciso 2 del art. 61 del Código Procesal Constitucional, desarrolló el concepto del derecho a la autodeterminación informativa[9].

En palabras del propio TC, se entiende como derecho a la autodeterminación efectiva al conjunto de prerrogativas y derechos que posee todo ciudadano de poder tener mayor manejo de la data que se encuentra en registros privados, públicos, incluso informáticos. Este derecho está estrechamente relacionado con el control de la información, como la autonomía en la vida personal. La autodeterminación informativa tiene como objetivo proteger al individuo, no solo en los derechos que pertenecen a su dimensión personal, sino también en los demás[10].

Resulta importante señalar que el contenido del derecho a la autodeterminación informativa comprende lo siguiente:

- El derecho de requerir al ente jurisdiccional el acceso a los registros sin importar la naturaleza de los archivos donde se almacenen los datos personales. En palabras del tribunal antes señalado, se persigue el propósito de que se sepa la finalidad con la que se registraron los datos.

- La facultad de agregar información al registro de cara a que se restablezcan los datos registrados, que sean imprescindibles.

---

[8] Praeli, *"El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú"*, 132.
[9] Celis, *"El derecho a la protección de datos personales en el Perú: 27 años desde su incorporación en la constitución política de 1993"*, 86.
[10] Tribunal Constitucional, EXP.N° 4739-2007-PHD/TC, de 15 de octubre de 2007.

- El poder modificar la información registrada.
- El poder oponerse a que la información sea divulgada con fines ajenos a los motivos por los cuales se registró la información.

En aras de perfeccionar el reconocimiento de la Constitución, se promulgó en el 2011 la Ley de Protección de Datos Personales, junto con su reglamento, aprobado mediante el Decreto Supremo N.° 003-2013-JUS, que fue publicado el 22 de marzo de 2013[11].

2.2. En el marco normativo nacional

A nivel nacional, en nuestro marco regulatorio se establecen diversas disposiciones legales enfocadas en distintos aspectos de la protección de derechos fundamentales. En este sentido, una de las áreas de mayor relevancia es la protección de datos frente a los medios digitales.

> (...)*" En el Perú, la defensa de la privacidad informativa frente al creciente uso de los medios tecnológicos se sustenta en vías de mejora. Ley Nº29733- Ley de Protección de Datos Personales, establece los principios y derechos fundamentales para garantizar la privacidad. Esta ley se complementa con el Decreto Supremo Nº003-2013-JUS, que aprueba su reglamento, proporcionando directrices claras para su aplicación. Además, la Resolución Directoral Nº019-2013-JUS implementa la Directiva de Seguridad de información, asegurando el resguardo de datos sensibles. Con la Resolución Directoral Nº002-2020-JUS/DGTAIPD, se regula el tratamiento de datos mediante videovigilancia, un medio cada vez más utilizado. Asimismo, la Norma Técnica Peruana NTP-ISO/EIC270001:2008, adoptada de manera obligatoria por la Resolución Ministerial Nº129-2013-JUS, establece estándares internacionales para los sistemas de gestión de seguridad de la información).*

La LPDP y su reglamento establecen las normas para el tratamiento de datos personales de individuos en bancos de datos, ya sean públicos o privados, en el estado peruano. Se trata de reglas de orden público, lo que implica que tanto las autoridades del sector público como del privado están obligadas a cumplirlas.

---

[11] Moore, *"El derecho fundamental a la protección de datos personales en el entorno laboral"*, 274.

El Reglamento y la LPDP ofrecen definiciones relevantes. Una de las más esenciales es la de "dato personal": El art. 2, numeral 4 del Reglamento establece que "aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que pueden ser razonablemente utilizados"[12].

Además, la aplicación de la LPDP se basa en dos factores cruciales. La primera es lo que la LPDP llama "bases de datos". El cual hace referencia al "conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera sea la forma o modalidad de su creación, formación, almacenamiento, organización y acceso"[13].

El segundo elemento en tomar atención es el "tratamiento" de los datos, que se define como "cualquier operación o procedimiento técnico, automatizado o no, que permita la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, uso, bloqueo, supresión, comunicación por transferencia o difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos"[14].

El principio fundamental de esta rama del derecho es establecer que ningún "tratamiento" de estos se realizarán si un consentimiento anticipado, plenamente informado, claro y explícito del titular, salvo en los casos que la ley disponga excepciones específicas. Sin embargo, es importante destacar que en algunos casos establecidos en el art. 14 de la LPDP[15], el consentimiento del titular de datos personales no es necesario. Algunos ejemplos de estas excepciones son:

- Cuando se recopilan o transfieren datos personales para que las entidades públicas realicen sus funciones dentro de su ámbito de actuación.

- En situaciones donde la información personal está prevista para su disponibilidad en registro públicos.

[12] Decreto Supremo N.º 003-2013-JUS, 22 de marzo de 2013, Reglamento de la Ley N.º 29733-Ley de Protección de Datos Personales (Lima, 25 de marzo de 2013).
[13] Ley 29733
[14] Decreto Supremo N.º 003-2013-JUS
[15] Ley 29733

- Cuando se trata de información personal relacionada con la solvencia financiera y de crédito, se deben cumplir las normas específicas de la materia.

- Aquellos necesarios para el cumplir un contrato en el que el titular esté involucrado, o para el desarrollo de una relación profesional del mismo.

El consentimiento se refiere a datos sensibles, como datos de identificación biométrica que identifican a la persona; así como aquellos datos relacionados con el origen racial y étnico, ingresos económicos, y creencias políticas, religiosas, filosóficas o morales. También incluye la afiliación sindical y la información sobre características físicas, morales o emocionales, así como hechos o circunstancias de su entorno familiar. Es fundamental seguir los principios de finalidad, proporcionalidad, calidad y seguridad en el tratamiento de esta información.

Aparte, de la regla del consentimiento, se debe recordar que las siguientes son las principales recomendaciones para cumplir con las Leyes de Protección de Datos:

- **Bases de datos:** Estos deben registrarse en el Registro Nacional de Protección de Datos Personales.

- **Flujo transfronterizo:** Es necesario comunicar el flujo transfronterizo a la Autoridad de Protección de Datos Personales, a través de una modificación en el formulario de inscripción de la base de datos. Solo si el país destinatario mantiene niveles adecuados de protección, el titular del banco de datos personales puede enviar esos datos por vía internacional. El emisor de datos transfronterizos debe asegurarse de que el manejo de los datos con información privada cumpla con la legislación vigente o conseguir el consentimiento del titular en otras circunstancias si el país destinatario carece de protección adecuada.

- **La seguridad:** El propietario del banco de datos personales y aquellos que participan en el tratamiento de esta información, tienen la obligación de preservar la confidencialidad. Esto significa que a pesar de que los nexos con el propietario del banco de datos han terminado, esta responsabilidad sigue siendo necesaria. Del mismo modo, aquellos que poseen bancos de datos personales deben tomar medidas para proteger sus datos.

- **Preservación de la información:** Los datos personales que se tratarán deben preservarse por el tiempo imprescindible para lograr con la finalidad del tratamiento. Las organizaciones tendrán la capacidad de almacenar los datos durante el período de tiempo que sea necesario.

- **Derechos Arcos:** Los cuales brindan a las personas el control sobre sus datos personales a través de la LPDP y su Reglamento, incluidos los derechos de acceso, rectificación, cancelación y opción. Los cuales tienen sus propios requisitos y plazos específicos para su ejercicio. Al recibir una respuesta negativa o insatisfactoria, el solicitante tiene la capacidad de iniciar un procedimiento ante la Dirección General de Protección de Datos Personales o presentar un Hábeas data en el Poder Judicial.

- **El Deber de información:** En esencia, implica que el propietario del banco de datos personales proporcione al propietario de los datos personales toda la información sobre el "tratamiento" de sus datos. En consecuencia, conlleva que el titular de aquellos datos debe recibir dicha información previamente a su recopilación y que sea adecuada y precisa.

En resumen, el marco normativo peruano tiene su sustento legal en diversas disposiciones tales como la Ley N.°29733 y su reglamento. Normativa que establece los derechos y responsabilidades relacionadas con el manejo de información privada, asegurándose que se respeten principios fundamentales como el consentimiento y la seguridad. Asimismo, se definen situaciones en las que el consentimiento no es necesario, garantizando así el equilibrio entre la protección de los derechos de los individuos y las necesidades operativas de las organizaciones. Por lo tanto, es vital que tanto las entidades públicas como privadas cumplan con estas normas para resguardar la privacidad de los ciudadanos.

2.3. Ley de Protección de datos personales

2.3.1. Nociones conceptuales

2.3.1.1.Datos personales

La protección de los datos personales, también conocida como "autodeterminación informativa" o "libertad informática", ha sido

desarrollada a partir de su reconocimiento constitucional en la jurisprudencia, especialmente en Alemania. Este derecho tiene como objetivo principal salvaguardar la privacidad de quienes son titulares de los datos personales, permitiéndoles decidir qué persona puede acceder a esa información y con qué finalidad[16].

Este principio de autodeterminación informativa ha sido incorporado en varias legislaciones alrededor del mundo, adaptándose a las realidades nacionales de cada país. En el caso del Perú, la protección de los datos personales ha sido regulada con mayor precisión mediante leyes específicas destinadas a asegurar que este derecho sea respetado y protegido. Un ejemplo de ello es el Reglamento de la Ley de Protección de Datos Personales (en adelante LPDP), que detalla los aspectos técnicos y normativos sobre la protección de la información.

En el Reglamento de la LPDP, art. 2, inciso 4 se establece un concepto amplio de dicha denominación, precisando que el dato personal es aquella información numérica, alfabética, fotográfica gráfica, acústica, sobre los costumbres personales, o cualquiera que haga reconocibles a las personales[17].

Podemos observar que nuestro marco legal adopta una definición amplia de lo que se considera objeto de tutela en cuanto a datos personales, el cual responde a una política pública de protección integral, alineada con los principios establecidos por la Organización de las Naciones Unidas (ONU), la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y otros organismos internacionales. Esta amplitud permite que tanto entidades públicas como privadas utilicen grandes volúmenes de datos para diversas actividades, lo que otorga a la información personal una relevancia económica significativa. Además, el correcto almacenamiento y manejo de estos datos facilita la toma de decisiones en ámbitos económicos, académicos y financieros[18]. Sin embargo, no se

[16] Praeli, *"El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú"*, 132.
[17] Ley 29733
[18] Peña, *"Breves reflexiones sobre la responsabilidad civil derivada del tratamiento indebido de datos personales en el Perú"*, 337-338.

puede ser esquivo a las consecuencias inherentes de los desarrollos tecnológicos que han ido amplificando aún más el listado de los datos personales. Últimamente, un dato personal que cobra mayor envergadura, es la información de geolocalización.

