**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**

**ESCUELA DE POSGRADO**

**Título**

# EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES DE LOS TRABAJADORES FRENTE AL CONTROL LABORAL A TRAVÉS DEL SISTEMA DE GEOLOCALIZACIÓN GPS. LÍMITES Y PROPUESTAS.

**TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN DERECHO CON MENCIÓN EN DERECHO CONSTITUCIONAL**


**AUTORA**

María de Lourdes Zamudio Salinas

**ASESORA**

Milagros Aurora Revilla Izquierdo


Marzo, 2021

A mis amadísimos padres:

Ulises y Merlini

## RESUMEN

En el Perú existe una situación de falta de regulación específica sobre la protección de los datos personales de los trabajadores en el ámbito laboral, y en particular sobre el tratamiento de sus datos geolocalizados. Tampoco existen criterios jurisprudenciales ni administrativos al respecto. Situación que sumada al uso, cada vez más frecuente, de la tecnología del GPS por parte del empleador, dificulta que este actúe dentro de los límites, que le corresponden, a su facultad de control laboral sobre la persona de sus trabajadores, favoreciendo un escenario de violación de derechos fundamentales de estos.

Frente a la situación problemática descrita; se abordará la necesidad de la interpretación y aplicación adecuada de los principios rectores de la protección de datos personales al tratamiento de los datos geolocalizados de los trabajadores con fines de control laboral; así como, propuestas de regulación a nivel de la normativa general; y de la normativa interna de la empresa, tanto obligatoria como consensual.

De las conclusiones destacamos la necesidad de que, antes que el empleador utilice la geolocalización como medida de control laboral, deberá, someterla al principio constitucional de proporcionalidad; para luego de superado el mismo, evaluar su implementación definitiva, previa adecuación a la normativa sobre protección de datos personales.

## ÍNDICE

**Pág.**

## INTRODUCCIÓN

El derecho a la protección de datos personales es un derecho fundamental de última generación que a pesar de tener en el Perú, su reconocimiento constitucional (1993); su ley de desarrollo constitucional (2011) y su reglamento (2013); así como, una autoridad administrativa de control sobre la materia desde el año 2011; está caracterizado por su desconocimiento en un sector importante de la población, e inclusive por parte de las autoridades; por lo tanto, no hay debida conciencia sobre el mismo; lo que trae como consecuencia diversas afectaciones a dicho derecho.

El tratamiento de los datos personales de los trabajadores, por parte del empleador en el contexto de la relación laboral, constituye un área específica donde el riesgo de indebidos tratamientos es grande; más aún, por el uso de las tecnologías de la información y comunicación, como el Sistema de Posicionamiento Global GPS, cada día más generalizado; cuyas capacidades y avances constantes, incrementan los riesgos para los derechos de las personas. Lo señalado, sumado a la carencia de disposiciones específicas sobre protección de datos aplicables al ámbito laboral, caracterizado por una relación asimétrica, en la que el trabajador es la parte más débil; genera una situación de mayor vulnerabilidad para el mismo.

El problema que motiva el presente trabajo de investigación, es la falta de regulación específica sobre protección de datos personales en el uso, cada vez más frecuente, de la tecnología del GPS por parte del empleador; y que dificulta, que este actúe dentro de los límites, que le corresponden, a su facultad de control laboral sobre la persona de sus trabajadores, favoreciendo un escenario de violación de derechos fundamentales de estos. Situación que se ha comprobado con el presente estudio.

Frente a la situación problemática de carencia de regulación específica; se plantea la hipótesis de la necesidad de la interpretación y aplicación adecuada de los principios

rectores de la protección de datos personales al tratamiento de los datos geolocalizados de los trabajadores, que realiza el empleador en ejercicio de su facultad de control laboral; así como, la elaboración de una propuesta de regulación que dote de mayores garantías a los trabajadores, cuando son objetos de control laboral, mediante el GPS.

Para comprobar la hipótesis señalada, se ha seguido el método de investigación de naturaleza dogmática y documental, realizando un examen técnico jurídico de la normativa sobre protección de datos personales en el Perú.

Además, como en América Latina, la legislación sobre la materia, no ha abordado el tema del presente trabajo, ni tampoco lo ha hecho la jurisprudencia ni la doctrina nacional; se ha tomado como fuente principal al ordenamiento jurídico español sobre protección de datos personales. Se ha recurrido a la jurisprudencia; así como a resoluciones de la Agencia Española de Protección de Datos. En igual forma, se ha apelado a la jurisprudencia del espacio europeo emitida por el Tribunal Europeo de Derechos humanos, en lo pertinente.

En la línea de lo señalado, es oportuno tomar en consideración que la legislación sobre protección de datos peruana tomó como fuente directa y fundamental a la normativa española sobre la materia; la misma que hoy constituye, un parámetro de mayor garantía para el derecho fundamental que nos ocupa y sigue siendo el principal referente para la región Latinoamericana.

El trabajo se divide en tres capítulos. En el primer capítulo se aborda el derecho a la protección de datos personales como un derecho fundamental y autónomo; la forma en que está regulado en nuestro ordenamiento jurídico; recurriendo para ello, a sus antecedentes, analizando como es recogido en la Constitución Política de1993, el Código Procesal Constitucional (2004) y Ley de Protección de Datos Personales (2011). Asimismo, cómo la jurisprudencia del Tribunal Constitucional fue dotándole de contenido a este nuevo derecho.

Se tratará la definición del derecho, su contenido y su naturaleza relacional; todo lo que nos permitirá comprender mejor su importancia. Terminaremos este capítulo primero, haciendo referencia a la regulación europea pertinente conformada por el

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; así como, a Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales de España; pues ambas ya hacen referencia al tratamiento de los datos personales en el entorno laboral; siendo que, la segunda, además se refiere en específico al tratamiento de los datos geolocalizados de los trabajadores.

En el segundo capítulo, se comienza con el tratamiento de la libertad de empresa como sustento fundamental del poder de dirección empresarial. En atención a ello, se aborda este derecho mencionando las libertades que comporta para reparar en la libertad de organización; que es la que a su vez, le sirve de base jurídica, al poder de dirección que le corresponde al empresario. De manera similar, se hace referencia al derecho a la propiedad como otro sustento al poder de dirección empresarial; esto, en la medida en que el empleador es el propietario de los medios o herramientas laborales que pone a disposición del trabajador. Fluirá del poder de dirección, como una de sus facultades, la de control, que permitirá verificar el cumplimiento de las obligaciones y deberes laborares que le corresponden al trabajador.
Dentro de los límites a ese poder, se analiza el derecho a la protección de datos personales como un derecho laboral inespecífico. Asimismo, se conocerá, en sus aspectos generales, al sistema de posicionamiento global GPS y sus posibles usos empresariales, enfatizando aquellos relacionados con el control y vigilancia laboral.

De otro lado, y con el fin de conocer si hay alcances jurisprudenciales o administrativos que puedan complementar la inexistente normatividad específica sobre el tema central de este trabajo, se han buscado los pronunciamientos del Tribunal Constitucional y en su caso del Poder Judicial, así como aquellos que pudieran encontrarse a nivel de opiniones y resoluciones administrativas de la Autoridad Nacional de Protección de Datos Personales. Búsqueda que refuerza la inexistencia de regulación y criterios jurídicos que coadyuven a un adecuado tratamiento de los datos geolocalizados de los trabajadores objeto de control laboral.

En el tercer capítulo, nos detenemos de manera específica y analítica en los principios rectores de la protección de datos personales: Consentimiento, Finalidad, Proporcionalidad, Calidad, Seguridad y Legalidad; para identificar sus alcances y aplicaciones en la relación laboral, y específicamente cómo se deben aplicar estos principios a la hora en que un empleador decide realizar el tratamiento de los datos personales geolocalizados de sus trabajadores en ejercicio de su facultad de control. Principios a los que debe recurrir obligatoriamente el empleador, como responsable del tratamiento, desde la recogida hasta la supresión de los datos geolocalizados.

Culminaremos este capítulo presentando tres opciones de regulación que podrían darse como complemento a la inexistencia de: normativa específica, criterios jurisprudenciales y administrativos, sobre el tratamiento de los datos personales geolocalizados de los trabajadores en el ámbito laboral con fines de control; se presentarán propuestas a nivel de la normativa general y de la regulación interna de la empresa, tanto obligatoria como consensual.

Todo esto con el fin de complementar y precisar la legislación general sobre protección de datos personales existente, para que se ofrezca una garantía más efectiva, de los derechos de los trabajadores frente al uso cada vez más dinámico, generalizado e invasivo de la tecnología del GPS como mecanismo de control laboral en el contexto de un Estado Constitucional de Derecho.

Del apartado de las conclusiones destacamos la necesidad de que, antes que el empleador utilice la geolocalización como medida de control laboral, deberá, someterla al principio constitucional de proporcionalidad; para luego de superado el mismo, evaluar su implementación definitiva, previa adecuación a la normativa sobre protección de datos personales.

Asimismo, debe quedar claramente determinada y ser previamente informada, la descripción de la finalidad de fiscalizar para sancionar, para que el empleador pueda tratar los datos geolocalizados del trabajador con ese fin. El empleador debería implementar un protocolo de cancelación de la información geolocalizada excesiva

para el control laboral; y con relación a las salvaguardas que puede implementar, estas pueden traducirse en políticas del tratamiento de los datos personales en general y en especial de los datos geolocalizados; en protocolos sobre el tratamiento de este tipo de datos; y en actividades de capacitación del personal.

Con relación a la bibliografía encontraremos en el texto las referencias que corresponden a las fuentes normativas, jurisprudenciales y administrativas; y en el apartado correspondiente: los libros, artículos de revistas y documentos internacionales.

## Capítulo 1: El derecho fundamental a la protección de datos personales en el ordenamiento constitucional peruano

### 1.1. La evolución del derecho fundamental a la protección de datos personales

#### 1.1.1. Antecedentes

Los derechos fundamentales no son categorías taxativas ni cerradas, su reconocimiento en los textos constitucionales es producto de la evolución de la humanidad, del impacto en la vida personal y social de sus propias actividades, de la exigencia de atender sus necesidades básicas y del respeto a la dignidad del ser humano.

El avance de la ciencia y la tecnología, y el uso de los productos y servicios que ellas nos brindan, generan beneficios pero, también pueden suponer riesgos para la dignidad y los derechos de la persona. La llegada de internet[1] y los avances científicos en los ámbitos de la informática y de las telecomunicaciones que desarrollaron las Tecnologías de la Información y Comunicación, en adelante las Tic, han supuesto un cambio en la vida de la humanidad en todos sus ámbitos. Han ingresado en nuestra vida cotidiana y su uso hace que dejemos huellas de nuestros comportamientos, preferencias, posiciones, creencias, y de distintas actividades que incluyen ámbitos reservados y privados que antes era imposible pensar que pudieran ser de conocimiento de terceros.

Muchas veces, sin que lo sepamos, nuestra información personal, es accesible para otros; personas naturales, corporaciones, entidades gubernamentales, etc., que

[1] "Teniendo en cuenta que mediante el Internet es posible acceder y recabar información disponible en cualquier país, así como llevar a cabo un tratamiento de la misma, como recabar datos de millones de personas sin estar físicamente domiciliado allí, circunstancia que no debería constituirse en un factor que impida la efectiva protección de los derechos y libertades de las personas en el ciberespacio;" (22) Estándares de la Red Iberoamericana de Protección de Datos. Consulta al 24 de mayo de 2020 en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

acceden a nuestra información, la recopilan, la graban, la almacenan, la modifican, la publican, la transfieren nacional o internacionalmente, etc.; con intenciones y fines que no consentimos, porque ni siquiera conocemos de ello.

Cada día hay más demandas para que se implementen el uso de diversas tecnologías para mejorar la realización de diversas actividades tanto en el sector privado como en el público; si pensamos por ejemplo en el incremento del uso de las cámaras de vídeo vigilancia, la geolocalización, los drones, lo que constituye el internet de las cosas (IoT)[2] etc., que se consideran necesarios para la mejor consecución de diversos fines; tales como la seguridad; la mejor prestación de servicios básicos, como la salud; la productividad; el ahorro de tiempo en nuestras actividades diarias, la simplificación de trámites, el acceso a información y una más rápida interconexión, entre otros fines[3].