En ese sentido, la Autoridad Nacional de Protección de datos Personales- cuya denominación en siglas es ANPDP- a través de la Resolución Directoral N.º008-2017-JUS/DGPDP, manifestó que los celulares e instrumentos electrónicos de similar naturaleza permiten que se identifique y reconozca a las personas a través de la geolocalización, debido a que con ese dato se conoce la circulación y desplazamiento de los sujetos; por ello, esta información de geolocalización constituye en efecto un dato personal y consecuentemente, estará sujeto a la aplicación de la LPDP[19].

Por otro lado, se debe indicar que dentro de la categoría de datos personales, subyace la categoría referida a los "datos sensibles", los cuales del mismo nombre denotan la exigencia de una tutela singular y especial, debido a que su transgresión puede causar un daño trascendental a la persona. En esa misma línea, como datos sensibles tenemos a los datos relacionados con el origen racial, ingresos, opiniones e ideales políticos, filosóficos y religiosos, así como información relacionada con la salud, entiéndase sentimental y sexual[20].

Conviene indicar que la mencionada ley tiene como campo de protección únicamente a los datos personales de las personas naturales, quedando excluidos los datos personales de las empresas.

Con el propósito de un mejor entendimiento, debemos señalar que para poder identificar que estamos ante un dato personal, se necesita que concurran dos elementos, por un lado, un "dato" y también, que dicho dato debe ser capaz de identificar o deberá tener el potencial para hacer factible que pueda identificarse a un sujeto.

---

[19] Resolución Directoral, EXP.N° 008-2017-JUS/DGPDP, de 25 de enero de 2017.
[20] Ley 29733-2011

2.3.1.1.1. Datos sensibles

Se hace referencia a la información personal que puede evidenciar características íntimas de una persona. Esto incluye detalles sobre sus características físicas, emocionales o morales, así como eventos o situaciones en su entorno personal o familiar. También abarca hábitos personales y cualquier información relacionada con la salud, ya sea física o no, que pueda impactar su privacidad[21].

De este modo, al ser datos sensibles, es necesario que el consentimiento se otorgue por escrito. Esto puede hacerse a través de una firma escrita a mano, una firma digital o cualquier otro método de autenticación[22].

A excepción de lo que indica el inciso 13.6 la LPDP, señala que los datos sensibles pueden ser tratados siempre que la ley lo autorice y que el tratamiento esté respaldado por razones de interés público. Esto podría aplicarse en contextos en los que la salud pública, la seguridad nacional, u otros que exijan la recopilación o el uso de datos sensibles.

Un caso relevante en la protección de datos sensibles son los datos biométricos, los cuales son resguardados por la RENIEC y utilizados de acuerdo con lo que establece la legislación. Estos datos tienen una relación directa con derechos fundamentales, como los de intimidad, privacidad y otros derechos conexos que deben ser debidamente protegidos. Dado que se trata de datos sensibles, su tratamiento requiere la autorización del titular o, en su defecto, estar respaldado por una ley expresa en criterios de interés público. En consecuencia, el manejo de la identificación biométrica debe regirse por los principios de veracidad, seguridad y confidencialidad[23].

---

[21] Decreto Supremo N.º 003-2013-JUS
[22] Ley 29733
[23] Tribunal Constitucional, EXP.N° 02834-2013-PHC/TC, de 25 de enero de 2017.

2.3.1.2. Titular de los datos personales

Como mencionamos en el acápite anterior, la legislación peruana suprime a las personas jurídicas del ámbito de aplicación. Esta determinación se fundamenta en la idea de que la protección de estos datos, cuyo objetivo principal es resguardar los derechos de las personas naturales, quienes son más propensas a ser vulnerables en la manipulación de su información personal. En este sentido, el art. 2, inciso 16 de la LPDP, aclara que los únicos titulares son las personas naturales a quienes corresponden dichos datos.

El art. 19 de la LPDP, el titular de los datos tiene el derecho de solicitar información sobre sus propios datos que sean objeto de tratamiento en bases de datos de entidades públicas o privadas. Este derecho incluye conocer cómo se recopilaron estos datos, con qué motivos, quién solicitó dicha información, y si estos datos han sido transferidos a terceros[24].

2.3.1.3. Tratamiento de los datos personales

De acuerdo con la definición realizada, mediante el art. 2, inciso 19, se señala que el tratamiento de datos personales es aquel procedimiento automatizado o no, que posibilita la compilación, registro, modificación, provisión, bloqueo o cualquier otro modo de procesamiento que facilite el acceso a los datos personales.

Este procedimiento al que nos referimos puede efectuarse a través de un banco de datos personales, así como puede efectuarse sin necesidad de este. Por ejemplo, cuando un individuo se toma una fotografía con el celular, está efectuando evidentemente un tratamiento de datos, pero sin hacer uso de un banco de datos.

En ese sentido, basta que se haga uso de un dato personal, lo que consiste en la sola recolección del dato hasta su conservación, modificación o anulación. Si bien es cierto la finalidad y su tratamiento serán determinados por quien sea el titular del banco de datos o quien sea responsable del tratamiento, desde que se acopia esos datos personales ya

[24] Ley 29733

existe un tratamiento como tal, y ya supone que estemos ante el campo de aplicación de la normativa de protección de datos personales.

2.3.1.4. Banco de datos

La recopilación, alteración o eliminación de información personal recolectada para el uso de agencias públicas o privadas, deben estar sujetas a lo indicado por el reglamento, salvo disposición contraría contenida en otra ley[25]. Esta normativa es clave, ya que los bancos de datos recopilan información personal sensible, y una mala gestión o tratamiento de estos datos puede representar un riesgo significativo para la privacidad y seguridad de las personas.

En este contexto, es importante definir a qué nos referimos con "bancos de datos". Los bancos de datos constituyen un grupo estructurado de información, que puede estar automatizado o no, independientemente del tipo de soporte utilizado, ya sea magnético, físico, digital u óptico. Independientemente de la forma en que se recopilen, organicen o accedan los datos, estos deben estar sujetos a una correcta regulación para garantizar un manejo responsable y transparente de la información.

Dada la importancia de proteger la información personal de los individuos, el art. 34 de la LPDP establece la creación del Registro Nacional de Protección de Datos Personales, administrado por la Autoridad Nacional de Protección de Datos Personales (en adelante la ANPDP). En este registro, deberán inscribirse los bancos de datos organizados por instituciones públicas o privadas; sin embargo, según el inciso 2 del mismo artículo, la ANPDP no tiene acceso al contenido de las bases de datos inscritas, excepto dentro del contexto de un procedimiento administrativo que lo respalde y justifique[26].

[25] Ley 29733
[26] Praeli, "*El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú"*, 137.

2.3.1.5. Titular del Banco de datos personales

El titular de un banco de datos personales es la persona, ya sea natural o jurídica, que posee la propiedad o la gestión de un conjunto organizado de información personal. Este titular tiene la responsabilidad de garantizar que dichos datos se recopilen, almacenen y procesen conforme a las normas legales vigentes, protegiendo los derechos de los individuos cuyos datos se encuentran en el banco.

De acuerdo con el principio de seguridad, quien esté a cargo de un banco de datos personales debe implementar las medidas técnicas, organizativas y legales necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información. Estas medidas buscan prevenir la alteración, pérdida, desvío de datos o cualquier uso indebido, ya sea intencional o no, sin importar si el riesgo proviene de acciones humanas o fallos técnicos. Además, dichos procedimientos de seguridad deben ser adecuados según el tipo de tratamiento que se realizará y la naturaleza de los datos personales que se manejen[27].

Por tal motivo, la función del titular del banco de datos resulta fundamental para asumir las obligaciones derivadas de cualquier incumplimiento normativo. Esto incluye responder ante el individuo perjudicado por el uso indebido de sus datos y ante el organismo responsable de supervisar el cumplimiento de las normativas.

2.3.2 Principios y directrices

2.3.2.1. Principio de seguridad

El principio de seguridad en la protección de datos personales obliga al responsable del tratamiento de los datos a implementar medidas adecuadas. Dichas medidas tienen el fin de prevenir la alteración o el acceso no autorizado de terceros inescrupulosos a los datos personales, con el fin de no poner en peligro el control sobre la información almacenada.

---

[27]Alvarado, *"La gestión de la seguridad de la información en el Régimen Peruano de Protección de Datos Personales"*, 28-29.

Si estos incidentes ocurren, se estaría afectando la privacidad del titular de los datos, ya que se estaría violando las condiciones bajo las cuales consintió el tratamiento de su información[28].

Este principio está regulado en los art. 9 y 16 de la LPDP. El art. 9 establece las responsabilidades tanto del titular del banco de datos personales como del encargado de su tratamiento, subrayando que, al manejarse información sensible o confidencial, debe implementarse un conjunto de medidas técnicas, organizativas y legales adecuadas para garantizar la protección de los datos. De manera similar, el art. 16 detalla los requisitos y condiciones de seguridad que deben cumplir los titulares de los bancos de datos, resaltando la urgencia de cumplir las directrices establecidas por la ANPDP[29].

Ambos artículos destacan la relevancia de adoptar medidas que aseguren la integridad y confidencialidad de los datos, lo que implica una política de seguridad muy rigurosa que abarque aspectos técnicos hasta normativas organizativas y legales, para prevenir cualquier tipo de vulneración o uso indebido de la información.

De la interpretación conjunta de ambos artículos, se puede concluir que el propósito principal de este principio es asegurar la protección de los datos personales frente a los riesgos específicos tales como[30]:

- Alteración: Es la modificación de los datos personales al momento de ser recopilados. En el caso de un tratamiento no automatizado, esta manipulación se puede dar en documentos impresos o escritos que contengan la misma información sensible. Es decir, la alteración se puede dar por medio de actividades manuales, actividades que requieran la intervención directa de una persona.

---

[28] Rodríguez,*"El principio de seguridad de la Ley de protección de datos personales"* Lp Pasión por el Derecho.
[29] Rodríguez, *" La responsabilidad proactiva en la normativa peruana de protección de datos personales"*, 33.
[30] Rodríguez, "*El principio de seguridad de la Ley de protección de datos personales"* Lp Pasión por el Derecho.

- Pérdida: Se refiere a la situación en la que la información relacionada con un individuo ya no está accesible o no puede ser recuperada, ya sea de forma total o parcial. Esto puede ocurrir debido a la eliminación accidental, la destrucción o la sustracción de los medios de almacenamiento, ya sean físicos, como documentos impresos, o digitales, como bases de datos. Estas circunstancias implican que el soporte que contenía los datos ha sido afectado, lo que resulta en la indisponibilidad de la información.

- Tratamiento o acceso no autorizado: El acceso a información privada, por parte de una entidad o persona no autorizada, se considera ilegítimo si dicha entidad no cuenta con las autorizaciones necesarias o con el cargo correspondiente para llevar a cabo dichas actividades.

Se entiende que el control de estos riesgos tiene como objetivo mantener la integridad y precisión de los datos almacenados, garantizando que puedan ser utilizados de manera adecuada y para fines lícitos. Además, este acceso y uso deben estar limitados únicamente a personas autorizadas, protegiendo así los principios de integridad, disponibilidad y confidencialidad de la información.

2.3.2.2. Principio de legalidad

El principio de legalidad es un principio fundamental que se encuentra consagrado en las constituciones de diferentes países, en donde se encargan de guiar la interpretación y ejecución de las leyes, asegurándose de que todas las acciones del Estado se realicen dentro de un marco legal claro y consistente.

Este principio establece que existe una relación de superioridad entre el estado y los ciudadanos, es decir, que las acciones del estado pueden afectar los derechos de las personas.

Esto sucede porque el Estado crea leyes y toma decisiones que pueden ir más allá de lo que cada individuo puede manejar[31].

Por ello, el principio de legalidad se opone a cualquier acción que infrinja la ley o que no esté autorizada por esta. Dicho principio se manifiesta en dos dimensiones: una estática y otra dinámica. Cuando hablamos de la dimensión estática, establece quién tiene la autoridad para realizar un acto o cómo debe llevarse a cabo. Mientras que en su dimensión dinámica, se asegura de que tanto la actuación de la autoridad como sus resultados estén en conformidad con la ley.

Una de las mejores formas de entender este principio es a través de la idea de que "la autoridad solo puede hacer lo que la ley le permite", lo que implica que la autoridad debe actuar dentro de su competencia legal y bajo control, vigilando que sus decisiones se ajusten al marco normativo. Además, el principio exige que todos los órganos del Estado se sometan a la ley, asegurando que cualquier acto o procedimiento llevado a cabo por las autoridades esté respaldado por una norma legal que cumpla con la Constitución en fondo y forma[32].

El principio de legalidad es esencial para garantizar que el Estado actúe siempre dentro de un marco normativo claro, lo cual resguarda los derechos fundamentales de los ciudadanos. Al estar consagrado en las constituciones, regula cómo deben interpretarse y aplicarse las leyes, asegurando que toda acción estatal esté sustentada en normas claras y predecibles.

Este principio no solo asegura que las acciones del estado se ajusten a un marco normativo claro, sino que también impone la obligación de establecer mecanismos de control y supervisión adecuados para velar por el cumplimiento de las leyes, como la LPDP. Esta ley no solo prohíbe la captación de información personal por medios deshonestos o contrarios a la ley, sino que además establece un régimen sancionador para quienes infrinjan sus disposiciones.

---

[31] Montes,*"Sobre el principio de legalidad"*, Corte Interamericana de Derechos Humanos.
[32] Montes,*"Sobre el principio de legalidad"*, Corte Interamericana de Derechos Humanos.

Estas sanciones tienen como objetivo disuadir conductas que vulneren los derechos fundamentales de los ciudadanos, garantizando que el tratamiento de los datos personales se realice bajo estrictos estándares de transparencia y equidad. Asimismo, la autoridad reguladora en materia de protección de datos tiene la responsabilidad de monitorear y sancionar las prácticas que comprometan la privacidad de las personas.

Considerando que el tratamiento de los datos personales se realiza de acuerdo con lo estipulado en la LPDP. La gestión de esta información debe realizarse con pleno respeto a los derechos fundamentales y en cumplimiento de lo dispuesto en el art. 4 de la mencionada ley, el cual prohíbe la recolección de datos personales mediante métodos fraudulentos, desleales o ilegales[33].

Por ende, el principio de legalidad establece que el responsable de la gestión de información privada debe implementar medidas adecuadas para prevenir la recolección de datos con fines que puedan comprometer los derechos fundamentales de aquellos que los proporcionan.

2.3.2.3. Principio de Proporcionalidad

El art. 7 de la LPDP establece el principio de proporcionalidad, que indica que cualquier tratamiento de datos personales debe ser apropiado, pertinente y no sobrepasar lo necesario para el propósito con el que fueron recolectados[34]. En otras palabras, el principio de proporcionalidad es una regla que exige que cualquier tratamiento de datos personales esté adecuadamente equilibrado. Esto implica que las acciones de las entidades que manejan datos personales, al afectar los derechos de los titulares, deben ser apropiadas, necesarias y no excesivas.

En otras palabras, la recolección, almacenamiento o uso de datos debe ajustarse estrictamente a los fines permitidos por la ley, sin imponer restricciones o vulnerar la privacidad más allá de lo necesario para alcanzar un objetivo legítimo.

[33] Ley 29733
[34] Ley 29733

En el contexto de la era digital actual, el principio de proporcionalidad se ajusta a los avances en inteligencia artificial (en adelante IA) y Big Data, reflejando la necesidad de un manejo ético y responsable de la información. Este principio requiere que los desarrolladores y las entidades encargadas del tratamiento de datos analicen minuciosamente el modelo que emplearán para seleccionar la información que se proporcionará a la IA[35].

Es fundamental que los datos sean relevantes y necesarios para alcanzar los objetivos establecidos, lo que implica que el encargado del tratamiento debe elegir la alternativa que cause el menor impacto posible en la privacidad de las personas cuyos datos están siendo utilizados. Además, se recomienda que esta decisión sea documentada, para que pueda ser presentada a la ANPDP.

2.3.2.4. Principio de calidad

El art. 8 de la LPDP menciona que la información que se maneja debe ser verdadera, precisa y adecuada para su uso. Además, es esencial que se almacene de manera segura y solo durante el tiempo necesario para alcanzar el propósito para el cual fue recopilada. Esto asegura que la información se mantenga confiable y se protejan los derechos de las personas[36].

El principio de calidad, consagrado en el art. 9 de la LPDP destaca la importancia de que la información contenida en los bancos de datos se ajuste fielmente a la realidad[37]. Este principio garantiza que la información tratada sea precisa y confiable, protegiendo así los derechos del titular. Se presume, además, que los datos proporcionados directamente por el titular son exactos, lo que refuerza la necesidad de un manejo diligente y responsable por parte de quienes gestionan dicha información. Este enfoque busca evitar errores que puedan generar perjuicios y asegura que el tratamiento de los datos se realice de manera legítima y transparente.

[35] Cáceres, *"El impacto de la inteligencia artificial en el Derecho"*, 65.
[36] Ley 29733
[37] Ley 29733

2.3.2.5. Principio de consentimiento

De acuerdo con el art. 5 de la LPDP, el manejo de datos personales requiere la autorización del titular. Esto significa que solo se pueden tratar los datos si la persona titular de ellos brinda su autorización. De igual manera, el numeral 13.5 del art. 13 indica que, en caso una ley autorice lo contrario, es necesario contar con el consentimiento del titular. Este consentimiento debe ser previo, claro, explícito y sin lugar a dudas[38].

Cuando se trata de datos sensibles, es necesario obtener el consentimiento del titular de manera adicional y por escrito. Además, se deben cumplir con las disposiciones del art. 18 de la LPDP. Esto implica que, antes de recolectar los datos, el titular debe ser informado sobre la finalidad del tratamiento, quiénes serán los posibles destinatarios de esos datos, si existe un banco de datos donde serán almacenados, así como la identificación y dirección del responsable y, en su caso, de quienes gestionarán el tratamiento de los datos personales[39].

Lo que se busca garantizar y proteger cuando una entidad pública o privada maneja nuestros datos personales es que lo hagan de acuerdo con ciertas normas y principios. En términos simples, estos principios incluyen[40]:

- La divulgación de datos debe consistir en información verdadera, sin alterar la historia de los hechos, así como respetar los límites legales y razonables para su exposición.

- Si se dará uso de estos datos personales, que sea con el consentimiento del titular, de manera proporcional y para el fin que fue solicitado.

---

[38] Praeli, *"El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú"*, 137.
[39] Ley 29733
[40] Cervantes, *"Preguntas y respuestas varias sobre la protección de datos personales en el Perú"*, 255-256.

- Si se van a transferir, que se informe a dónde y quién tendrá acceso a dichos datos.

- Si se van a almacenar o procesar, que se haga de manera segura e informada al titular y autoridad competente.

Si alguna de estas acciones incumple la ley o vulnera los derechos del titular de los datos, este tiene la facultad de recurrir a la autoridad competente para solicitar la debida corrección[41]. En resumen, el objetivo es salvaguardar los datos personales frente a un uso indebido y asegurar que el titular mantenga siempre el control sobre ellos.

2.3.2.6. Principio de finalidad

El art. 6 de la LPDP, que se refiere al principio de finalidad, establece que los datos personales deben ser recolectados con un propósito claro, específico y legal. Además, una vez que se han recopilado, su uso debe limitarse a ese propósito original y no puede ampliarse a otros fines que no hayan sido claramente definidos en el momento de la recolección. Sin embargo, se permiten excepciones en situaciones donde se utilizan los datos para actividades de valor histórico, estadístico o científico, siempre que se aplique un método de disociación o anonimización para proteger la identidad de las personas involucradas[42]. Es decir, este principio tiene como objetivo definir los propósitos específicos para los cuales se utilizarán los datos personales, garantizando así que el titular de los datos tenga el derecho a conocer y controlar a quién se proporciona su información personal y con qué motivos.

Un ejemplo evidente de infracción del principio de finalidad es el uso de los test *online*, los cuales, al buscar recopilar datos, solicitan que el usuario inicie sesión de su cuenta de *Facebook* (o cualquier otra red social) para completar dicha encuesta.

---

[41] Cervantes, "*Preguntas y respuestas varias sobre la protección de datos personales en el Perú"*, 255-256.
[42] Ley 29733

> Aunque, esta información se utiliza para crear anuncios personalizados, las empresas no siempre son transparentes en cómo manejan estos datos, y una parte considerable de la información personal obtenida es desviada para fines que no siempre son lícitos[43].
>
> Por tal motivo, el principio de finalidad es fundamental para proteger los derechos de los titulares de datos personales, asegurándose que dicha información que se obtenga de ellos, sea utilizada con propósitos específicos, lícitos y bajo el conocimiento del titular. De esta manera, es crucial que las entidades sean más responsables en su manejo de los datos y que se establezcan mecanismos que permitan a los usuarios tener un control efectivo sobre cómo y por qué se utiliza su información personal. Esto no solo fomenta la confianza en las plataformas digitales, sino que también garantiza el respeto por los derechos fundamentales de los individuos.