En efecto el uso de las tecnologías como las Tic, facilitan nuestra vida, nos ayudan a conseguir objetivos personales y sociales; no obstante, frente a esto, es necesario reconocer que la vida humana, en su existencia individual y social, presenta una permeabilidad ante su avance, dejando cada día menos espacios libres a la injerencia y a los impactos de las Tic; lo que exige preguntarnos ¿los titulares de la información, quienes son objeto de tratamiento o control o monitorización por estos aparatos o dispositivos tecnológicos, son conscientes de que sus datos personales son tratados por terceros?; ¿ son conscientes de las condiciones y de todas las finalidades con que las que se usan sus datos?; ¿qué límites deben ser respetados?; la respuesta es no;

[2] "el internet de las Cosas es "la interconexión a través de Internet de dispositivos informáticos integrados en objetos cotidianos, lo que les permite enviar y recibir datos". En otras palabras IoT conecta tus dispositivos a Internet o a otros aparatos, para que puedan realizar nuevas funciones, como por ejemplo controlar elementos inteligentes de forma remota y recibir alertas y actualizaciones de estado. Se refiere a los miles de millones de dispositivos físicos en todo el mundo que ahora están conectados, recolectando y compartiendo datos. Gracias a las redes inalámbricas y el bajo costo de los nuevos procesadores, es posible que casi cualquier cosa, desde una aspiradora inteligente hasta un vehículo autónomo, forme parte de la IoT. Esto agrega un nivel de inteligencia digital a los dispositivos que les permite comunicar datos en tiempo real sin la participación de un ser humano, fusionando de alguna manera el mundo digital con el físico […]" Consulta al 30 de setiembre de 2020 en: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

[3] "Analizando más en detalle estas dinámicas, nos damos cuenta de que a menudo a los ciudadanos se les promete un futuro lleno de eficiencia administrativa y se les oculta un presente en que los instrumentos de un control cada vez más invasivo y capilar se multiplican. Casi parece que se estén construyendo dos mundos que no se comunican, y que el *e-government, la* Administración electrónica, pueda desarrollarse sin tener en cuenta el aplastamiento contemporáneo de derechos individuales y colectivos, con la excusa de exigencias de eficiencia o de seguridad." (Rodotá 2011: 19).

porque la tecnología y sus capacidades avanzan y su uso no siempre responde a lo éticamente aceptado o incluso legalmente permitido.

Las Tic y su irrefrenable evolución tecnológica, han permitido, cada día más, un intercambio masivo y fluido de la información a escala global; el uso de dispositivos electrónicos en el ámbito personal, laboral, profesional, recreacional, para la promoción y venta de bienes y servicios, administración estatal, atención de servicios vitales, etc. con capacidad de procesamiento de los datos, en tiempo real y forma imperceptible para los titulares de la información, generan riesgos y afectaciones que ponen en tela de juicio la defensa de la dignidad de la persona y de sus libertades como finalidad de nuestros Estados Constitucionales de Derecho.

Tenemos que reconocer que no ha sido posible prever el desarrollo de las nuevas tecnologías y de internet en nuestra vida personal y social ni de sus repercusiones en el ámbito de los derechos humanos. Normalmente cuando ocurren circunstancias como las brevemente descritas uno de los ámbitos desde los que se responde es la legislación, porque el Estado está en la obligación de garantizar los derechos fundamentales. Las primeras regulaciones sobre protección de datos se dan en la década de los setenta y aparecen vinculadas al derecho a la intimidad personal y familiar, fundamentalmente con el objetivo de proteger a este derecho de los posibles abusos que el tratamiento de la información por medio de la informática podría acarrear (Troncoso 2003:233; Piñar 2005:19).

En Europa[4] y como referentes significativos en el primer nivel de los ordenamientos jurídicos, podemos mencionar a las Constituciones Portuguesa de 1976 y a la Española de 1978 como las primeras en hacer una referencia específica a la protección de datos personales (Troncoso 2003:234). La Constitución Portuguesa[5] señalaba en su artículo 26.2, que:

[4] Contexto político y geográfico pionero en el reconocimiento del derecho que a la protección de datos personales y tecnológicamente más avanzado que, por ejemplo, América Latina.
[5] Reformada en 1982 y en 1991.

> […] la ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones referentes a las personas y a las familias" y en su artículo 35: "1. Todo ciudadano tendrá derecho a tener conocimiento de lo que conste en forma de registros informáticos acerca de él y de la finalidad a que se destinan esos datos, y podrá exigir su rectificación, así como su actualización, sin perjuicio de lo dispuesto en la ley sobre secretos de Estado y secreto de actuaciones judiciales. 2. Se prohíbe el acceso a ficheros y registros informáticos para el conocimiento de datos personales referentes a terceros y la respectiva interconexión, salvo casos excepcionales previstos por ley. 3. No podrá utilizarse la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliación a partidos o a sindicatos, fe religiosa o vida privada, salvo cuando se trata de tratamiento de datos estadísticos no identificables individualmente. 4. La ley definirá el concepto de datos personales para fines de registro informático, así como de bases y bancos de datos y las respectivas condiciones de acceso, constitución y utilización por entes públicos y privados. 5. Se prohíbe la asignación a un número nacional único a los ciudadanos. 6. La Ley determinará el régimen aplicable a los flujos de datos allende las fronteras, estableciendo formas adecuadas de protección de los datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional.

Como puede apreciarse, el texto de la Constitución Portuguesa, contiene varios aspectos del nuevo derecho. Proteccionista, pues reserva a la ley el establecer garantías efectivas contra las informaciones referentes a la persona que afecten su dignidad; de empoderamiento, reconociendo al titular de la información las facultades de acceso, rectificación y actualización de sus datos; prohibitiva y protectora frente al uso de la informática para el tratamiento de datos sensibles así como el enmarcar los flujos transfronterizos de datos dentro de un debido tratamiento de la información personal.

Por su parte la Constitución Española de 1978[6], en su artículo 18, reconoce y dispone

[6] Artículo 18 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Consulta al 30 de junio de 2020 en: https://www.lamoncloa.gob.es/documents/constitucion_es1.pdf

junto al derecho al honor, a la intimidad personal y familiar, a la imagen, a la inviolabilidad de domicilio, al secreto de las comunicaciones, el que la "ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (Art. 18.4); como se aprecia no le dedica una disposición independiente para la única vez en que dicha Constitución se refiere al uso de la informática y además lo hace en un sentido restrictivo, pues establece que la ley va a limitar su uso en defensa del honor, la intimidad personal y familiar y el pleno ejercicio de los derechos.

Del texto del artículo 18.4 no se anuncia un nuevo y autónomo derecho, independiente del derecho a la intimidad; sino que se requerirá del desarrollo jurisprudencial para que, vía interpretación constitucional, identifique y diseñe su contenido esencial. El Tribunal Constitucional Español, en el año 1993 lo interpreta así:

> Dispone el art. 18.4 C.E. que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".[7]

La labor jurisprudencial en España tendrá un largo recorrido que encontrará su expresión clara y definitiva, en la Sentencia del Tribunal Constitucional Español, 292/2000, de 30 de noviembre, en la que se desarrollan aspectos esenciales para la

[7] STC 254/1993, de 20 de julio de 1993. FJ 6 (reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). Consulta al 20 de junio de 2020 en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383

configuración de este nuevo derecho. Así, dicha sentencia señala que:

> […] el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.[8]

En Alemania, se configuró el derecho a la protección de datos personales a partir de la interpretación de otros preceptos de su norma de mayor nivel jerárquico dentro de su ordenamiento jurídico. El Tribunal Constitucional Federal de Alemania, se basó para esta tarea de configuración de un nuevo derecho, en la interpretación que realizó sobre el derecho a la personalidad y sobre la dignidad de la persona. Tal como lo señala Troncoso afirmando que:

> […] en la clave de la bóveda del ordenamiento de la Ley Fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre, y a cuya protección se encamina este derecho de la personalidad. La jurisprudencia alemana afirma las limitaciones del derecho a la intimidad para tutelar a la persona frente a las tecnologías de la información y ha optado por volver al propio principio del libre desarrollo de la personalidad, donde hacen tanto el derecho a la intimidad como el derecho a la autodeterminación informativa. De esta forma, el Tribunal Constitucional Federal alemán ha establecido las bases del derecho a la

[8] STC 292/2000, de 30 de noviembre de 2000. Fj. 7. Consulta al 20 de junio de 2020 en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

> autodeterminación informativa- iformationelle Selbstbestimmungsrecht-, que fue proclamado en la Sentencia, de 15 de diciembre de 1983[9], que declara inconstitucionales algunos preceptos de la Ley del Censo, de 4 de marzo de 1982. Este derecho trata de proteger el ámbito de la personalidad que asegure al individuo su plena libertad y capacidad de decisión frente al abuso de quien maneja bases de datos personales. (2003: 237-238).

Como puede apreciarse, el Tribunal Constitucional Federal Alemán se refiere, al derecho que nos ocupa, como "derecho a la autodeterminación informativa".[10]

En cuanto a los principales instrumentos internacionales en materia de protección de datos y en orden cronológico, previos al reconocimiento de este derecho en Perú, podemos mencionar a la OCDE, Organización para la Cooperación y el Desarrollo Económicos, a través de sus Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales, adoptada el 23 de septiembre de 1980[11]. Las que constituyen el primer documento internacional que analiza el derecho a la protección de datos personales.

Estas directrices tuvieron como finalidad fundamental establecer "guías generales para la recogida y gestión de la información personal" que garanticen la no existencia de obstáculos para los flujos transfronterizos de datos; los principios que establecen las Directrices abarcan todos los medios y tipos de procesamiento de datos personales, así como las diversas categorías de datos; con el fin de que se puedan aplicar en el ámbito nacional e internacional.[12]

El Convenio N° 108 del Consejo de Europa, de 28 de enero de 1981, "Convenio para

[9] Tribunal Constitucional de la República Federal de Alemania, sentencia de la Sala de 15 de diciembre de 1983, sobre la Ley de censo de población, profesión y lugares de trabajo / Ley de Censo).
[10] Sobre el nombre del derecho que estamos tratando, podemos encontrar diferentes expresiones: "derecho a la protección de datos personales", "libertad informática" y "derecho a la autodeterminación informativa" como es la que utiliza el Tribunal Constitucional Alemán citado. Nosotros usaremos el más generalizado tanto por la doctrina como por las legislaciones, el de protección de datos personales, que además es el que ha sido por el que ha optado el legislador peruano, en la Ley de protección de datos personales, Ley N° 29733.
[11] Consulta al 12 de junio de 2020 en: https://www.oecd.org/sti/ieconomy/15590267.pdf
[12] Ibidem.

la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos.

El fin del convenio está definido en su artículo 1, como sigue "[ …] garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)"; en sus considerandos se señala el deseo de ampliar la protección de los derechos y de las libertades fundamentales, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.

Detalla los principios y las obligaciones para el tratamiento de los datos personales en protección de la intimidad y privacidad de las personas. Recoge los principios contenidos en las Directrices de la OCDE y hace un desarrollo más sistemático de ellos (Puente 2005:55-59).

Las Directrices de la Resolución 45/95 de la Asamblea General de las Naciones Unidas, del 14 de diciembre de 1990, relativa a los principios rectores sobre la reglamentación de los ficheros computarizados de datos personales. Constituyen el primer documento de ámbito universal sobre la materia de protección de datos. Establece los principios básicos para los tratamientos automatizados de datos personales, pero posibilita a los Estados miembros para aplicarlos a los tratamientos de datos de tipo manual.[13]

Luego de esta breve referencia al contexto internacional de la legislación fundamental sobre la materia de protección de datos personales, que precede a la introducción de

[13] Con posterioridad la Asamblea General de la ONU ha hecho referencia en diversas resoluciones a la protección de la privacidad en el entorno digital. (Resolución 68/167, adoptada el 18 de diciembre del 2013; Resolución 73/179, adoptada el 17 de diciembre del 2018)

este derecho en Perú, vamos a ver cómo se recoge este nuevo derecho en nuestro país.