2.4. El derecho a la protección de datos personales en el contexto laboral

La administración de una entidad generalmente conlleva el manejo de información personal de los empleados con diversos propósitos como la contratación de personal, el cumplimiento de responsabilidades laborales y la supervisión de actividades dentro o fuera de la empresa (esto dependerá del tipo de actividades que se desarrollen).

A menudo, los empleadores no son conscientes de que están actuando como responsables legales de un sistema de información personal, lo que puede resultar en una administración inadecuada de los peligros y posibles sanciones. Asimismo, esta falta de conocimiento dificulta asegurar los derechos fundamentales de los trabajadores respecto a sus datos[44].

No hay cambios en la normativa específica, excepto en el caso de la videovigilancia, donde se evidencia la falta de jurisprudencia que analice la correcta alineación de estos principios con las necesidades de monitoreo y control de los empleadores. Esto genera, o, en su defecto, podría generar en el futuro, tensiones debido al avance tecnológico.

---

[43] Cáceres, *"El impacto de la inteligencia artificial en el Derecho"*, 63.
[44] Moore, *"El derecho fundamental a la protección de datos personales en el entorno laboral"*. 278-279.

A nivel internacional, existen lineamientos, como los proporcionados por la Organización Internacional del Trabajo (en adelante la OIT) en el documento *"Protection of Worker's Personal Data*", que ofrecen principios relevantes para la administración de estos datos, como son:

- La limitación del tratamiento de los datos personales de los empleados a asuntos relacionados con su vínculo laboral y hacerlo de manera justa y equitativa.
- El uso de los datos para propósitos establecidos.
- Los trabajadores tienen que revisar regularmente sus técnicas de tratamiento de datos para minimizar al máximo la clase y la cantidad de datos asociados y optimizar la protección de la privacidad de los empleados.
- Los sujetos que se ocupan del tratamiento de datos personales deben recibir capacitación regular para comprender el proceso de recopilación de datos y su función en la implementación de los principios.

Es importante destacar que, dentro del entorno laboral, la normativa peruana adopta los mismos principios de protección de datos personales establecidos en la LPDP. Por lo tanto, en el contexto contractual, el empleador no necesita obtener la autorización del trabajador para procesar sus datos personales, siempre que dicha gestión esté vinculada al contrato laboral. Esto conlleva que el empleador debe cumplir con ciertas obligaciones, como informar al trabajador, garantizar la proporcionalidad y salvaguardar la protección de la información, entre otros requisitos. Sin embargo, cuando los datos se utilizan para otros fines, como es el de publicidad, sí es necesario contar con dicho consentimiento[45].

Por ello, la protección de datos personales en el ámbito laboral implica que los empleadores deben manejar la información de los empleados de forma confidencial y segura, respetando sus derechos de privacidad y cumpliendo con las normativas vigentes sobre el tratamiento de datos en el ámbito laboral.

[45] Moore, *"El derecho fundamental a la protección de datos personales en el entorno laboral"*, 278-279

2.4.1. El poder de dirección del empleador

El poder de dirección del empleador es una facultad reconocida tanto por la ley como por el contrato de trabajo. Esta potestad es fundamental para el funcionamiento de la empresa, ya que le otorga al empleador el derecho a organizar y controlar la labor del trabajador. Este poder no solo incluye la capacidad de dar órdenes e impartir instrucciones, sino también la de supervisar y sancionar, garantizando el cumplimiento de las obligaciones del trabajador. Así, el poder de dirección implica un control técnico, económico y funcional, indispensable para coordinar la actividad laboral dentro de la empresa[46].

Por otro lado, el ejercicio de esta facultad está limitado por el respeto a los derechos del trabajador, como su dignidad y sus condiciones laborales esenciales. Además, aunque el empleador puede realizar modificaciones en la prestación de los servicios, estos no deben ser arbitrarios ni lesionar los intereses del trabajador. En definitiva, el poder de dirección está sujeto a la legalidad y debe ejercerse de manera equilibrada, buscando siempre el correcto funcionamiento de la empresa sin vulnerar los derechos laborales.

Lizama sostiene que en nuestro medio, el poder de dirección no tiene una denominación unívoca. Por lo tanto, la jurisprudencia administrativa y una parte de la doctrina nacional lo denominan "poder de mando", "poder de mando" o simplemente "poder de dirección"[47].

Según una parte de la doctrina, la base del poder de dirección se basa en el contrato de trabajo, el cual es otorgado al empleador y representa la subordinación, ya que el trabajador se somete a la autoridad del empleador como una característica esencial del contrato.

Sobre el poder de dirección del empleador, sostiene Vida, que incluye la facultad de supervisar y supervisar las acciones del trabajador. La teoría sostiene que el poder de control es una de las expresiones más importantes y controvertidas del poder de liderazgo[48].

---

[46] Rueda, "Poder de dirección del empleador, 1-865", 405-407.
[47] Portal, "*Manual de Derecho Individual del Trabajo"*, 113-114.
[48] José Vida Soria, Cristóbal Mouna Navarrete, *Manual de Derecho del Trabajo* (Granada: Comares S.L, 2003),488.

Este aspecto del poder de dirección no es nuevo, ya que ha existido desde el principio y se ha configurado como uno de sus instrumentos más adecuados para garantizar que el trabajador cumpla con su prestación laboral.

Dentro del poder de dirección, se encuentran las facultades de control y vigilancia, así como la supervisión de los trabajos realizados y el grado de cumplimiento de las órdenes del empleador, que están estrechamente relacionadas con el poder de dirección. Sin las facultades de control, el empresario no podría garantizar que se cumplan los mandatos, ya que el empleador podría burlarse fácilmente de ellos.[49]

En el caso de los empleadores que realizan actividades fuera del trabajo, a distancia o a domicilio, donde lo más importante es el resultado final de la tarea encomendada, se suele utilizar este control con más frecuencia. Por otro lado, la vigilancia tiene lugar generalmente en las labores realizadas en el lugar de trabajo controlado por el empleador, motivado también por las obligaciones propias de la seguridad, que requieren vigilar el trabajo ordenado.

El poder directivo del empleador no está limitado por la Ley. El ámbito de aplicación del contrato de trabajo lo limita y no puede adoptar la forma de una conducta activa o pasiva del trabajador para ejecutar los servicios encomendados. Además, su comportamiento en la empresa es una manifestación del poder de mando[50].

Como bien sabemos, todas las facultades no pueden ser ejercidas sin restricción alguna; en otras palabras, encuentra límites, no sólo circunscritos al ámbito laboral, sino que va más allá en protección de los derechos constitucionales de los trabajadores.

Aunque el empleado está sujeto a ciertas pautas impuestas por la libertad de organización de tendencia, esto no significa que esté completamente sujeto a ella. Las libertades generales que tenía antes de suscribir el contrato de trabajo se mantienen y deben ejercerse, excepto en casos específicos. Por supuesto, desde el punto de vista del empleador, los derechos fundamentales de los trabajadores

[49]Soria y Mouna Navarrete, *Manual de Derecho del Trabajo,* 488.
[50] Soria y Mouna Navarrete, *Manual de Derecho del Trabajo,* 488.

deben ser protegidos sin que esto implique que el empleador tenga que ajustar su organización para cumplir con los derechos fundamentales de los trabajadores.

Consecuentemente, se advierte que existe una serie de limitaciones o restricciones al uso desproporcionado del poder de dirección por parte del empleador. Por lo tanto, es necesario llevar a cabo una investigación sobre cada uno de estos controles, entre los que podemos mencionar: dignidad humana, igualdad de trato y dignidad.

2.4.2. Teletrabajo

La Ley N.° 30036, conocida como Ley del Teletrabajo, fue promulgada en Perú el 5 de junio de 2013, con el objetivo de establecer directrices generales para esta modalidad especial de prestación de servicios. La reglamentación de dicha ley llegó el 3 de noviembre de 2015, a través del Decreto Supremo N.° 017-2015-TR, proporcionando un marco regulatorio necesario para que las organizaciones pudieran implementar el teletrabajo de manera adecuada[51].

Aunque, la Ley del Teletrabajo ya había sido promulgada en 2013 y reglamentada en 2015, el teletrabajo no había sido adoptado de manera masiva en el país antes de la pandemia. Sin embargo, la emergencia sanitaria provocada por el Covid-19 aceleró significativamente su implementación, obligando a las empresas y al Estado a darle mayor relevancia y aplicarlo como una solución inmediata y necesaria para asegurar la continuidad laboral durante la crisis. Esta coyuntura resaltó la importancia de esta modalidad, que hasta entonces había sido vista como una alternativa limitada.

Así, en el Perú, al igual que en muchos otros países, la pandemia causada por el Covid-19 impulsó de manera inevitable la implementación del trabajo remoto o teletrabajo. Durante este período, el Decreto de Urgencia N.° 026-2020, publicado el 15 de marzo de 2020, permitió la adopción de esta modalidad laboral como medida de emergencia para contener la propagación del virus.

---

[51] Fernandez y González Torres, *"El teletrabajo: Una innovadora forma de organización del trabajo, una herramienta de inclusión laboral y su regulación jurídica en el Perú"*, 102.

Posteriormente, la Ley N.° 31572, promulgada el 14 de septiembre de 2022, estableció el retorno gradual a la presencialidad, derogando las disposiciones temporales que regían el teletrabajo[52].

No obstante, con fecha 22 de julio del 2024 se modificó la Ley del Teletrabajo mediante la Ley 32102 (Ley que modifica la Ley 31572, respecto a los derechos y deberes de los teletrabajadores). Con esta modificatoria se implementaron diferentes cambios en esta modalidad de trabajo, uno de los más relevantes fue el relacionado con la prohibición de que el teletrabajador abandone su lugar habitual de teletrabajo y realicé actividades particulares. De esta manera, con la modificatoria señalada en caso de que el teletrabajador abandone su lugar de teletrabajo deberá justificarlo. En caso contrario podrá ser sancionado incluso con la reversión de la modalidad de teletrabajo a trabajo presencial.

Por otro lado, se establecen criterios sobre los derechos del teletrabajador contemplando los supuestos en los que se interrumpa la prestación de aquél por causas ajenas a su voluntad como los cortes de electricidad e internet, imposibilitando que dichas interrupciones puedan ser objetos de descuentos por parte del empleador. Además, se establece que el lugar desempeñado para la ejecución de labores por parte del teletrabajador será de conocimiento expreso del empleador y, en caso de que se cambie dicho lugar, el teletrabajador deberá informar con una anticipación de 5 días hábiles.