### 1.1.2. Constitución de 1979

La constitución política de 1979 no reconoce el derecho a la protección de datos personales; si lo hace con relación al derecho a la intimidad, en su aspecto personal y familiar[14]. Si bien es cierto que los derechos a la intimidad y a la protección de datos personales son independientes uno de otro, es frecuente el reconocimiento del segundo vinculado al primero, tal como lo hacen, entre otras, las Constituciones del Reino de España[15]; la Constitución Política de los Estados Unidos Mexicanos; [16] la Constitución Política de Colombia[17] ; la Constitución Política de la República de Chile[18]; así como la Constitución Política del Perú[19].

En el segundo nivel del ordenamiento jurídico, podemos encontrar leyes sobre la materia de protección de datos que tienen esta característica de relacionar los dos

---

[14] "Artículo 2. Toda persona tiene derecho:5. Al honor y la buena reputación, a la intimidad personal y familiar y a la propia imagen. Toda persona afectada por afirmaciones inexactas o agraviada en su honor por publicaciones en cualquier medio de comunicación social, tiene derecho de rectificación en forma gratuita, sin perjuicio de la responsabilidad de ley."

[15] De 1978. Artículo 18. - "4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[16] Artículo 6. - "[...]La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. [...]"

[17] "Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución."

[18] "Artículo 19.4"La Constitución asegura a todas las personas: (…) 4°. El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley"."

[19] "Artículo 2. Toda persona tiene derecho: 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar." (1993).

derechos fundamentales mencionados, tales como las leyes de la República Dominicana[20]; de Nicaragua[21], de México[22]; de Andorra[23]; de Costa Rica[24] y de Argentina[25], entre otras; la explicación es lo comentado en los acápites anteriores referido a que el derecho a la protección de datos personales nace íntimamente vinculado a la intimidad y como un derecho que tiene como una de sus finalidades fundamentales proteger la intimidad de la persona, especialmente frente al uso de la informática.

### 1.1.3. Constitución de 1993

La Constitución Política de 1993, es la que incorpora en su texto, como novedad, el

[20] Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. No. 10737 del 15 de diciembre de 2013. "Artículo 1. Objeto. La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean éstos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el Artículo 44 de la Constitución de la República Dominicana.(…)"

[21] LEY N°. 787, Aprobada el 21 de Marzo de 2012 "Artículo 1 Objeto La presente ley tiene por objeto la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa."

[22] LEY N°. 787, Aprobada el 21 de Marzo de 2012, Ley Federal de Protección de datos personales en posesión de los particulares. "Artículo 1. La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas."

[23] Ley cualificada 15/2003, del 18 de diciembre, de protección de datos personales "Artículo 1 Objetivo Esta Ley tiene por objetivo proteger y garantizar, en lo que se refiere al tratamiento y al uso de datos personales, los derechos fundamentales de las personas, y especialmente los relativos a la intimidad."

[24] Protección de la persona frente al tratamiento de sus datos personales Ley N° 8968 "ARTÍCULO 1. Objetivo y fin . Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."

[25] PROTECCION DE LOS DATOS PERSONALES. Ley 25.326

reconocimiento del derecho a la protección de datos personales, como uno de los aportes, que busca reforzar la defensa de la dignidad de la persona misma en nuestro Estado Constitucional de Derecho. Es importante, como punto de partida de nuestro análisis, conocer lo que entendieron por este derecho y lo que pretendieron con su incorporación los constituyentes del año 1993.

### a) Debate a nivel de la Comisión de Constitución y Reglamento[26] del Congreso Constituyente Democrático

El diario de debates de la Comisión de Constitución y Reglamento del Congreso Constituyente Democrático, en adelante el CCD, título I, denominado "De la Persona y la Sociedad" , capítulo 1 denominado "De los derechos Fundamentales de la Persona"[27] da cuenta sobre la inclusión en el inciso 6) del artículo 2° de lo que llegó a denominarse formalmente muchos años después[28], como el derecho a la protección de datos personales, y también del nivel del conocimiento de este derecho y de su contenido, en ese momento en nuestro país; limitado en cuanto a su contenido y naturaleza, pero suficiente para lograr su incorporación como reconocimiento de un nuevo derecho, de última generación, en la carta fundamental de 1993, y posibilitar a partir de allí su desarrollo jurisprudencial y legal posterior, como veremos en los siguientes apartados.

La propuesta[29] inicial era la siguiente: "A exigir que los servicios informáticos públicos o privados supriman informaciones personales, salvo los casos de seguridad nacional establecidos por ley"[30]. Los cuestionamientos fundamentales a esta redacción

[26] Tomo I. Debate Constitucional 1993.Comisión de Constitución y de Reglamento. Congreso Constituyente Democrático. Publicación oficial. Este texto no ha sido publicado en el Diario Oficial "El Peruano", a solicitud del Ministerio de Justicia, ha sido enviado por el Congreso de la República, mediante Oficio N° 294-2007-2008-DGP/CR, de fecha 27 de diciembre de 2007). Consulta al 10 de junio de 2020 en: http://spij.minjus.gob.pe/Textos-PDF/Constitucion_1993/ComConstReglam93/Tomo_I.pdf

[27] El debate se realizó sobre el proyecto contenido en el proyecto presentado por Nueva Mayoría-Cambio 90.

[28] En el año 2011, con la Ley N° 29773 que es la que lo desarrolla, Ley de Protección de Datos Personales.

[29] Fue presentada por la Bancada mayoritaria conformada por Nueva mayoría Cambio 90.

[30] Diario de Debates pág. 161.

radicaron en las siguientes frases: “informaciones personales”, “servicios informáticos” y “supriman informaciones”.

-El cuestionamiento a “informaciones personales” radicaba en que debía quedar claro la separación entre la información personal en general y la información personal de carácter privado, puesto que no toda información personal es íntima o privada.
Lo que se decidió fue que debía referirse a las informaciones personales de carácter íntimo y no a las informaciones personales en forma genérica.[31] Por ese motivo la propuesta varió, con relación a este tema, a la siguiente redacción: “A exigir que los servicios informáticos públicos o privados supriman informaciones que afectan la intimidad personal, salvo los casos de seguridad nacional establecidos por ley”. Introduciéndose a la intimidad personal como derecho estrechamente vinculado a la protección de datos y objeto de protección de éste último en cuanto a la información que perteneciera al ámbito de la misma. Poniéndose en evidencia además la visión restrictiva en aquél momento sobre los alcances del derecho; pues si bien es cierto la relación particular existente del derecho a la protección de datos personales con el derecho a la intimidad[32], se desconocía la naturaleza relacional del primero, el mismo que trasciende al ámbito de la intimidad.

- Con relación a “suprimir informaciones”. Una posición sustentaba que una persona podía poseer información de otra persona, inclusive sin que el titular de la misma lo supiera y nadie tenía por qué impedir ese tratamiento, más aún si había sido conseguida por la primera. Que en todo caso, lo que se podría prohibir es que esa información – perteneciente a otra persona- sea proporcionada a un tercero, pero no que sea borrada de sus archivos. Discutiéndose el término suprimir de la redacción original.[33]
Esta posición, cuya relevancia de citarla radica en que representaba y, aún representa, el pensamiento de un sector de la población[34]; posición que considera que tratar datos de otras personas puede ser similar a hacer un inventario, o tratar

[31] Diario de Debates pág. 162.
[32] Podríamos decir una relación de origen
[33] Diario de Debates pág. 162.
[34] Dentro del cual encontramos a personas, autoridades, propietarios de empresas, etc.

bienes o activos inertes, que se pueden poseer y de los que se puede obtener provecho; sin atender ni entender la gran diferencia que radica en la naturaleza de la información de una persona, pues dependiendo de lo que se haga con ella, puede afectarse la dignidad y la vida de la persona misma, cuyos datos se están tratando sin su conocimiento y menos con su consentimiento. Esta posición va a ser el sustento de una modificación de la propuesta.

Frente a esta posición surgió la que en discrepancia buscaba un equilibrio, señalando que "uno no tiene derecho a tener la información de nadie, salvo que sea un abogado o un médico, y que esté específicamente relacionado a un caso […] ninguno debiera de poder indagar todo tipo de detalles, aun cuando no los vaya a usar"[35].
La sustitución de la frase "suprimir informaciones" cedió ante la frase "no suministrar" por el argumento fáctico de que no se puede exigir o prohibir algo que no es posible controlar, "Cuando yo exijo es porque conozco, puedo conocer previamente que se va a dar esa información"[36] Discusión que hoy a la luz de la ley de protección de datos personales no tendría sentido porque el hecho de recopilar, o almacenar, por supuesto transmitir o difundir información sobre otra persona, todas constituyen actividades de tratamiento de datos personales, por lo que deben sujetarse a lo establecido en la Ley y en el Reglamento.[37]

-La frase " servicios informáticos", de acuerdo a los proponentes, aludía necesariamente y solo a los servicios "computarizados"[38], por los mayores riesgos a los que el tratamiento de la información personal está expuesta por dichos medios que manejan globalmente la información con múltiples capacidades como su reproducción nacional e internacional; pudiendo suponer un uso masivo de la información sobre las personas.[39] Poniendo en evidencia la diferencia entre el manejo privado sobre la información personal de manera mecánica, del uso masivo de la

[35] Diario de Debates. Pág. 163. Congresista Ferrero Costa.
[36] Diario de Debates. Pág. 164.
[37] Ley N° 29733, Art. 2, inciso 19. Tratamiento de datos personales.
[38] Diario de Debates. Págs. 162 y 164. Congresista Torres y Torres Lara.
[39] Diario de Debates. Pág. 162. Congresista Torres y Torres Lara.

misma a través de los sistemas computarizados.[40]

Razón por la cual se agregó el término computarizados a la frase "servicios informáticos". No obstante y tal como lo manifestó una voz en el debate, dentro de esta lógica, sería lícito que se proporcione información de carácter íntimo que no está computarizada.[41] La respuesta fue que si una persona tiene un dato de otra persona "es imposible que la ley pueda detener la trasmisión oral…o escrita: pero la transmisión computarizada puede afectar gravísimamente el control de la sociedad"[42] aludiéndose a que el derecho en debate no es un invento sino que proviene de constituciones modernas que lo han recogido en los últimos diez años.

A la luz de lo que hoy sabemos la transmisión oral o escrita de un dato personal implica un tratamiento que puede afectar, en mayor o menor medida, al titular de la misma dependiendo de las circunstancias en que se dé.

El texto aprobado en la Comisión de Constitución y Reglamento fue el siguiente: "6) A que los servicios informáticos computarizados públicos o privados no suministren informaciones que afectan la intimidad personal, salvo los casos establecidos por ley"[43].

Como vamos a apreciar, el Pleno va a introducir dos modificaciones a este texto; una referida a los servicios informáticos computarizados, comprendiendo también a los servicios informáticos no computarizados y otra referida a la ampliación del derecho a la intimidad personal, incluyendo a la intimidad familiar.

[40] Hay que tener en cuenta el estado de la tecnología en el año de 1993 donde había computadoras e internet y herramientas tecnológicas que ya entrañaban riesgos para los derechos de las personas; riesgos que al día de hoy se han incrementado en atención al aumento de su capacidad de tratamiento y procesamiento de la información personal, de manera exponencial.

[41] Diario de Debates. Pág. 165. Congresista Olivera Vega.

[42] Diario de Debates. Pág. 165. Congresista Torres y Torres Lara.

[43] Diario de Debates. Pág. 166.

### b) Debate Constitucional a nivel del Pleno - 1993[44]

El debate en el Pleno del CCD tuvo como sustento fundamental que se trataba de una innovación que ya estaba recogida en algunas constituciones modernas, tales como las de Brasil, España y Portugal. La revolución informática que se experimentaba en los últimos años a nivel mundial, había supuesto un cambio en cuanto al poder que da la información para quien la maneja y según el fin con que lo haga, lo cual puede ser incontrolable cuando se hace a través de los sistemas más modernos de computarización, todo lo que puede suponer un riesgo importante para la intimidad personal, que como seguimos apreciando, este último derecho es el que, sustenta fundamentalmente, el reconocimiento del nuevo derecho que nos ocupa.[45]

Dentro del sustento de los proponentes se hizo alusión a que la Constitución de Brasil estableció la facultad de cualquier ciudadano para que se modifiquen las informaciones que sobre él existiesen en las computadoras, pudiendo el titular afectado acudir a un juez para solicitar la rectificación correspondiente.
Esto nos permite apreciar que aunque en la redacción del artículo de la Constitución peruana solo se va a aludir a la facultad del titular del dato a que no se suministren informaciones que afecten su intimidad, nos podemos dar cuenta que en la voluntad de los constituyentes se encontraban otras acciones que este derecho debía facultar a los titulares de la información, como es el derecho a rectificar una información que pudiera ser inexacta.[46]

Otro aspecto que muestra el entendimiento limitado del contenido del derecho a la protección de datos personales por nuestros constituyentes,[47] se puso de manifiesto cuando se señaló que la Comisión de Constitución y Reglamento llegó a la conclusión

[44] Tomo I. Diario de los Debates del Pleno. Publicación oficial. Este texto no ha sido publicado en el Diario Oficial "El Peruano", a solicitud del Ministerio de Justicia, ha sido enviado por el Congreso de la República, mediante Oficio N° 294-2007-2008-DGP/CR, de fecha 27 de diciembre de 2007). Publicación ubicada al mes de mayo de 2020 en: Consulta al 10 de mayo de 2020 en: http://spij.minjus.gob.pe/Textos-PDF/Constitucion_1993/DebConst-Pleno93/DebConst-Pleno93TOMO1.pdf

[45] Diario de los Debates del Pleno. Pág. 111.

[46] Diario de los Debates del Pleno. Págs. 111-112.

[47] Con esta afirmación no se quiere emitir un calificativo negativo, pues hay que evaluar las posiciones en su momento, y en América Latina el conocimiento y entendimiento de este derecho era muy limitado, comparado con lo que sucedía a nivel de Europa.

de que la obtención de la información personal y su conservación no serían el problema, sino su comunicación a un tercero. Esto, puesto que sería más dañino comunicar una información negativa de una persona que solamente acumulando la misma.

Por lo señalado, la Comisión sustentadora del proyecto entendía que la protección que debía dar la Constitución sería el permitir a cualquier persona proteger su propia intimidad impidiendo que se transmita esa información, independientemente de la certeza o no de la información, pues lo que se debía tener en consideración es el daño a la intimidad de la persona, de su familia o de su entorno. Si bien es cierto que la transmisión de la información personal, y a través de los medios computarizados y el internet puede suponer un mayor daño que hacerlo al modo "tradicional" hasta ese entonces[48], el hecho solo de transmitir, de cualquier forma, una información sin el consentimiento del titular de la misma atenta contra la autodeterminación informativa de la persona; pero no solo el trasmitirla, sino el recopilar o recoger y conservar una información de otra persona sin su consentimiento o sin estar legitimado para ello, independiente del contenido positivo o negativo de dicha información.

Lo acabado de señalar va a ser parte del contenido del derecho fundamental a la protección de datos personales que a partir de la Constitución de 1993, la jurisprudencia y la ley de la materia reconocerán, pero que en este momento gestacional no se tuvo la información suficiente, por el nivel del conocimiento de la materia en dicho contexto temporal.

Nos parece pertinente comentar lo que, a nivel del debate en el Pleno, parece expresado con poca claridad conceptual o, por lo menos, con poca claridad de lenguaje al señalar que "la información patrimonial no tiene reserva y puede informarse ampliamente".
En efecto, se señala que "pueden instalarse empresas que vayan acumulando información sobre los ciudadanos y que van a vender y transmitir esa información, lo cual es totalmente legítimo; por ejemplo la información patrimonial" se señala

[48] Mecánicamente, de mano en mano, a través de conversaciones, pegando en una pizarra, etc.

“cualquier información” y se da como ejemplo, la patrimonial.

El concepto de información patrimonial sin duda puede ser muy amplio, sin embargo casi inmediatamente se agrega “de repente estamos prohibiendo que se dé información patrimonial: quién paga sus deudas o no, qué patrimonio tiene o no”[49] ; a continuación, se sostiene “La información sobre el patrimonio de cada uno, sobre el manejo económico de cada uno, sobre lo que tiene o lo que no tiene, es amplia no tiene ninguna reserva y puede informarse ampliamente”. Se dijo “no tiene ninguna reserva”.

Al respecto y en relación a lo señalado, la información patrimonial de una persona es un dato personal sujeto a protección; hay información patrimonial que aparece en Registros Públicos o información de rentas o ingresos que por ley debe ser declarada y aparecer en registros públicos, o información de riesgos que son objeto del negocio de las Centrales Privadas de Información y de Riesgos; pero en todos esos casos nos encontraríamos ante datos personales que en virtud de una ley son tratados sin consentimiento de sus titulares, es decir son situaciones excepcionales habilitadas legalmente.
No obstante, por ejemplo el ingreso, el sueldo, los honorarios de las personas naturales del sector privado, como regla, son datos personales que forman parte del derecho que nos ocupa.

Como dato, y sin pretender que los miembros el CCD debían leer el futuro en el siglo XXI, cuando se aprueba en el 2011, la Ley N° 29733, Ley de Protección de Datos Personales, en la que no solo se va a considerar a los ingresos económicos como cualquier dato personal, sino como dato personal sensible, por lo que es un dato personal objeto de mayor protección[50]. Debemos reconocer que esta parte del debate no ha significado en el futuro desarrollo del derecho una restricción a su contenido a nivel de la legislación ni jurisprudencialmente en nuestro país.

[49] Diario de los Debates del Pleno. Pág. 112.
[50] Considerar a los ingresos económicos como dato personal es lo común; el que se le dé la categoría especial de dato sensible es lo poco común a nivel de la legislación comparada. No hay nada sobre esta posición en la exposición de motivos de la Ley N°29733

Sobre la inclusión de los "servicios computarizados" hasta este momento quedaba claro que la protección de este derecho estaba dirigida a la información tratada a través de los servicios computarizados. No obstante, y creemos con acierto, [51] se pone de manifiesto la inconveniencia de circunscribir la protección de este derecho a un indebido tratamiento a través solo de los servicios computarizados, porque sería una limitación a la protección que se pretendía, pues la afectación al derecho también podría provenir de servicios informáticos que no fueran computarizados tales como las tarjetas IBM[52] las cadenas radiales internacionales[53], etc.

La redacción podría haber quedado solo referida a los servicios informáticos, sin especificar computarizados, pues así se comprendería a éstos y a los que no lo fueran; no obstante se prefirió especificar, "sacrificando un poco el lenguaje"[54] "servicios informáticos computarizados o no" para evitar la interpretación errónea de equiparar servicios "informáticos" con " informativos" de tal manera que quedara claro que no se estaban refiriendo a los medios de información o de prensa, que pudiera considerarse una forma de controlar a esta.

Coincidimos y concordamos que fue preferible especificar "computarizados o no" porque la protección, fuera de toda duda abarcará al uso o manejo de los datos "personales" independientemente del medio y tecnología en que éstos sean tratados. La tecnología computarizada avanza pero no ha eliminado ni sustituido por completo los espacios ni las diversas formas tradicionales de tratar indebidamente la información personal.[55]

---

[51] Diario de los Debates del Pleno. Pág. 112. El congresista Cáceres Velásquez.
[52] El Congresista Cáceres Velásquez las pone como ejemplo.
[53] El Congresista Sotomarino Chávez las pone como ejemplo. Pág. 113.
[54] El Congresista Torres y Torres Lara. .Pág. 113
[55] Nos parece pertinente traer la cita de García González, Aristeo, sobre el peligro que amenaza la vida privada protegida por el artículo 1.1 de la Ley de Bonn: consistente en que:
"a) Los datos personales, es decir, incluso los correspondientes a la esfera privada del individuo (por ejemplo: informaciones sobre el estado de salud, defectos físicos, etcétera) pueden quedar registrados y ser transmitidos de forma discrecional sin conocimiento del afectado o sin darle posibilidad de intervenir, e incluso con celeridad, hasta los últimos confines de la tierra en beneficio de terceros.
b) Que los datos archivados, incluso siendo correctos sean transmitidos fuera de contexto, esto es, sin conexión con otras informaciones que serían necesarias para su correcta interpretación (tendencia inherente por razones técnicas a la distorsión en el procesamiento de datos)." La protección da datos

### c) Derecho reconocido en la Constitución de 1993

Conforme a lo señalado en los apartados anteriores, el texto que se aprobó en el Pleno y que quedó en la redacción final de la Constitución Política de 1993 del Perú, en el Artículo 2°, inciso 6) fue el siguiente: Toda persona tiene derecho: "A que los servicios informáticos computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar".

En la medida que el derecho a la intimidad personal y familiar quedaron reconocidos en el inciso 7°[56] constitucional, se puede entender que dentro de las necesidades de establecer el inciso 6°, está que dichos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el derecho a la protección de datos personales, por medio del actual art. 2, inciso 6., no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el artículo 2, inciso 7).[57]

La incorporación del derecho a la protección de datos personales en la Constitución de 1993, colocaba al Perú como uno de los pocos países en América Latina, que en ese momento, le habían dado un reconocimiento formal a este derecho en sus cartas fundamentales.[58] La redacción del inciso 6°, contiene por una lado un mandato

---

personales: derecho fundamental del siglo XXI. Un estudio comparado. Boletín mexicano de derecho comparado. Año XI. N° 120.Setiembre-diciembre 2007. Consultado al 22 de junio de 2020 en: https://dialnet.unirioja.es/servlet/articulo?codigo=2382666

[56] "7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias […]"

[57] STC 292/2000, de 30 de noviembre de 2000. Fj. 4. http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

[58] En América Latina la constitución Brasilera fue la primera norma fundamental en regular sobre la materia de protección de datos. Constitución de la República Federativa de Brasil de 1988. Artículo 5° "LXXII Se concederá "habeas data": para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o

prohibitivo para suministrar informaciones -provengan del uso de la informática o no- que puedan afectar el derecho a la intimidad; no se refiere a otras actividades o tratamientos que se pueden dar a la información de una persona diferentes al suministro, tales como, la recogida, la grabación, la organización, el bloqueo, la modificación, la supresión, etc.; de otro lado, vincula al nuevo derecho de manera explícita solo con el derecho a la intimidad, y no con otros derechos, como si lo hace la constitución Española de 1978, en su artículo 18.4, y que ya ha sido objeto de comentario en acápites anteriores.

Sí hace referencia explícita a que la protección abarca tanto al uso de la información provengan del sector público como del privado. No se denomina al derecho y tampoco se delimita de manera clara el bien jurídico objeto de protección de esta nueva libertad reconocida. Situación que hizo necesario un desarrollo jurisprudencial y legal posterior; pues la redacción del numeral 6) del Artículo 2, no parecía ser suficiente desde el punto de vista técnico jurídico para su cabal aplicación por todos los obligados a respetar y garantizar este "nuevo" derecho fundamental, comenzando por el mismo Estado y por supuesto, abarcando a toda la colectividad.

La Constitución Política de 1993 vuelve a referirse de manera implícita, al derecho a la protección de datos personales, en el Título V de las Garantías Constitucionales, al incorporar, en nuestro sistema jurídico, la novísima[59] garantía, para la década de los noventa, denominada el Hábeas data, en el artículo 200º inciso 3).
La Garantía Constitucional del Hábeas Data protege dos derechos, el derecho de

---

de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;".
Constitución de Colombia de 1991, Artículo15: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución".
Constitución de Paraguay de 1992: "Artículo 135 - DEL HABEAS DATA. Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos."

[59] Incorporada en América en el año 1988 con la Constitución Brasileña.

acceso a la información pública, inciso 5); y el derecho a la protección de datos personales, inciso 6); ambos reconocidos en el artículo 2º de la Carta fundamental.

La incorporación de una garantía procesal específica y autónoma, como la mencionada, tiene como fin fundamental, garantizar de manera más efectiva a los derechos fundamentales; y en el caso del derecho que nos ocupa buscará cumplir dicho fin a través de la defensa de la información personal frente a los tratamientos indebidos o abusos que puedan significar una vulneración o amenaza, que puedan provenir de cualquier persona, funcionario o autoridad.