En esa línea, estas modificaciones tienden a restarle flexibilidad a la modalidad de teletrabajo, abriendo paso a que se consideren a los mecanismos de fiscalización laboral, materia de la presente investigación. En este contexto, las modificaciones propuestas limitan la flexibilidad del teletrabajo al permitir que se apliquen mecanismos de supervisión laboral.

Lo anterior se explica en la medida en la que la norma ha previsto el supuesto de sanciones para los teletrabajadores que cambien el lugar desde donde desarrollan el teletrabajo o cuando abandonen injustificadamente su posición dentro de su jornada laboral. Es decir, la posibilidad de establecer un marco de responsabilidad y control en el teletrabajo.

---

[52] Villasante, *"El teletrabajo en el Perú. Evolución normativa"*, Lp Pasión por el Derecho.

En atención a ello el empleador podría disponer del uso de geolocalizadores como el GPS para asegurar el lugar desde donde se desarrolla el teletrabajo o en su defecto pedirle al teletrabajador que encienda su cámara durante su jornada de trabajo a fin de garantizar que se encuentre en su lugar habitual y no desarrolle actividades extraoficiales durante su jornada de trabajo. Sin embargo, las medidas señaladas solo serán válidas siempre y cuando se ajusten a los principios de razonabilidad, seguridad y finalidad que hemos desarrollado previamente.

Cabe resaltar que por ejemplo no resultaría razonable que se obligue al teletrabajador estar con su cámara encendida durante las 8 horas de su jornada, toda vez que su lugar de teletrabajo podría tratarse tranquilamente de su hogar y por tanto al mantener encendida la cámara durante la jornada completa el teletrabajador estaría develando aspectos de su vida personal que no incumben al empleador y que en cambio vulneran el derecho a la protección de la información personal del teletrabajador y a los derechos correlacionados con la señalada materia.

En síntesis, si bien pueden aplicarse medidas de fiscalización laboral que se soporten en las nuevas tecnologías (como la geolocalización por GPS o la videovigilancia) en el teletrabajo, dichas medidas aunque puedan sustentarse en la última modificatoria con la Ley 32102, no podrán ser aplicados salvo que se encuentren en armonía con los principios rectores señalados anteriormente y siempre que no vulneren los derechos fundamentales derivados del derecho de protección de datos a los trabajadores.

2.4.3. Sistemas de Geolocalización

2.4.3.1. Concepto

El sistema de geolocalización, o denominado como Global Positioning System, fue construido por Estados Unidos, inicialmente para fines militares. Posteriormente, fue implementado en otros sectores como el minero, aeronáutica, transporte ferroviario, marítimo y para otros fines que no fueron pensados[53].

[53] Gobierno de los Estados Unidos. “El sistema de posicionamiento global”, GPS.GOV, 17 de octubre de 2020, :https://www.gps.gov/systems/gps/spanish.php

Este se compone de tres elementos: la sección espacial incluye un conjunto de 24 satélites activos que emiten señales en una sola dirección, proporcionando información sobre la ubicación y el tiempo de los satélites del GPS; la sección de control está formada por terminales encargadas de monitorear y gestionar, repartidas globalmente, para asegurar que los satélites permanezcan en la órbita correcta; estas estaciones también vigilan los satélites GPS y garantizan el adecuado desenvolvimiento del sistema. Finalmente, el segmento de usuario, que representa los dispositivos receptores del GPS, capta las señales emitidas por los satélites GPS y las procesa con el fin de calcular la ubicación y la hora precisa.

Aunque no es ideal, este sistema permite localizar a individuos u objetos en cualquier lugar del mundo con un margen de error de entre 30 y 50 metros y monitorear e inscribir todos sus movimientos en el posicionamiento global de un "objetivo", lo que hace que las fronteras físicas no representen una limitación para su seguimiento. En resumen, este sistema resulta efectivo para monitorear ubicaciones y movimientos a nivel global, a pesar de algunas limitaciones.

Si bien esta tecnología otorga ventajas evidentes, su empleo no está libre de inseguridades y peligros, siendo el primordial la transgresión de la intimidad. Esto se debe a la cercanía del vínculo entre los individuos y el dispositivo electrónico, lo cual propicia la identificación de la situación geográfica de los terminales y, a la vez, el reconocimiento directo y veloz del propietario del dispositivo. Entonces, resulta suficiente colocar la relación de los datos de posición geográfica de un terminal con los datos de quien exhibe su propiedad, para así poder comprender y saber detalles íntimos de la vida de las personas.

Este alto grado de probabilidad de que este tipo de tecnología impacte negativamente en la intimidad de las personas representa un tema de suma relevancia internacional.

Sobre este punto, debemos señalar que la Agencia Española de Protección de Datos ha expuesto en reiteradas resoluciones, como es el Dictamen aprobado por el Grupo de Trabajo del 16 de mayo del 2011[54] y en la Sentencia del Caso Uzun vs Alemania del 2 de Septiembre del 2010, emitido por el Tribunal Europeo[55], la conclusión de que el uso de la geolocalización permanente sí afecta a la vida privada de los sujetos.

2.4.3.2. Los sistemas de geolocalización en el mundo empresarial

Nuestra Autoridad Nacional de Protección de Datos personales, a través del Expediente 14-2016-RD-08-2007-DGPDP ha expresado que la geolocalización se comprende como la ubicación geográfica de un objeto o sujeto en el espacio, la medición se lleva a cabo a través de coordenadas geográficas, las cuales son coordenadas de latitud y longitud.

Algunas de las funciones del GPS son la localización del objeto en el tiempo real, visualización de las rutas recorridas, visualización del trayecto recorrido con exceso de velocidad, localización de vehículos, calles próximas y creación de alarmas, información estadística que faculta realizar informes de distancia día por día, por períodos, etc[56].

Naturalmente, las empresas buscan aumentar su eficiencia y productividad en un mundo globalizado, interconectado y competitivo. En ese sentido, para lograrlo, crean varias estrategias que incluyen la incorporación de diversas tecnologías que les permitan alcanzar sus objetivos empresariales de manera más efectiva, a través del uso del GPS.

Para lo cual, se enumerarán algunas necesidades que pueden satisfacer las empresas mediante la instrumentalización del sistema mencionado. Las empresas pueden colocarlo en los vehículos de sus empleados para tener un control total sobre sus viajes, y se ha sugerido que las compañías de seguros utilicen los datos recopilados para monitorear el

[54] Agencia Española de Protección de Datos, "Publicaciones y resoluciones", AEPD, 8 de octubre de 2024, https://www.aepd.es/publicaciones-y-resoluciones.
[55] Tribunal Europeo de Derechos Humanos, *Uzum vs Alemania*, sentencia de 2 de septiembre de 2010.
[56] Tribunal Superior de Justicia de Asturias, STSJ. ASTURIAS 3058/2017, de 27 de diciembre de 2017.

comportamiento de sus clientes, también, para poder rastrear la mercancía enviada y ver un status en tiempo real de esta, además, de poder usar la información entregada por el sistema para replantear su estrategia comercial y disminuir los tiempos de distribución de sus productos. Como se puede ver, son diversos los usos productivos que las empresas pueden darle a esta tecnología.

No obstante, no debe dejarse de lado que también existen razones de seguridad que pueden sustentar su uso empresarial, los GPS instalados en los automóviles de la empresa nos permite acceder a la información geográfica de dichos vehículos ante eventuales robos de los vehículos, incluso de la mercadería que se encuentra de estos, nos permite mandar alertas sobre los frecuentes excesos de velocidad u otros hechos que son relevantes en el curso de conducción.

Para los fines del presente trabajo, en el siguiente acápite, se analizará el uso del sistema de geolocalización como dispositivo y mecanismo de control laboral en un escenario en el cual no sería posible que el empleador pueda efectuar una inspección minuciosa sobre las actividades asignadas, salvo con el uso de dicha tecnología.

2.4.2.3. Los datos personales derivados de la geolocalización

La investigación actual se centra principalmente en el tratamiento de los datos de geolocalización y videovigilancia de los empleados, obtenidos mediante las potestades de intervención y vigilancia de los empleadores. Sin perjuicio de ello, en este apartado nos centraremos en evaluar si los datos recopilados por el sistema GPS son considerados datos personales y, consecuentemente, determinar su tratamiento en aplicación a la legislación peruana. Lo anterior será desarrollado en el siguiente orden:

2.4.2.3.1 Tratamiento de datos de geolocalización en la normativa nacional y extranjera

La LPDP, en el numeral 4 del art. 2, especifica que "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados"[57].

En esa misma dirección, la ANPDP mencionó que una persona es identificable de forma directa o indirecta, debido a que para identificarse, será necesario integrar el nombre con otras características de identificación tales como, su fecha de nacimiento, dirección actual, DNI, entre otros.

Para la Agencia Española no será un sujeto identificable si se "requiere plazos o actividades desproporcionadas". Asimismo, manifestó la autoridad que no es "imprescindible para que exista un dato personal, una plena coincidencia entre el dato y una información concreta", será suficiente para realizar dicha identificación sin esfuerzos desproporcionados[58].

La geolocalización, como hemos mencionado, proporciona detalles sobre la localización exacta de un objeto en tiempo real, así como sus desplazamientos y el tiempo que le tomaría ir de un lugar a otro, además de los períodos de pausa o detención. Es decir, cualquier persona que cuente con un dispositivo moderno, el cual tenga integrado un GPS, podrá ser ubicada en tiempo real.

El uso de este tipo de tecnologías es un arma de doble filo. Es evidente las ventajas que puede obtener el empleador, al igual que es evidente la preocupación sobre el monitoreo constante de los trabajadores.

---

[57] Ley 29733

[58] Agencia Española de Protección de Datos, *"Publicaciones y resoluciones"*, AEPD.

Podríamos estar frente a una trasgresión a la intimidad, dado que el empleador sabría la posición geográfica exacta de todos sus trabajadores ya que estos estarían conectados al sistema GPS.

Lo anterior, ha sido reafirmado a nivel jurisprudencial por la Agencia Española de Protección de Datos, la cual sostuvo que la información producida por el dispositivo electrónico referida a la ubicación geográfica de un sujeto identificado o identificable, siempre constituye un dato personal[59].

De manera similar, el Parlamento Europeo, en el art. 2 de la Directiva 2002/58/CE, relacionada con la gestión de datos personales, establece que la información de ubicación, como los datos procesados en una red de telecomunicaciones electrónicas, muestra la posición geográfica del dispositivo terminal de un usuario de servicios de comunicación electrónica accesibles al público[60].