Perú va a tener que esperar once años para que se regule dicha garantía en una norma adjetiva específica, como el Código Procesal Constitucional que verá la luz en el año 2004.[60]

### 1.1.4. Código Procesal Constitucional

La Ley Nº 28237 aprobó el primer Código Procesal Constitucional del Perú, en adelante el CPC, norma que comenzó a regir el 01 de diciembre de 2004. El CPC, desarrolló más aspectos del contenido del derecho a la protección de datos personales con relación a lo que reconoció el texto de la Constitución Política de 1993, sin duda recogiendo algunos de los fallos de la jurisprudencia constitucional sobre dicho derecho, en el periodo de los 11 años que mediaron entre la Constitución Política y la dación del CPC.

En su artículo 61, inciso 2), el CPC, establece que toda persona puede recurrir al proceso de Hábeas Data para "2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o

[60] Mediante la Ley N° 26301, se aprobaron disposiciones referidas a la aplicación de la Acción de Hábeas Data, para aspectos de su tramitación; norma aprobada en el mes de abril de 1994. Como reza la primera parte de su artículo "1°. En tanto se dicte la ley específica de la materia […]".

acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales".

Del texto del CPC se desprende que los derechos del titular de la información que pueden ser directamente demandados a través del proceso de Hábeas Data comprenden los derechos de acceso o conocimiento de la información, el cual resulta básico para poder ejercer el control sobre el tratamiento que se le esté dando a los datos personales; el derecho a actualizar o incluir los datos personales, que permite cuidar la calidad de la información que se trata; la facultad de rectificar los datos, que permite subsanar errores en la información personal; así como suprimir o cancelar datos personales en general, poniendo especial énfasis si se trata de datos sensibles o privados sobre los que también se puede oponer a que sean suministrados o transferidos.

Esta serie de facultades reconocidas expresamente en la norma adjetiva, materializan más concretamente el poder o la facultad que el derecho a la protección de datos personales le da al titular de la información, dotándole de mayores garantías; lo cual es necesario tratándose de los derechos fundamentales, que deben poseer recursos efectivos frente su amenaza o violación.

### 1.1.5. Jurisprudencia constitucional

El máximo intérprete de la Constitución en el Perú, a partir del reconocimiento constitucional del derecho a la protección de datos personales (1993), comenzó a definir sus contornos desde el proceso de Hábeas Data, hasta la dación del Código Procesal Constitucional (2004); y posteriormente a esta norma adjetiva, la Jurisprudencia del Tribunal Constitucional continuó delimitando su contenido, hasta la aprobación de la Ley que desarrolla este derecho, Ley N° 29733 (2011), luego de la cual la labor del Tribunal Constitucional ha seguido, precisando, por ejemplo sobre los principios a los que debe someterse todo tratamiento de datos personales, sea dentro del ámbito de la administración pública como de la privada.

Veamos algunos pronunciamientos ilustrativos sobre aspectos importantes de la

configuración del derecho a la protección de datos personales desde el proceso constitucional de Hábeas Data.

### a) Denominación del derecho

El Tribunal Constitucional denomina al derecho reconocido en el artículo 2°, inciso 6 de nuestra carta fundamental, como el derecho a la autodeterminación informativa en la gran mayoría de sus sentencias, como desde la recaída en el expediente N°. 666-1996-HD/TC[61], entre otras muchas, así como la recaída en el expediente Nº 1797-2002-HD/TC, de fecha 29 de enero de 2003, en el marco de un proceso de Hábeas Data.[62]

Nuestro alto tribunal señaló que tomó de la doctrina esa denominación del derecho. No obstante no siempre nuestro máximo intérprete de la Constitución se ha referido al derecho con la denominación autodeterminación informativa, también, si bien es cierto en muy contadas ocasiones, lo ha denominado como derecho a la protección de datos personales, aunque esto ha acontecido, luego de la dación de la ley sobre la materia, la Ley N° 29733, del año 2011. Citamos come ejemplo la sentencia recaída en el expediente N° 01396-2014-PHD/TC.[63]

Para precisar el aspecto de la denominación del derecho que nos ocupa, consideramos necesario referirnos a su tratamiento legal. Por su parte, la Ley Nº 29733[64], Ley de protección de datos personales, utiliza la denominación de "derecho

[61] En el portal web del Tribunal Constitucional solo aparecen las sentencias emitidas desde 1996, es decir, ya con el Tribunal Constitucional y no se encuentra jurisprudencia del Tribunal de Garantías Constitucionales.

[62] "El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina *derecho a la autodeterminación informativa* y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les (sic) conciernen". Fj. 3.

[63] Fundamento jurídico 3.

[64] Publicada el 03 de julio de 2011.

fundamental a la protección de datos personales".[65] Colocando legalmente el epígrafe al derecho reconocido en el artículo 2, inciso 6), como el derecho fundamental a la protección de datos personales.

La Ley Peruana, sigue la tendencia legislativa mayoritaria en Iberoamérica de la denominación del derecho que nos ocupa, como derecho a la protección de datos personales. En atención a lo señalado, será propio en nuestro contexto jurídico, referirnos indistintamente al mismo derecho como derecho a la protección de datos personales (calificación legal) o como derecho a la autodeterminación informativa (calificación del Tribunal Constitucional) (Zamudio 2014: 1159-1162).

**b) Titularidad del derecho**

Es indiscutible que la titularidad de los derechos fundamentales, le corresponde a la persona humana ("titular primario"). El Tribunal Constitucional en diversos pronunciamientos ha abordado esta cuestión. Cuando la Constitución proclama o reconoce los derechos fundamentales, lo hace preferentemente o, antes que nada, pensando en la persona humana, esto es, en el ser humano física y moralmente individualizado. Hacia él se encuentran canalizados los diversos atributos, facultades y libertades y, por tanto, es él quien primordialmente puede invocar su respeto y protección a título subjetivo.[66]

En determinadas circunstancias y supuestos, la titularidad de los derechos fundamentales que le corresponde a la persona natural puede extenderse a las personas jurídicas. El no reconocimiento expreso de derechos fundamentales sobre las personas jurídicas no significa negar absolutamente dicha posibilidad, pues la sola existencia de un Estado constitucional democrático de derecho implica dotar de garantías a las instituciones por él reconocidas. De otro lado,

> […] quienes integran las personas jurídicas retienen para sí un interminable repertorio

[65] "Artículo 1. Objeto de la Ley. La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, […]."
[66] EXP. N.° 4972-2006-PA/TC. Fundamento 4. EXP. N.° 02714-2009-PA/TC. Fundamento 4

de derechos fundamentales nacidos de su propia condición de seres dignos, no siendo posible que dicho estatus, en esencia natural, se vea minimizado o, peor aún, desconocido, cuando se forma parte de una persona jurídica o moral. En tales circunstancias, queda claro que sin perjuicio de los atributos expresos que acompañan a cada persona individual que decide organizarse, puede hablarse de un derecho no enumerado al reconocimiento y tutela de las personas jurídicas, sustentado en los citados principios del Estado democrático de derecho y correlativamente de la dignidad de la persona.[67]

El Tribunal Constitucional, ha señalado que es constitucionalmente legítimo el reconocimiento de derechos fundamentales sobre las personas jurídicas, lo cual no puede tampoco llevar a la afirmación que todos los derechos atribuciones y libertades reconocidas a la persona natural sean compatibles con la naturaleza o características de cada organización de individuos, siendo el juez constitucional el que deberá cumplir el rol de "merituador" de cada caso, según las características o particularidades que le acompañan. [68]

Conforme a lo expuesto, en el expediente N.° 4972-2006-PA/TC. Fundamento jurídico 14, el Tribunal Constitucional señaló una enumeración enunciativa de los derechos que pueden resultar compatibles con la naturaleza o estatus de las personas jurídicas, dentro de los cuales mencionó, entre otros a "... e) El derecho a la autodeterminación informativa…". Esta afirmación del Tribunal Constitucional no es categórica ni determinante, sino que la misma deberá entenderse e interpretarse, según las circunstancias y en determinados supuestos.

Tal como se pudo apreciar en el marco del proceso de Hábeas Data, a través de su sentencia, de fecha 20 de febrero de 2009, recaída en el Exp. N. º 04670-2007-PHD/TC. En dicho proceso, la recurrente fue la empresa, Pesquera Alejandría S.A.C. y el demandado, fue el Ministerio de la Producción; la pretensión consistía en que dicho Ministerio se abstenga de suministrar a asociaciones, gremios pesqueros y/o

[67]EXP. N.° 4972-2006-PA/TC. Fundamento 11.
[68] EXP. N.° 4972-2006-PA/TC. Fundamento 13.

cualquier tercero, sin permiso de la recurrente o su autorización expresa, los datos, reportes e información individualizada proveniente del Sistema de Seguimiento Satelital (SISESAT); invocando entre otros la vulneración de sus derechos a la autodeterminación informativa, al secreto de las comunicaciones, a la privacidad de la intimidad personal. El Tribunal Constitucional, señaló en el fundamento jurídico 9, lo siguiente:

> Como es de verse, la información recabada no tiene el carácter de sensible ni reservada, de manera que, en el caso de autos no se está violentando el derecho constitucional a la autodeterminación informativa de la recurrente, por cuanto los datos objeto de difusión por parte del Ministerio de la Producción no tienen el carácter de sensible ni privado, ni se encuentran referidos a algún mecanismo o procedimiento que afecte de manera alguna el secreto industrial o empresarial de la recurrente, ya que la información difundida sólo se refiere a la ubicación y desplazamiento de las embarcaciones pesqueras. En ese sentido, el Tribunal Constitucional estima que la revelación de dichos datos a terceros no afecta el derecho a la autodeterminación informativa de la recurrente.

Queda claro entonces que en principio, y a la luz del reconocimiento constitucional del derecho fundamental a la protección de datos personales, el titular de este derecho será siempre la persona natural; pero vía proceso de Hábeas Data podrá serlo también, la persona jurídica dependiendo del análisis del caso concreto que realice el Poder Judicial o el Tribunal Constitucional según corresponda. Podemos apreciar en este punto, cómo el Máximo intérprete de la Constitución, vía interpretación, le otorga el reconocimiento de la titularidad de este derecho también a la persona jurídica; con lo cual ambas clases de personas, pueden buscar el amparo del derecho a la autodeterminación informativa vía jurisdiccional. Situación que no ocurrirá en la tutela administrativa que instaura la Ley de la materia N° 29733 y que veremos en el acápite correspondiente.

### c) Facultades del titular de la información

Previo a la dación del CPC, y partiendo del reconocimiento del derecho a la

autodeterminación informativa en virtud a lo dispuesto por Constitución Política de 1993, en el artículo 2°, inciso 6, el Tribunal Constitucional mediante la sentencia recaída en el Expediente N.º 666-1996-HD/TC, define varios aspectos que comprende el derecho a la autodeterminación informativa, a través del proceso de Hábeas Data; reconoce la ampliación de las facultades contenidas en el texto constitucional para el titular de la información y consagra lo que la doctrina ha venido denominando como derechos ARCO: a) El derecho de acceso, que luego estará consagrado en el artículo 61°, inciso 2 del CPC y mucho después en el artículo 19 de la Ley N° 29733[69].

El acceso, para el alto tribunal, supone "la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información […]." b) El derecho de actualización, inclusión, rectificación y supresión, que luego estará en el mismo artículo mencionado del CPC y en el artículo 20° de la Ley N° 29733[70], señalando que:

> […] el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien

[69] Artículo 19. Derecho de acceso del titular de datos personales. "El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos."

[70] "Artículo 20. Derecho de actualización, inclusión, rectificación y supresión

El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

Si sus datos personales hubieran sido transferidos previamente, el encargado del banco de datos personales debe comunicar la actualización, inclusión, rectificación o supresión a quienes se hayan transferido, en el caso que se mantenga el tratamiento por este último, quien debe también proceder a la actualización, inclusión, rectificación o supresión, según corresponda.

Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado del banco de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias, según ley, las que deben informar que se encuentra en trámite cualquiera de los mencionados procesos. (…)"

> con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que ésta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados.

Asimismo, podemos mencionar otra sentencia en igual sentido y también previa a la dación del CPC, la recaída en el expediente 1797-2002-HD/TC[71], sin perjuicio de las varias dadas con posterioridad a aquél cuerpo normativo.

En sentencia posterior, el Tribunal Constitucional reconoce, el derecho a impedir que se suministren datos o informaciones de carácter sensible, consolidando vía jurisprudencial lo que el CPC reconocía en el artículo 61°, inciso 2; lo que da cuenta de las amplias facultades que el derecho a la protección de datos le da al titular de los mismos. "…el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos". STC 04739-2007-PHD/TC. Fj 4.[72]

No podemos dejar de mencionar la labor pedagógica en este tema que el Tribunal Constitucional realizó en la sentencia de fecha 21 de diciembre de 2007, recaída en el Exp. N° 06164-2007-HD/TC, al dar una clasificación de los tipos de Hábeas Data en relación con las distintas facultades que le corresponden al titular de la información en virtud del derecho a la autodeterminación informativa o de protección de datos personales, en base a lo dispuesto tanto en la Constitución Política (art. 200, inciso 3)

---

[71] Emitida el 29 de enero de 2003. Fj 4.

[72] La sentencia citada se refiere a la oposición de la transmisión difusión de los datos sensibles, que son una categoría de datos personales más delimitada que los datos o información del ámbito privado, al que se refiere el artículo 61°, inciso 2 del CPC.

como en el Código Procesal Constitucional (art. 61 °)[73].

En el fundamento 2 de dicha sentencia, clasifica al Hábeas Data Puro, como el

[73] Fj. 2.**1. Hábeas Data Puro:** Reparar agresiones contra la manipulación de datos personalísimos almacenados en bancos de información computarizados o no.

**1.1. Hábeas Data de Cognición:** No se trata de un proceso en virtud del cual se pretende la manipulación de los datos, sino efectuar una tarea de conocimiento y de supervisión sobre la forma en que la información personal almacenada está siendo utilizada.

**1.1.1. Hábeas Data Informativo:** Está dirigido a conocer el contenido de la información que se almacena en el banco de datos (qué se guarda).

**1.1.2. Hábeas Data Inquisitivo:** Para que se diga el nombre de la persona que proporcionó el dato (quién).

**1.1.3. Hábeas Data Teleológico:** Busca esclarecer los motivos que han llevado al sujeto activo a la creación del dato personal (para qué).

**1.1.4. Hábeas Data de Ubicación:** Tiene como objeto que el sujeto activo del poder informático responda dónde está ubicado el dato, a fin de que el sujeto pasivo -el accionante- pueda ejercer su derecho (dónde).

**1.2. Hábeas Data Manipulador:** No tiene como propósito el conocimiento de la información almacenada, sino su modificación.

**1.2.1. Hábeas Data Aditivo:** Agrega al banco de datos una información no contenida. Esta información puede consistir: en la actualización de una información cierta pero que por el paso del tiempo se ha visto modificada; también puede tratarse de una información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado; o incorporar al banco de datos una información omitida que perjudica al sujeto pasivo.

**1.2.2. Hábeas Data Correctivo:** Tiene como objeto modificar los datos imprecisos y cambiar o borrar los falsos.

**1.2.3. Hábeas Data Supresorio:** Busca eliminar la información sensible o datos que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona. También puede proceder cuando la información que se almacena no guarda relación con la finalidad para la cual ha sido creado el banco de datos.

**1.2.4. Hábeas Data Confidencial:** Impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada. En este tipo, se incluye la prohibición de datos que por el paso del tiempo o por sentencia firme se impide su comunicación a terceros.

**1.2.5. Hábeas Data Desvinculador**: Sirve para impedir que terceros conozcan la identificación de una o más personas cuyos datos han sido almacenados en función de determinados aspectos generales como la edad, raza, sexo, ubicación social, grado de instrucción, idioma, profesión.

**1.2.6. Hábeas Data Cifrador:** Tiene como objeto que el dato sea guardado bajo un código que sólo puede ser descifrado por quien está autorizado a hacerlo.

**1.2.7. Hábeas Data Cautelar:** Tiene como propósito impedir la manipulación o publicación del dato en el marco de un proceso, a fin de asegurar la eficacia del derecho a protegerse.

**1.2.8. Hábeas Data Garantista:** Buscan el control técnico en el manejo de los datos, a fin de determinar si el sistema informativo, computarizado o no, garantiza la confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.

**1.2.9. Hábeas Data Interpretativo:** Tiene como objeto impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.

**1.2.10.Hábeas Data Indemnizatorio:** Aunque no es de recibo en nuestro ordenamiento, este tipo de habeas data consiste en solicitar la indemnización por el daño causado con la propalación de la información.

**2. Habeas Data Impuro:** Solicitar el auxilio jurisdiccional para recabar una información pública que le es negada al agraviado.

**2.1. Hábeas Data de Acceso a Información Pública:** Consiste en hacer valer el derecho de toda persona a acceder a la información que obra en la administración pública, salvo las que están expresamente prohibidas por la ley.

referido al derecho a la protección de datos personales y al Hábeas Data Impuro, el referido al derecho de acceso a la información pública.

Dentro del Hábeas Data Puro, hay dos sub clases, el Hábeas Data de Cognición, cuya finalidad es conocer la información y supervisar la forma en que ella está siendo tratada ( la que a su vez se sub clasifica en los Hábeas Data Informativo, Inquisitivo, teleológico y de ubicación ); y el Hábeas Data Manipulador, cuya finalidad es modificar la información almacenada ( la que a su vez se sub clasifica en los Hábeas Data Aditivo, Correctivo, Supresorio, Confidencial, Desvinculador, Cifrador, Cautelar, Garantista, Interpretativo e Indemnizatorio).

Importante también es la declaración que el Tribunal Constitucional hace, al concluir este mismo fundamento, pues deja sentado que las pretensiones en el Hábeas Data no tienen por qué entenderse limitadas a los casos que establece la ley, pues existe la posibilidad de extender su alcance protector a otras situaciones o alternativas que pudieran darse en la realidad.

### d) Aplicación del principio iura novit curia y deber de confidencialidad

En muchas sentencias el Tribunal Constitucional en aplicación del principio iura novit curia y en atención a una función pedagógica, particularmente relevante ante el nuevo derecho de la protección de datos personales o autodeterminación informativa, ha tenido que identificar y aplicar este derecho aunque el demandante haya invocado el de acceso a la información pública,[74] ambos derechos protegidos por el proceso del Hábeas Data. [75] Analicemos una sentencia donde se aplica el principio iura novit curia, y se pone en relieve el deber de confidencialidad con relación al tratamiento de los datos personales de un tercero.

[74] Resolución N. º 00569-2003-AC/TC Asimismo, se precisa sus límites. En ese sentido, el Colegiado precisa que cuando se trate del aforismo iura novit curia, al aplicarse el derecho a las cuestiones debatidas, se buscará no alterar ni sustituir las pretensiones y hechos fácticos que sustentan la demanda y resulten acreditados en el proceso (FJ 5-13).

[75] Por ejemplo las recaídas en los siguientes expedientes: N° 00281-2015PHD/TC; N° 00356-2015PHD/TC; N° 00412-2014PHD/TC; N° 00425-2014PHD/TC; N° 00700-2014PHD/TC; N° 04031-2013HD/TC; N° 02204-2014HD/TC; entre otras.

En la sentencia recaída en el Exp. N. º 04387-2011-PHD/TC[76], el Tribunal Constitucional declaró fundada la demanda de Hábeas Data, por haberse acreditado la violación del derecho a la autodeterminación informativa. En este caso, el actor consideraba que se había vulnerado su derecho de acceso a la información pública, pues había solicitado las copias certificadas de las actas de evaluación final pertenecientes a un institución educativa privada por el período comprendido desde el año 1997 hasta el año 2008, pues el actor se encontraba participando en un concurso público magisterial nivel I para nombramiento en una de las plazas vacantes de profesores de educación básica regular, y necesitaba comprobar su experiencia laboral docente en las instituciones educativas privadas, donde había laborado.

El Tribunal Constitucional estimó, en aplicación del principio iura novit curia, que el derecho cuya afectación debía ser objeto de dilucidación era el derecho a la autodeterminación informativa, en los términos establecidos por el artículo 2, inciso 6 de la Constitución y el artículo 61, inciso 2, del Código Procesal Constitucional. El Tribunal Constitucional estimó que las actas de evaluación final que correspondían al curso de computación e Informática, en tanto fueron suscritas por el actor y contenían una información que puede revelar no sólo su experiencia profesional sino su desempeño docente (en este caso para efectos de su postulación a la Carrera Pública Magisterial), correspondían también a un "dato personal" suyo, dentro de una relación laboral. [77]

Asimismo en la sentencia se precisó que:

> […] no se produjo sustracción de la materia, en tanto si el recurrente pretendía acceder a sus datos personales, al margen de que ya no se encontrara presente el motivo que dio origen a la solicitud (el Concurso Público para nombramiento de profesores en el Área de Gestión Pedagógica año 2011 habría concluido), pues dicho acceso puede efectuarse en cualquier momento, encuadrando la pretensión del recurrente en el derecho de acceso a los datos personales registrados en una entidad pública, regulado en el artículo 19 de la Ley Nº 29733 (hábeas data de cognición, en su modalidad

[76] Expedida a los 29 días del mes de agosto de 2013.
[77] Fundamento 10

específica de hábeas data informativo); precisó también, que el derecho de acceso a datos personales almacenados en un banco de datos, supone que una persona tiene derecho a obtener copia de la información particular que le concierne, al margen de si ésta se encuentra disponible en una entidad pública o privada (STC 0746-2010-PHD/TC, FJ. 5).

El Tribunal Constitucional identificó también a otros titulares de información personal, cuyos datos iban a ser puestos de manifiestos en las copias de las actas de evaluación final solicitadas por el recurrente; y precisa adecuadamente, que en tanto las actas de evaluación final contienen también datos relativos al rendimiento académico de los niños que fueron evaluados, dichas actas de evaluación a entregarse debían ser tachadas en la parte pertinente a la identidad (nombre) de los niños que allí figuraban a efectos de resguardar debidamente su identidad e intimidad. Ordenó al recurrente guardar el deber de confidencialidad sobre dichos datos, pudiendo utilizarlos sólo para fines de acreditación de su experiencia y desempeño docente, en los términos establecidos por el artículo 17 de la Ley Nº 29733.[78]

### 1.1.6. Ley de Protección de Datos Personales

El derecho a la protección de datos personales fue objeto de desarrollo legislativo a través de la ley N°29733, Ley de protección de datos personales, dieciocho años después de su reconocimiento constitucional[79].

Hasta el tres de julio de 2011[80], el único instrumento de tutela del derecho a la protección de datos personales en Perú era la acción de Hábeas Data. Con La Ley N° 29733, en adelante la Ley, se crea una autoridad de control, denominada Autoridad Nacional de Protección de Datos Personales, que reside en el Ministerio de Justicia y

[78] "Artículo 17. Confidencialidad de datos personales. El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales".

[79] Publicada el 03 de julio de 2011 en el Diario oficial El Peruano.

[80] Disposiciones complementarias finales. "DUODÉCIMA. Vigencia de la Ley. La presente Ley entra en vigencia conforme a lo siguiente: 1. Las disposiciones previstas en el Título II, en el primer párrafo del artículo 32 y en las primera, segunda, tercera, cuarta, novena y décima disposiciones complementarias finales rigen a partir del día siguiente de la publicación de esta Ley. […]"

Derechos Humanos, con lo que se suma a la tutela jurisdiccional del derecho, existente en el hábeas data, otra, desde el ámbito administrativo con la finalidad de que sea más efectiva y rápida.

A continuación, abordaremos algunos conceptos básicos de la Ley, relevantes para el presente trabajo.

#### 1.1.6.1. Conceptos fundamentales

**a) Dato personal**

La ley define como datos personales a "Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados"[81]. Serán datos personales, por ejemplo, la información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales,[82] antecedentes personales, datos académicos, laborales, características personales, datos de localización, entre otros. El legislador evita dar una lista cerrada de los datos personales.