2.4.3.4. El tratamiento del uso del GPS como mecanismo de monitoreo laboral

En el Perú, aún existe una insuficiencia a nivel legislativo respecto a la instrumentalización del GPS en el contexto laboral, entonces con la intención de alcanzar los objetivos propuestos en este trabajo de suficiencia profesional, se efectuará una búsqueda en nuestros órganos jurisdiccionales, entiéndase, el Tribunal Constitucional y Poder Judicial.

En primer lugar, respecto al Tribunal Constitucional, no se ha hallado ninguna sentencia cuya materia controvertida sea el uso de los GPS como mecanismo de control.

[59] Agencia Española de Protección de Datos, *"Publicaciones y resoluciones"*, AEPD.
[60] Directiva 2002/58/CE

En segundo lugar, respecto al Poder judicial, se ha encontrado un Pleno Jurisdiccional Regional Laboral de Chiclayo del año 2010[61], del cual respecto a lo que nos concierne, se puede identificar que el Pleno jurisdiccional opta por la posición de considerar el GPS como un método de supervisión directo del empleador; sin embargo, en el mencionado pleno no se desarrolla un análisis desde la perspectiva de protección de datos personales de los empleados.

Por otro lado, se logró identificar la Casación Laboral N.º3776-2015- La libertad, cuya materia fue de despido arbitrario. Si bien es cierto que la Corte Suprema confirmó la sentencia de la Corte Superior que revocó la sentencia que declaró infundada la demanda, no debe desatenderse el argumento que sustenta su fallo, ello según se detalla a continuación:

> (...)*" Según la Casación Laboral N° 3776-2015, establece que no se han probado los hechos atribuidos al demandante durante el proceso. Dado que no se demostró que se encontrara en la localidad de Casa Grande los días dos y tres de marzo del 2012, ya que la empresa basó sus acusaciones en datos de un sistema GPS que no se encontraba homologado. Esto genera dudas sobre la fiabilidad de la información proporcionada por este geolocalizador en ese momento. Además se ha comprobado que el demandante trabajó el dos de marzo en Compin, donde pasó la noche antes de regresar a Trujillo al día siguiente. Por lo tanto, se concluye que el despido del demandante fue fraudulento).*

Así, se advierte que la Corte no hubiese tenido reparos en considerar la información suministrada por el GPS como válida siempre y que hubiese existido una homologación[62].

---

[61] Poder Judicial de Perú. "Plenos Jurisdiccionales". Poder Judicial de Perú. 13 de octubre de 2024. https://www.pj.gob.pe/wps/wcm/connect/cij/s_corte_suprema_utilitarios/as_home/as_cij/as_plenos_jurisdiccionales/

[62] Casación Laboral N° 3776-2015

2.4.4. La Videovigilancia

Como sostuvo Blume Moore, los datos personales protegidos por LDPD incluye la voz y las imágenes de una persona grabadas por tecnologías como las cámaras de videovigilancia[63].

Este es uno de los pocos casos en los que el Perú ha creado una directiva específica para aplicar el derecho a la protección de datos, como muestra esta la directiva que entró en vigencia el 16 de marzo de 2020 sobre el tratamiento de datos personales a través de sistemas de videovigilancia.

En la Directiva N.º001-2020- JUS/DGTAI-PD-2020, se han desarrollado las responsabilidades, compromisos y consejos aplicables en el ámbito laboral, las cuales son:

- El consentimiento: Salvo en casos que no estén sujetos a su poder de dirección, que incluye el control, supervisión de las labores, protección de bienes, seguridad y salud en el trabajo, entre otros, la empresa no requiere el consentimiento de sus empleados[64].

- Proporcionalidad: Este principio dicta que las cámaras de videovigilancia no deben estar en áreas de descanso, vestuarios o baños. La videovigilancia debe ser apropiada, relevante y no excesiva en comparación con el propósito y el área en la que se instalaron las cámaras[65].

- Conservación: Las grabaciones de imágenes o voces deben almacenarse entre 30 y 60 días. Si contienen pruebas de posibles infracciones laborales o accidentes de trabajo, deben conservarse por 120 días., a menos que existan razones justificadas para conservarlas por un período mayor. Vale, precisar que se debe notificar de inmediato a la autoridad si hay indicios de delito o

[63] Moore, *"Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales"*,1.
[64] Directiva N° 01-2020-JUS/DGTAI-PD, de 16 de enero de 2020, Tratamiento de Datos Personales mediante Sistemas de Videovigilancia. (Lima, 17 de marzo de 2020).
[65] Directiva N° 01-2020-JUS/DGTAI-PD

falta. Además, estos archivos serán eliminados dentro de los dos días hábiles del plazo máximo.

- Derecho de acceso: Los empleados podrán solicitar ver las grabaciones o a una copia digital de cualquier error o incumplimiento que se les haya atribuido.

- Registrar bases de datos: Los sistemas de videovigilancia que implican la propiedad de una o más bases de datos deben registrarse ante la autoridad de protección de datos personales, al igual que con cualquier dato.

- Medidas de seguridad: Las imágenes capturadas por los sistemas de video deben mantenerse garantizadas y confidenciales, y la empresa debe evitar la alteración, la pérdida, el tratamiento o el acceso no autorizado. Se sugiere, por ello, implementar las medidas técnicas, organizativas y legales que correspondan.

- Informar: Cada área de videovigilancia debe contar con un cartel visible que contraste con la pared, informando sobre la identidad y ubicación de la empresa, así como sobre cómo los individuos pueden ejercer sus derechos dentro de esta entidad. Esta información deberá realizarse a través de colocación de letreros claros y precisos para el público objetivo.

- No afectar a terceros: La empresa debe prever medidas que eviten la captación de imágenes de personas ajenas.

- Confidencialidad: Es necesario que se celebren acuerdos de confidencialidad con las personas que van a desempeñar la labor de videovigilancia.

- Derechos ARCO: Se fijan normas específicas para que los titulares ejerzan uso de sus prerrogativas como los derechos de cancelación, rectificación, oposición y acceso.

Pese a estas regulaciones, la implementación de videovigilancia en el trabajo genera preocupaciones sobre hasta qué punto se respeta la privacidad de los empleados. También menciona el desafío de equilibrar la protección de la información personal con las necesidades de monitoreo por parte del empleador.

La OIT a través del international labour office[66] dispuso que los empleadores pueden supervisar a sus empleados a través del uso de la videovigilancia, pero deben ejecutarse previendo ciertos requisitos, como se indicó en los párrafos anteriores, conforme a la directiva peruana. Asimismo, se señala que este sistema puede usarse siempre y que los empleados estén debidamente informados, nada debe realizarse de manera oculta. También, se señala que los empleadores no son autónomos de la toma de elección del método de monitoreo, sino que debe atenderse el impacto que estas pueden tener en la privacidad de los trabajadores, es así que debe favorecer los medios menos gravosos.

Debe indicarse que en el caso del monitoreo oculto es mucho más limitante, puesto que solo deberá restringirse a los casos en los que el monitoreo es necesario para abordar problemas específicos de seguridad y salud o protección de la propiedad.

La observancia de las recomendaciones antes mencionadas refleja la necesidad de incorporar factores subjetivos como la intencionalidad del empleador y sus razones para hacer uso de dicho sistema.

En relación a ello, dentro de la casuística existe una jurisprudencia del 25 de Septiembre del 2020 donde el TC acordó desestimar una demanda interpuesta por el Sindicato de obreros de P y AD'Onofrio S.A. cuya pretensión fue que se ordene el retiro de un sistema de cámaras de videovigilancia implementada en las áreas de fabricación y depósito, en tanto que se vulnerara su derecho a la dignidad e intimidad.

En el Expediente Nº002208-2017-PA/TCM 2020, el TC resolvió que la empresa demandada cumplio con informar a los empleadores sobre la instalación de cámaras de seguridad. Asimismo, se determinó que el uso de las cámaras era proporcional a los fines perseguidos, ya que su implementación se realizó en

[66] Organización Internacional del Trabajo, “Conferencia Internacional del trabajo”, Organización Internacional del Trabajo, 9 de octubre de 2024, https://www.ilo.org/es

zonas no íntimas, respetando así la privacidad de los trabajadores. Esto es sumamente relevante pues otorga una legitimidad al uso de esta tecnología como mecanismo de control en el ámbito laboral y se acentúa la trascendencia de la proporcionalidad para la utilización de esta tecnología.

Aunque, se mencionó que existe un deber de información de los empleadores, el Tribunal Europeo de los Derechos Humanos a través del caso Lopez Ribalda[67],en el cual se tolero la falta de información, debido a que habían dudas suficientes de que había inobservancias graves de las obligaciones laborales, por ejemplo, robo a la empresa.

2.5. Análisis Casuístico

Como se ha señalado a lo largo de la presente investigación, en nuestro país no contamos con un ordenamiento jurídico que contemple expresamente la protección de datos personales ante el uso de Tecnologías de la Información y Comunicación(en adelante TIC), específicamente aquellas que se realicen en el marco del poder de fiscalización del empleador como las de monitoreo digital por GPS o videovigilancia.

Sin perjuicio de ello, con el propósito de tener un panorama más claro del tratamiento de datos personales en los señalados supuestos en Perú y conocer el impacto que ha generado dicho tratamiento de datos personales, hemos procedido a realizar una búsqueda de los casos más relevantes dentro de las instancias judiciales y constitucionales; así como en resoluciones administrativas. Con lo cual a continuación esbozaremos algunos de los más relevantes:

A. Sentencias de Casación Laboral y del Tribunal Constitucional

De la revisión realizada en la consulta de expedientes judiciales y Recursos de Casación, se han podido identificar 2 sentencias, en las cuales se hace alusión a la protección de datos personales de los trabajadores en el marco de una relación de trabajo y cuando su uso es razonable y legítimo.

[67] Tribunal Europeo de Derechos Humanos. EXP N°1874 -2018

i. Casación Laboral N° 14614-2016

El caso desarrollado por la Corte Suprema en la casación señalada se circunscribe en un proceso seguido por Nestlé Perú S.A.(en adelante Nestlé o la Empresa), contra el Sindicato Único Nacional de Trabajadores, es así que la referida empresa interpone el recurso con la finalidad de anular la sentencia de vista, la cual confirma en parte el fallo de primera instancia, mediante el cual declaran fundada en parte la pretensión del Sindicato.

Sobre este particular, debemos precisar que la controversia en el presente proceso surge debido a la modificación del Reglamento Interno de Trabajo de Nestlé, quien dentro del referido documento pretendía atribuirse la propiedad de la información que pudiera hallarse en los equipos suministrados por dicha empresa, tales como el equipo de cómputo, el celular, entre otros dispositivos.