Dentro de los datos personales existe una categoría especial constituida por los datos sensibles, que se consideran como tales porque merecen una especial protección, en la medida que un indebido tratamiento de los mismos, puede causar graves daños a la persona. Dentro de esta categoría especial de datos sensibles están los datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas; religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida amorosa y sexual[83]

De la definición de los datos personales es claro que quedan fuera del ámbito de aplicación de la Ley, los datos relacionados a las personas jurídicas; refiriéndose la Ley N° 29733, solo a la información personal de los seres humanos.

[81] Art.2, inciso 4.
[82] Art. 2, inciso 4. del Reglamento.
[83] Artículo 2, inciso 5 de la Ley y del Reglamento.

Para entender que estamos frente a un dato personal se requiere que concurra un doble elemento: por una parte, que exista una información o dato; y de otra parte, que dicho dato o información pueda vincularse a una persona física identificada o identificable. El dato personal debe proporcionarnos una información sobre una persona y debe ser posible asociar esa información al titular de la misma; que nos lleve a su identificación o nos permita identificarla.

Una persona es identificada cuando se la distingue de todas los demás, siendo el identificador más común el nombre (nombre y apellidos). Una persona será identificable, de manera directa o indirectamente, cuando sea posible hacerlo, porque para establecer la identidad se necesitará combinar el nombre con otros atributos, como dirección domiciliaria, fecha de nacimiento, fotografía, DNI, entre otros.[84] Para que una persona sea considerada identificable, deben tomarse en cuenta el conjunto de medios que puedan ser razonablemente usados para identificar a la persona, es decir si no se requieren plazos o actividades desproporcionados.

**b) Titular de datos personales**

El legislador peruano ha optado por circunscribir bajo el ámbito de protección de la Ley, -y por lo tanto dentro de la tutela administrativa del derecho- a la persona natural o física, excluyendo a las personas jurídicas, morales o de naturaleza ideal. El titular será la persona natural a quien correspondan los datos personales. El artículo 2, inciso 16 así lo dispone: "Titular de datos personales. Persona natural a quien corresponde los datos personales."

No obstante lo señalado, y remitiéndonos a lo expuesto en el acápite 1.1.5.b), para efectos de la tutela jurisdiccional, la titularidad podrá extenderse a la persona jurídica; lo que deberá entenderse e interpretarse, según las circunstancias y en determinados supuestos.

[84] Ver EXP. 9-PTT2015. En este sentido la Autoridad Peruana señala que el criterio que permite determinar si una información es o no dato personal consiste en preguntarse si el conocimiento por parte de terceros de esos datos puede tener consecuencias para el titular o si a partir de esa información puede tornarse alguna decisión que lo afecte.

### c) Tratamiento de datos personales

El tratamiento de datos personales es un concepto amplio, que en virtud del artículo 2, inciso 19, de la Ley, consiste en: "Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales."

El tratamiento de los datos personales puede realizarse dentro de un banco de datos personales o sin la existencia de éste. Así por ejemplo quien sube una foto de una persona a internet o recoge imágenes de una persona a través de una cámara de videovigilancia, pero no las graba, está realizando tratamiento de datos personales pero no lo hace dentro de un banco de datos.

Asimismo, tratamiento puede referirse a cualquier operación o procedimiento que se realice con un dato personal, puede ser de manera física, técnica o automatizada. Basta que se use un dato personal, lo que va desde su recogida, pasando por la simple conservación hasta su cancelación o supresión.

El tratamiento mismo y su finalidad serán definidos por el titular del banco de datos, o por el responsable del tratamiento (en el caso en el que no esté realizándose el tratamiento en el contexto de un banco de datos personales). Por lo señalado, desde que una persona, empresa u organización, recoge, o recopila datos de otra persona, ya está realizando una actividad de tratamiento. El hecho, por ejemplo, de almacenar una foto o imagen, aunque no se la utilizara para otra finalidad, ya supone un tratamiento y por ello estará dentro del ámbito de aplicación de la Ley y de su Reglamento.

### d) Banco de datos personales

Como se ha señalado, el tratamiento de los datos personales puede realizarse en el contexto de un banco de datos o fuera de él. En el caso de que el tratamiento de los

datos personales se lleve a cabo cuando existe un banco de datos, el elemento clave de su definición es que exista un conjunto organizado de datos personales, independientemente del soporte en que se encuentre. Así la Ley define al banco de datos personales como el: "Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso."[85]

Por lo señalado, la Ley y el Reglamento se aplicarán a los datos almacenados en soporte papel o en soporte automatizado. Cuando el almacenamiento de los datos personales sea en soporte papel se requerirá que estén organizados o estructurados conforme a criterios específicos relativos a las personas físicas, que hagan posible acceder sin esfuerzos desproporcionados a dichos datos.[86]

Los bancos de datos personales pueden ser de administración pública o privada. Serán de administración pública cuando su titularidad corresponde a una entidad del Estado; y serán de administración privada cuando su titularidad corresponde a una persona natural o jurídica de derecho privado.

### e) Titular del banco de datos personales y Responsable del tratamiento

La figura del titular del banco de datos o responsable del tratamiento de los datos personales es vital para efectos de la responsabilidad derivada del incumplimiento de la Ley y del Reglamento, frente a la persona afectada por un mal uso de la información que le concierne, y frente a la misma autoridad de control.

[85] Art. 2, inciso 1.
[86] Reglamento de la Ley Orgánica de Protección de Datos de Carácter personal Española, 15/1999, aprobado por Real Decreto 1720/2007 cuando define fichero no automatizado. art.5.1.n) " Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica"

Para la Ley peruana, el titular del banco de datos personales será la persona natural o jurídica que determina la finalidad y el contenido del banco de datos personales, así como el tratamiento de éstos y las medidas de seguridad que correspondan[87]. La Ley peruana no incorpora, en su texto, la figura del responsable del tratamiento. Consideramos que la figura del responsable del tratamiento es un concepto más amplio que abarca tanto al titular del banco de datos como a quien decida sobre el tratamiento de datos personales independientemente de que los datos consten o no en un banco. El Reglamento de la Ley, incorpora dentro de las definiciones[88] a la figura del responsable del tratamiento como aquél que decida sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos. Coexistirían entonces para legislación peruana la figura del titular del banco de datos con la del responsable del tratamiento.

### 1.1.6.2. Los principios rectores de la protección de datos personales

El derecho a la protección de datos personales requiere para su configuración de la adopción de determinadas garantías y principios que son los que establecen las pautas a los que debe ajustarse todo tratamiento de datos personales, desde el momento mismo de su recogida hasta su cancelación; la observación plena de los principios es garantía para estar frente a un tratamiento adecuado de la información de la persona.

Las Directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1009[89], han considerado como garantías mínimas una serie de principios:

[87] Art. 2. Inciso 17). La ley Argentina señala al Responsable de archivo, registro, base o banco de datos; la Ley de Costa Rica incorpora en su artículo 3, literal h), al responsable de la base de datos; y la ley de Nicaragua, al responsable del fichero de datos, en su artículo 2, literal k).
[88] Artículo 2, inciso 14).
[89] Consultado al 18 de noviembre en: http://transparencia.udg.mx/sites/default/files/Directrices%20para%20la%20regulaci%C3%B3n%20de%20los%20archivos%20de%20datos%20personales%20informatizados.pdf

1. Principio de legalidad y lealtad
2. Principio de exactitud
3. Principio de especificación de la finalidad
4. Principio de acceso de la persona interesada
5. Principio de no discriminación
6. Limitación de la facultad para hacer excepciones
7. Principio de seguridad
8. Supervisión y sanciones, a través de una autoridad que deberá ofrecer garantías de imparcialidad, independencia y competencia técnica
9. Flujo transfronterizo de datos basado en la similitud de las salvaguardas
10. Campo mínimo de aplicación general a todos los archivos informatizados públicos y privados.

La Ley peruana con carácter enunciativo, consagra los siguientes ocho principios rectores[90]: legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad,

[90] Artículo 4. Principio de legalidad
El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
Artículo 6. Principio de finalidad
Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.
Artículo 7. Principio de proporcionalidad
Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.
Artículo 8. Principio de calidad
Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.
Artículo 9. Principio de seguridad
El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.
Artículo 10. Principio de disposición de recurso
Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.
Artículo 11. Principio de nivel de protección adecuado
Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley

disposición de recurso y nivel de protección adecuado. El carácter enunciativo de los principios consagrados por la ley, daba margen para que el Reglamento pudiera incluir otros principios como podían ser los de transparencia o de responsabilidad, considerados por otras legislaciones;[91] o en su caso, haga un mayor y pedagógico desarrollo de los principios consagrados en la Ley; esto teniendo en cuenta el bajo nivel de conocimiento de la materia en la sociedad peruana en general; que la mayoría de los titulares de los bancos de datos, encargados de los mismos y responsables del tratamiento, no son abogados; y que además estamos ante una materia técnica; no obstante, el Reglamento de la Ley peruana optó por no hacer un mayor desarrollo de este aspecto esencial de toda normativa sobre protección de datos personales, lo cual desde nuestro punto de vista, debe suponer una labor más proactiva de la autoridad de control. (Zamudio 2014: 1165-1167).

Sin embargo, si partimos de los principios consagrados en el texto de la Ley peruana, se puede sostener que desde ella se pretende otorgar gran protección al tratamiento de los datos personales, siendo la misma Ley la que establece el valor de los principios. En efecto, de conformidad con lo señalado en el artículo 12 de la Ley, los principios constituyen guías para la actuación de los titulares de los bancos de datos personales, así como de los responsables y encargados de su tratamiento y, en general, de todos los que intervengan en alguna actividad de tratamiento con relación los datos personales; sirven de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su Reglamento; constituyen parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia.

Los principios servirán como parámetro obligatorio para determinar el nivel suficiente

o por los estándares internacionales en la materia.

[91] Principio de Transparencia: Estándares internacionales aprobados por la Resolución de Madrid 2009. 10. página 12. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Principio de responsabilidad: Estándares internacionales aprobados por la Resolución de Madrid 2009. 11. página 13. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. La ley Mexicana reconoce el principio de responsabilidad y la ley Colombiana el de transparencia.

de protección de los datos personales[92]; la Autoridad Nacional de Protección de Datos Personales tiene como una de sus funciones explícitas velar por el respeto de los principios[93]; y para cerrar el círculo, se establecen infracciones pasibles de sanción al tratamiento de datos personales contraviniendo los principios consagrados en la Ley[94].

Vamos a ocuparnos a continuación de cinco de los principios rectores que tienen particular relevancia a la hora del tratamiento de los datos personales de los trabajadores por parte del empleador en el contexto de la relación laboral; a saber los principios de: consentimiento, legalidad, finalidad, proporcionalidad y calidad.

a) **Principio de Consentimiento**

El principio de consentimiento se encuentra regulado en el artículo 5 de la ley: "Para el tratamiento de los datos personales debe mediar el consentimiento de su titular." El consentimiento del titular es la piedra angular que en nuestro ordenamiento jurídico legitima el tratamiento de la información personal y en torno al cual gira el sistema de protección de datos personales en Perú.
Por lo señalado el tratamiento de los datos personales será lícito si media el consentimiento del titular de los mismos.

La validez del consentimiento está supeditada a que se cumplan con determinadas características del mismo señaladas en el Reglamento; el cual establece que el consentimiento del titular debe ser libre, previo, expreso, informado e inequívoco. [95]

Libre; supone que el consentimiento se haya dado de manera voluntaria, sin que haya mediado error, mala fe, violencia o dolo.

[92] Artículo 2, inciso 10).
[93] Artículo 33, inciso 17).
[94] Reglamento de la LPDP. Cap. V, incorporado por el D.S. N° 019-2017-JUS.

[95] Reglamento de la Ley, artículo 12. Consultado al 08 de agosto de 2020 en: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf y https://www.aepd.es/sites/default/files/2019-09/memoria-AEPD-2000.pdf.

Previo; porque el consentimiento debe darse de manera previa a la recopilación del dato, o en su caso, anterior al tratamiento distinto a aquél por el cual ya se recogieron.