Así las cosas, el sindicato como contraparte impugna el referido reglamento mediante un proceso judicial, el cual es fundado en primera instancia y confirmado en parte en segunda; por lo que la empresa decide elevarlo a través de un Recurso de Casación ante la Corte Suprema. En esa línea, tenemos que la Suprema se pronuncia, señalando lo siguiente en su considerando Décimo Cuarto:

> (...)*"Sin duda, el uso por parte de los trabajadores de los elementos proporcionados por la empresa para fines personales constituye un incumplimiento contractual susceptible de ser sancionado por el empleador; y naturalmente la aparición de nuevas tecnologías ha mostrado que los empleadores hacen uso de nuevos sistemas de control de la actividad laboral de los trabajadores. Sin embargo, está facultad de control reconocida a nivel doctrinario como en la legislación interna como lógica consecuencia al poder de dirección no es irrestricta.*

> *Dicho control empresarial encuentra sus límites en que su ejercicio sea funcional y racional. Es funcional porque debe estar relacionado al contexto empresarial y el empleador no puede controlar la esfera privada del dependiente; por otro lado, cuando se dice que el control debe ser racional se parte de la idea de que el control debe ser el resultado de un proceso intelectual que lo justifique y que dé razón al proceso de toma de decisión).*

En síntesis, el pronunciamiento que nos ocupa ha delimitado que si bien el empleador en el ejercicio de su poder de dirección y a la luz de las nuevas tecnologías, puede hacer uso de estas últimas para fiscalizar la actividad de su personal, ello no lo faculta para que con dicho uso pueda acceder a datos personales de los colaboradores, a pesar de que dichas acciones de configuren en el marco de una relación de trabajo.

De esta manera, el colegiado citado ha establecido un precedente importante al señalar que el poder de dirección no es irrestricto, por el contrario precisa que el mismo debe encontrar límites funcionales y racionales, dejando en claro que bajo ningún supuesto puede vulnerar derechos fundamentales como el derecho a la privacidad o intimidad del trabajador. En dicho sentido, se deja en claro que el tratamiento de datos personales dentro de una relación laboral se da bajo criterios válidos y sin colisionar con los derechos fundamentales del dependiente.

ii. Tribunal Constitucional, EXP.N° 00943-2016-PA/TC

Resumen: El presente expediente en cuestión versa sobre el recurso de agravio constitucional interpuesto por el señor Marco Antonio Paucarcaja Mercado contra la resolución de la Sala Civil de la Corte Superior de Justicia de Huaura que declaró improcedente su demanda de amparo contra Emapa Huaral S.A.

En su demanda, el recurrente denuncia haber sido víctima de despido arbitrario por parte de la empresa, lo que considera una vulneración de sus derechos constitucionales al trabajo, al secreto y la inviolabilidad de las comunicaciones, así como de su presunción de inocencia y el debido proceso.

El señor Paucarcaja alegó que su despido carece de justificación, ya que la empresa fundamentó sus acusaciones en conversaciones privadas que él mantuvo a través de la red social Facebook con la asistente del Jefe de Logística, así como en la presunta manipulación de información confidencial de la empresa, entre la que se incluyen claves de seguridad de un sistema de información reservada por parte de la empresa. Además, reclamó que su derecho al debido proceso fue vulnerado, ya que la carta de despido fue emitida antes de que pudiera hacer sus descargos del caso.

Asimismo, la sentencia emitida por el Tribunal Constitucional discutió la magnitud de la intervención del empleador en las conversaciones privadas de sus empleados, considerando que los mensajes fueron intercambiados a través de redes sociales. El Tribunal señaló que esta intervención podría vulnerar el derecho al secreto y la inviolabilidad de las comunicaciones, salvo en situaciones excepcionales y debidamente justificadas. La intervención puede justificarse en situaciones en las que el trabajador otorgue su consentimiento expreso para el monitoreo de sus comunicaciones. Sin embargo, la información recopilada no debe referirse a la vida privada del trabajador, sino únicamente a datos relevantes para la actividad empresarial

Por esta razón, el Tribunal Constitucional ha declarado fundada la demanda, reconociendo la vulneración de los derechos al trabajo y al debido proceso. En consecuencia, se declara nulo el despido arbitrario y se ordena la reincorporación del señor Paucarcaja a la empresa, ya sea en el mismo cargo que ocupaba o en uno de igual o similar categoría.

Hechos relevantes:

El día 14 de octubre de 2014, Emapa Huaral S.A. le notifico al señor Paucarcaja sobre la apertura de un proceso sancionador en relación con sus funciones dentro de la empresa. Entre dichos incumplimientos se menciona: i) manipular información privada de la empresa y ii) no cumplir con la entrega de un informe de cuentas dentro de un periodo estipulado.

Ante esta situación, el señor Paucarcaja interpone una demanda de amparo contra Emapa Huaral S.A. Medio por el cual solicita dejar sin efecto el despido arbitrario emitido por dicha entidad y, en consecuencia, la restitución en su puesto de técnico en catastro comercial, el cual había estado desempeñando.

Que, con respecto a la primera falta, esta acusación se sustenta en conversaciones privadas obtenidas a través de Facebook con la asistente del Jefe de Logística.

Tras revisar las conversaciones a través de Facebook entre el señor Paucarcaja y la asistente del Jefe de Logística, se corrobora que el señor Paucarcaja solicitó la clave de acceso al Sistema de Logística, información de la cual la asistente no disponía. Sin embargo, no se demuestra que haya ingresado a dicho sistema.

El Tribunal reconoce que los empleadores tienen la autoridad para supervisar e intervenir en los correos electrónicos corporativos y monitorear las comunicaciones realizadas a través de este medio, siempre que se respete el principio de proporcionalidad para salvaguardar los derechos del trabajador. No obstante, es necesario evaluar si el empleador puede intervenir en las redes sociales de sus trabajadores o por el contrario, esto constituye una violación del derecho fundamental al secreto e inviolabilidad de las comunicaciones.

Las conversaciones fueron obtenidas a través de Facebook, una red social que no está relacionada con la empresa. Por lo tanto, este medio no debe recibir el mismo tratamiento que un correo electrónico corporativo,

lo que implica que intervenir en esas comunicaciones constituye una violación del derecho al secreto y a la inviolabilidad de las comunicaciones.

Valoración jurídica personal: El fallo del Tribunal Constitucional demuestra la diferencia que existe entre una comunicación vía correo corporativo y una red social. Por tal motivo, se determina que la privacidad de los trabajadores debe ser respetada y no vulnerada, especialmente en el caso de querer intervenir en sus comunicaciones privadas vía red social. La intervención en estos canales de comunicación, sin una justificación adecuada y sin tener en cuenta los principios como el de proporcionalidad o la notificación previa al trabajador, constituye una violación del derecho al secreto y a la inviolabilidad de las comunicaciones. En consecuencia, este fallo salvaguarda la privacidad del trabajador y prohíbe que el empleador utilice pruebas obtenidas de manera injustificada para sancionar o despedir a su personal.

CAPÍTULO III: CONCLUSIONES Y RECOMENDACIONES

3.1. Conclusiones

- Nuestra legislación nacional garantiza el derecho a la protección de datos personales, reconocido en el inciso 6 del art. 2 de la Constitución Política del Perú. Este derecho otorga a los titulares dos facultades clave: la disposición de sus datos, que se manifiesta a través del consentimiento, y el control sobre su información.

- En el ámbito laboral, este derecho tiene una especial relevancia, puesto que los empleadores se encuentran premunidos por el poder de dirección, el cual les permite implementar mecanismos de control y/o fiscalización necesarios para cumplir con su rol fiscalizador y de esta manera supervisar las obligaciones que se generan a partir del contrato de trabajo. Sin embargo, el señalado poder de dirección no supone un poder absoluto e ilimitado por parte del empleador, sino

que el poder de dirección se encontrará circunscrito a la observancia de los derechos fundamentales del trabajador.

- Si bien los empleados tienen el derecho de controlar la información, mediante el consentimiento y los derechos ARCO, los empleadores también tienen la facultad de supervisar y fiscalizar el cumplimiento de las obligaciones laborales. Esto genera la necesidad de encontrar un equilibrio entre ambos intereses, garantizando que el poder de dirección empresarial no vulnere los derechos fundamentales de los trabajadores.

- En ese sentido, el uso de nuevas tecnologías como el monitoreo por GPS o videovigilancia sí es posible de ser implementado como mecanismo de fiscalización hacia la actividad de los trabajadores, empero estas medidas deberán garantizar el respeto irrestricto a los derechos constitucionales de los trabajadores, entre ellos el derecho a la intimidad, privacidad y dignidad, los cuales se encuentran incluídos dentro del derecho de protección de datos personales.

- Sin embargo, aunque estas tecnologías pueden ser utilizadas, no existe en nuestro marco normativo una legislación específica que regule el uso de la tecnología GPS como medio de control laboral. Además, no se cuenta con una casuística directa que proporcione orientación sobre cómo debe llevarse a cabo el tratamiento de los datos geolocalizados en el contexto laboral.

- Sin perjuicio de ello, contamos con criterios generales para sostener que el uso y tratamiento de datos personales obtenidos por mecanismos de fiscalización mediante el uso nuevas tecnologías como el GPS o la videovigilancia, sí puede implementarse en la medida que dichos sistemas de monitoreo se encuentren en armonía con los derechos fundamentales de los trabajadores, como los derechos a la intimidad, privacidad y dignidad del dependiente. Aunado a ello, estos sistemas se deben integrar partiendo de principios de funcionalidad, finalidad, seguridad y razonabilidad.

3.2. Recomendaciones

- Consideramos que el Reglamento de la LPDP debe incluir un apartado que desarrolle el tratamiento de datos personales a partir del uso de Tecnologías de Información y Comunicación como mecanismo de fiscalización laboral, tal y como se ha hecho en la legislación Española. En específico, proponemos que se establezca un límite basado en los derechos fundamentales de la persona humana, como el derecho a la intimidad del trabajador.

- Sin perjuicio de ello, la ANPDP debe emitir una Directiva donde sean estipulados los lineamientos y pautas que deberán ser observadas por los empleadores, a fin de que se realice un uso proporcional y legítimo del GPS como medio de control laboral.

BIBLIOGRAFÍA

Libros

Lizama Portal, Luis. *Manual de Derecho Individual del Trabajo*. Santiago de Chile: Ediciones DER, Santiago, 2019.

Vida Soria, José y Cristóbal Mouna Navarrete, *Manual de Derecho del Trabajo* (Granada: Comares S.L, 2003.

Capítulo de libros

Hernández Rueda, Lupo. "Poder de dirección del empleador" En *Instituciones de derecho del trabajo y de la seguridad social.* Ciudad de México: Instituto de Investigaciones Jurídicas, 1997

Marecos Gamarra, Adriana Raquel. "La protección de datos personales como núcleo del derecho fundamental a la autodeterminación informativa.Una mirada desde el derecho español y europeo. En *Protección de datos personales*. Asunción: Corte Suprema de Justicia, 2010

Artículo de revistas académicas impresas

Culqui Fernandez, Angela y Adela González Torres. "El teletrabajo: Una innovadora forma de organización del trabajo, una herramienta de inclusión laboral y su regulación jurídica en el Perú". *Revista Derecho & Sociedad,* no.46 (2016): 95-109.

Hernández Peña, Jesús. "Breves reflexiones sobre la responsabilidad civil derivada del tratamiento indebido de datos personales en el Perú". *Revista Foro Jurídico*, no.20 (2022): 335-360.

Mubarak Aguad, Laisha. "El internet, el Bigdata y el tratamiento de datos personales". *Advocatus,* no.36 (2017): 205-223.

Morales Cáceres, Alejandro. "El impacto de la inteligencia artificial en el Derecho". *Advocatus,* no. 39 (2021): 40-72.

Vásquez Rodríguez, Raúl. “ La responsabilidad proactiva en la normativa peruana de protección de datos personales”. *Yachaq: Revista de Derecho,* no. 13 (2022): 25-37.

Artículo de revistas académicas electrónicas

Alvarado, Francisco Javier. “La gestión de la seguridad de la información en el Régimen Peruano de Protección de Datos Personales. *Foro Jurídico*, no 15 (2016): 26-41. https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19833.

Blume Moore, Iván. “Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales”. *THEMIS Revista De Derecho*, no. 79 (2021): 435-49. https://doi.org/10.18800/themis.202101.025.

Blancas Bustamante, Carlos. “La Constitución de 1979 y el derecho del trabajo”. *Derecho PUCP*, no 36 (1982): 7-53. https://doi.org/10.18800/derechopucp.198201.001.

Blume Moore, Iván. “El derecho fundamental a la protección de datos personales en el entorno laboral”. *Laborem,* no. 24 (2021): 265-287. https://www.spdtss.org.pe/wp-content/uploads/2021/09/Laborem24-12-1.pdf.

Espinoza Espinoza, Juan. “La tutela jurídica del tratamiento de los datos personales frente a los avances de la información. Propuesta para un redimensionamiento del denominado derecho general de la personalidad y para una definición común del denominado hábeas data”. *IUS ET VERITAS* 10, no. 20 (2000): 86-108. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15926.

Eguiguren Praeli, Francisco José. “El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú”. *THEMIS Revista De Derecho*, no. 67 (2015): 131-140. https://revistas.pucp.edu.pe/index.php/themis/article/view/14462.

Fernández Toledo, Raúl. "Configuración del poder de dirección del empleador: denominación, naturaleza jurídica, fundamento y contenido". *Revista de Derecho,* no.245 (2019): 52-97. https://www.scielo.cl/pdf/revderudec/v87n245/0718-591X-revderudec-87-245-00051.pdf

Fernández Sessarego, Carlos. "Las personas, el personalismo y la constitución peruana de 1979". *Derecho PUCP*, no.36 (1982): 81-95. https://doi.org/10.18800/derechopucp.198201.004.

Galvis Cano, Lucero y Daniel Alexander Pesca Mesa. "Límites del tratamiento de los datos personales en el ámbito laboral frente al uso de las tecnologías de la información y comunicación en la era digital". *IUSTA*, no. 52 (2020): 51-76. https://doi.org/10.15332/25005286.5482.

Luna Cervantes, Eduardo Javier. "Preguntas y respuestas varias sobre la protección de datos personales en el Perú". *Advocatus*, no. 039 (2021): 253-64. https://doi.org/10.26439/advocatus2021.n39.5133.

Olivos Celis, Milagros. "El derecho a la protección de datos personales en el Perú: 27 años desde su incorporación en la constitución política de 1993". *IUS: Revista De investigación De La Facultad De Derecho* 9, no.1 (2020): 83-100. https://doi.org/10.35383/ius-usat.v9i1.338.

Ojeda Bello, Zahira. "El derecho a la protección de datos personales desde un análisis histórico-doctrinal". *Tla-melaua*, no.38 (2015): 58-70.https://www.scielo.org.mx/pdf/tla/v9n38/1870-6916-tla-9-38-00058.pdf

Quiroz Papa de García, Rosalía. "El Hábeas Data, protección al derecho a la información y a la autodeterminación informativa". *Letras*, no. 87 (2016): 23-49. https://doi.org/10.30920/letras.87.126.2.

Zamudio Salinas, María de Lourdes. "Reflexiones sobre la observancia del derecho fundamental a la protección de datos personales en diversos actos regulados por el Código Civil". *Ius Et Praxis,* no. 55 (2022):65-90. https://doi.org/10.26439/iusetpraxis2022.n055.6093.

Artículos en espacios web académicos

Agencia Española de Protección de Datos. “Publicaciones y resoluciones”. AEPD, 8 de octubre de 2024, https://www.aepd.es/publicaciones-y-resoluciones.

Gobierno de los Estados Unidos. “El sistema de posicionamiento global”, GPS.GOV, 17 de octubre de 2020, :https://www.gps.gov/systems/gps/spanish.php

Islas Montes, Roberto. "Sobre el principio de legalidad". Corte Interamericana de Derechos Humanos. 10 de octubre de 2024. https://www.corteidh.or.cr/tablas/r23516.pdf.

Organización Internacional del Trabajo. “Conferencia Internacional del trabajo”, Organización Internacional del Trabajo, 9 de octubre de 2024, https://www.ilo.org/es

Poder Judicial de Perú. "Plenos Jurisdiccionales". Poder Judicial de Perú. 13 de octubre de 2024. https://www.pj.gob.pe/wps/wcm/connect/cij/s_corte_suprema_utilitarios/as_home/as_cij/as_plenos_jurisdiccionales/

Vega Villasante, Alvaro Javier. “El teletrabajo en el Perú. Evolución normativa”, Lp Pasión por el Derecho. 28 de marzo de 2023. https://lpderecho.pe/el-teletrabajo-en-el-peru-evolucion-normativa/

Normas jurídicas

Ley 29733-2011, de 3 de julio, Ley de Protección de Datos Personales. (Lima, 22 de julio de 2011).

Directiva N° 01-2020-JUS/DGTAI-PD, de 16 de enero de 2020, Tratamiento de Datos Personales mediante Sistemas de Videovigilancia. (Lima, 17 de marzo de 2020).

Decreto Supremo N.º 003-2013-JUS, 22 de marzo de 2013, Reglamento de la Ley N.º 29733-Ley de Protección de Datos Personales (Lima, 25 de marzo de 2013).

Jurisprudencia

Corte Suprema de Justicia, Casación Laboral N°14614-2016, de 10 de marzo de 2017.

Corte Suprema de Justicia, Casación Laboral N° 3776-2015, de 10 de agosto de 2016.

Ministerio de Justicia y Derechos Humanos, Informe Jurídico N°020-2023-DGTAIPD, 2 de junio de 2023.

Resolución Directoral, EXP.N° 008-2017-JUS/DGPDP, de 25 de enero de 2017.

Tribunal Constitucional, EXP.N° 4739-2007-PHD/TC, de 15 de octubre de 2007.

Tribunal Constitucional, EXP.N° 02834-2013-PHC/TC, de 25 de enero de 2017.

Tribunal Constitucional, EXP.N° 05532-2014-PA/TC, de 22 de febrero de 2017.

Tribunal Constitucional, EXP.N° 05484-2015-PHD/TC, de 3 de octubre de 2019.

Tribunal Constitucional, EXP.N° 00943-2016-PA/TC, de 14 de julio de 2020.

Tribunal Superior de Justicia de Asturias, STSJ. ASTURIAS 3058/2017, de 27 de diciembre de 2017.

Doctrina

Directiva 2002/58/CE, de 12 de julio de 2002, Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). (Parlamento Europeo, 31 de julio de 2002).

Tribunal Europeo de Derechos Humanos. *López Ribalda y otros v. España*, demandas núm. 1874/13 y 8567/13, sentencia del 9 de enero de 2018.

Tribunal Europeo de Derechos Humanos. *Uzum vs Alemania*, sentencia de 2 de septiembre de 2010.

ANEXOS

Anexo N°1: Matriz de consistencia

	GENERAL	ESPECÍFICO 1	ESPECÍFICO 2
PROBLEMÁTICA	¿El acceso a datos personales obtenidos mediante el uso de nuevas tecnologías para el control y fiscalización laboral- como el GPS y la videovigilancia- vulnera el derecho a la protección de datos personales del trabajador?	¿Qué criterios se deben emplear para acceder a datos de geolocalización o videovigilancia como mecanismos de fiscalización laboral en el marco de una relación de trabajo?	¿En el Perú contamos con un ordenamiento jurídico que regule de forma eficaz el uso de datos personales obtenidos por mecanismos de fiscalización laboral como el GPS o la videovigilancia dentro de una relación de trabajo?
OBJETIVOS	Analizar si el acceso a datos personales obtenidos mediante el uso de nuevas tecnologías para el control y fiscalización laboral- como el GPS y la videovigilancia- vulnera el derecho a la protección de datos personales del trabajador.	Determinar los criterios que deben aplicarse para acceder a datos de geolocalización o videovigilancia como mecanismos de fiscalización laboral en el marco de una relación de trabajo.	Evaluar si en el Perú contamos con un ordenamiento jurídico que regule de forma eficaz el uso de datos personales obtenidos por mecanismos de fiscalización laboral como el GPS y la videovigilancia dentro de una relación de trabajo.
HIPÓTESIS	El acceso a datos personales obtenidos mediante el uso de nuevas tecnologías de fiscalización laboral como el GPS y la videovigilancia sí supone una vulneración a la protección de datos personales del trabajador cuando el empleador incumpla con el deber de información y consentimiento para el tratamiento de estos datos. Asimismo, la vulneración que nos ocupa podrá ser confirmada por un test de proporcionalidad en los casos en los que colisionen derechos fundamentales al momento de realizar el tratamiento de datos de los trabajadores en el marco de una relación laboral.	Los criterios que deben aplicarse para acceder a datos de geolocalización o videovigilancia como mecanismos de fiscalización laboral en el marco de una relación de trabajo, tales como la proporcionalidad y finalidad, para garantizar el respeto a la protección de datos personales del trabajador.	El ordenamiento jurídico peruano no regula de manera eficaz el uso de datos personales obtenidos por mecanismos de fiscalización laboral como el GPS y la videovigilancia dentro de una relación de trabajo.