Expreso; es realizado a través de medios que están destinados a exteriorizar la voluntad del titular oralmente o por escrito. Oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral; y por escrito aquél que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo válido para el ordenamiento jurídico. El Reglamento señala que dentro del entorno digital, se acepta, como consentimiento expreso "hacer clic" "dar un toque" o similares y, como consentimiento escrito mediante el otorgamiento de firma electrónica o mediante escritura que quede grabada de tal forma que pueda ser leída o impresa.

Inequívoco; es el consentimiento otorgado de tal forma que no admita dudas de su otorgamiento.
Debe señalarse que tratándose de los datos sensibles o especialmente protegidos, la Ley exige que el consentimiento no basta que se dé expresamente, pues se requiere el consentimiento escrito, lo que viene a ser una manifestación del objeto de una protección reforzada a esta categoría de datos personales.

Informado; el consentimiento del titular requiere que, de manera previa a cualquier actividad de tratamiento, se le hayan informado sobre los alcances, las condiciones y por ende las finalidades del mismo; por dicha razón los artículos 18[96] de la Ley y el

[96] **"Artículo 18.** Derecho de información del titular de datos personales El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.
Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

12, inciso 4, del Reglamento se ocupan de señalar todo lo que el titular del Banco de Datos o Responsable del tratamiento debe poner en conocimiento del titular del dato en forma clara, expresa, de manera indubitable y con lenguaje sencillo. Este deber de información, que a su vez constituye un derecho[97] del titular del dato[98], es imprescindible para que este pueda ejercer su poder de control sobre su información a lo largo del tratamiento a la que sea sometida.

Así como el titular dispone de su información otorgando el consentimiento para que pueda iniciarse el tratamiento, también pone de manifiesto este poder, que es parte del contenido esencial del derecho, revocando el consentimiento que otorgó en su oportunidad. El artículo 13.7 de la Ley establece que: "El titular de datos personales puede revocar su consentimiento en cualquier momento, observando al efecto los mismos requisitos que con ocasión de su otorgamiento." El Reglamento desarrolla esta disposición legal, señalando que esta revocación del consentimiento puede realizarse sin justificación alguna y sin que se le atribuyan efectos retroactivos.[99]

---

En el caso que el titular del banco de datos establezca vinculación con un encargado de tratamiento de manera posterior al consentimiento, el accionar del encargado queda bajo responsabilidad del Titular del Banco de Datos, debiendo establecer un mecanismo de información personalizado para el titular de los
datos personales sobre dicho nuevo encargado de tratamiento.
Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento".

[97] Art. 18 de la Ley.

[98] "Artículo 60. Derecho a la información. El titular de datos personales tiene derecho, en vía de acceso, a que se le brinde toda la información señalada en el artículo 18 de la Ley y el numeral 4 del artículo 12 del presente reglamento. La respuesta contendrá los extremos previstos en los artículos citados en el párrafo anterior, salvo que el titular haya solicitado la información referida sólo a alguno de ellos. […]"

[99] "Artículo 16. Negación, revocación y alcances del consentimiento.

El titular de los datos personales podrá revocar su consentimiento para el tratamiento de sus datos personales en cualquier momento, sin justificación previa y sin que le atribuyan efectos retroactivos. Para la revocación del consentimiento se cumplirán los mismos requisitos observados con ocasión de su otorgamiento, pudiendo ser estos más simples, si así se hubiera señalado en tal oportunidad.

El titular de los datos personales podrá negar o revocar su consentimiento al tratamiento de sus datos personales para finalidades adicionales a aquellas que dan lugar a su tratamiento autorizado, sin que ello afecte la relación que da lugar al consentimiento que sí ha otorgado o no ha revocado. En caso de revocatoria, es obligación de quien efectúa el tratamiento de los datos personales adecuar los

El Reglamento cuida de señalar que será el titular del banco de datos o responsable del tratamiento en quien recaerá la carga de la prueba de la obtención del consentimiento.[100]

El derecho a la protección de datos personales convive con otros derechos y bienes jurídicos constitucionalmente protegidos, por lo que esta base fundamental, que constituye el consentimiento para que pueda iniciarse el tratamiento de los datos personales, admite excepciones, las que se encuentran reguladas en el artículo 14[101]

---

nuevos tratamientos a la revocatoria y los tratamientos que estuvieran en proceso de efectuarse, en el plazo que resulte de una actuación diligente, que no podrá ser mayor a cinco (5) días.

Si la revocatoria afecta la totalidad del tratamiento de datos personales que se venía haciendo, el titular o encargado del banco de datos personales, o en su caso el responsable del tratamiento, aplicará las reglas de cancelación o supresión de datos personales.

El titular del banco de datos personales o quien resulte responsable del tratamiento debe establecer mecanismos fácilmente accesibles e incondicionales, sencillos, rápidos y gratuitos para hacer efectiva la revocación."

[100] Art. 15.

[101] "Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos

de la Ley.

Dentro de los supuestos en los que no se requiere el consentimiento del titular de datos personales para los efectos de su tratamiento, encontramos a las entidades del Estado cuando transfieran datos para el ejercicio de sus funciones (inciso1); cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles al público, (inciso 2) como pueden ser Registros Públicos, las guías telefónicas, los diarios, revistas o informaciones que se propalan por los medios de comunicación social; cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento (inciso 5), entre otros supuestos.

Casos en los que si bien no es necesario el consentimiento del titular cuya información se está tratando, debe entenderse que al titular del banco de datos o responsable del tratamiento solo se le está dispensando del consentimiento y de ningún otro principio o deber derivado de la Ley y del Reglamento.
Por lo señalado en este apartado, tenemos que para el tratamiento de los datos personales, el titular del banco de datos o responsable del tratamiento requiere contar con el consentimiento del titular del dato o estar en alguno de los supuestos de excepción al consentimiento contenidos en el artículo 14 de la Ley.

---

sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos
y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.
12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley".

b) **Principio de Legalidad**

El artículo 4 de la Ley se ocupa de este principio de la siguiente forma**: "**El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos."

La Ley utiliza dos oraciones para definir de una manera más completa el principio de legalidad. La primera de las oraciones regula que "El tratamiento", es decir cualquier actividad que implique tratamiento de datos personales debe hacerse conforme a lo establecido en Ley y, por ende, en el Reglamento.
Pero este sentido de la legalidad supone, tal como lo señala el artículo 1º de la Ley, respetar no solo el derecho a la protección de datos personales, sino también los demás derechos fundamentales que la Constitución reconoce.

Además el segundo mandato que comprende el principio de legalidad, se refiere a la actividad de la recogida.

La recogida o recopilación es la actividad de tratamiento inicial o primera. Entendemos que al ser la primera, puede marcar la legalidad o ilegalidad del resto de actividades del tratamiento, lo que explicaría por qué la Ley quiso hacer énfasis en ella. Pero hay otra razón. La legalidad supone que los datos personales se traten desde la recogida a través de medios que sean legales, transparentes y lícitos.

El Informe del Comité Jurídico Interamericano de la OEA, sobre privacidad y protección de datos personales[102] se refiere a los medios justos y legales que son los que se deben emplear para recopilar los datos personales; entendiendo que esto se cumple cuando la recopilación es "compatible tanto con los requisitos jurídicos pertinentes como con las expectativas razonables de las personas basadas en su

[102] Adoptado en su 86º Período ordinario de sesiones, 23-27 de marzo de 2015, en Río de Janeiro, Brasil. Consultado al 18 de noviembre de 2020 en: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf; pág. 7.

relación con el controlador de datos o con otra entidad que recopile los datos y en el aviso o los avisos dados a las personas en el momento en que se recopilen los datos. Lo que excluye la obtención de datos personales por medio de fraude, engaño o con pretextos falsos."

El citado informe pone como ejemplo de violación de lo acabado de señalar, cuando una organización se hiciera pasar por otra en llamadas de tele marketing, aviso publicitarios impresos o mensajes por correo electrónico con el objetivo de engañar a los consumidores e inducirles a dar sus datos personales; como el número de su tarjeta de crédito, información sobre cuentas bancarias, entre otros.

Como podemos apreciar la legalidad en la recogida tendrá que ver con el cumplimiento por parte del responsable del tratamiento de informar de manera clara, expresa, indubitablemente y con lenguaje sencillo sobre las condiciones y características del tratamiento a que será sometida su información personal.

En todo caso sea desde la actividad de recogida, pasando por las de conservación, difusión, organización, consulta, transferencia, bloqueo, registro almacenamiento, etc. hasta llegar a la supresión, todas deben realizarse conforme a lo establecido en la Ley de Protección de Datos y en su Reglamento. Lo que incluye a los principios, normas para el tratamiento, derechos, etc.

c) **Principio de Finalidad**

El principio de finalidad está definido en el artículo 6 de la Ley como sigue: "Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización."

Podemos desdoblar en dos momentos la aplicación de este principio para su cabal

entendimiento.

- Primer momento: referida a la primera actividad del tratamiento, la recopilación. La finalidad[103] para la que se recogen los datos debe responder a ciertas características para que sea una finalidad válida a la luz de la Ley.

La finalidad debe ser: determinada, es decir cuando haya sido expresada con claridad, sin lugar a confusión[104], debe ser concreta; explícita, cuando se expresa de forma clara y determinada una cosa, tal como lo señaló la Autoridad Nacional de Protección de Datos Personales en el Expediente 28 PTT2016[105]; y lícita, cuando no sea contraria a la ley. Por lo tanto la finalidad para la que se recopilan los datos personales no puede ser confusa, no puede ser genérica o vaga que admita prácticamente cualquier cosa como podrían ser expresiones como: “para mejorar tu experiencia como cliente”, o “para finalidades similares”.

- Segundo momento: referido a todas las demás actividades del tratamiento, las cuales no pueden extenderse a una finalidad que no haya sido la establecida como tal al momento de la recopilación.

Esto significa que el consentimiento queda vinculado a las finalidades determinadas, explícitas y lícitas del momento de la recogida. Por lo que si el responsable del tratamiento desea realizar una actividad de tratamiento para una finalidad distinta de la que fue consentida, deberá solicitar un nuevo consentimiento para esa nueva finalidad. La finalidad, o finalidades que fueron objeto de consentimiento son las únicas que dan el marco o cobertura legal dentro del cual se pueden realizar las distintas actividades de tratamiento de manera legítima.

[103] O finalidades.
[104] Art. 8 del Reglamento.
[105] Página 10.

d) **Principio de proporcionalidad**

El principio de proporcionalidad está regulado por la Ley en su artículo 7, como sigue: "Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados." Como se desprende de la redacción legal, la proporcionalidad también se va a medir con relación a la finalidad del tratamiento autorizada.

Pongamos algunos ejemplos. ¿Por qué una "app" de música quiere acceder a la cámara del móvil? Es claro que una aplicación de música no necesita acceder a la cámara de tu celular para reproducir tus canciones favoritas, el tratamiento que haría de tus fotos sería excesivo y no adecuado para la finalidad musical.[106]

La proporcionalidad nos exige también entre los diversos tratamientos que nos permitirían cumplir la finalidad autorizada, elegir por aquél menos invasivo para la privacidad e intimidad.

Citemos como ejemplo una resolución del Tribunal Constitucional Español que censura a un Casino; el cual, para conseguir un adecuado control de la actividad laboral que se desarrollaba en las instalaciones dedicadas al juego de azar, en las dependencias de caja y en donde se hallaba ubicada la ruleta francesa, decidió completar uno de los sistemas de seguridad de que disponía, consistente en un circuito cerrado de televisión, con la instalación de micrófonos que permitieran recoger y grabar las conversaciones que pudieran producirse en las indicadas secciones del casino.

> […] la implantación del sistema de audición y grabación no ha sido en este caso

[106] Otro tema es el consentimiento que él o los titulares que acceden a estas aplicaciones suelen dar la mayoría de veces sin leer o sin leer detenidamente las políticas de privacidad. Consultado al 24 de mayo de 2020 en: https://www.abc.es/tecnologia/moviles/aplicaciones/abci-musica-quiere-acceder-camara-movil-cuidado-permisos-aplicaciones-201906020209_noticia.html?ref=https:%2F%2Fwww.google.com%2F

> conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial, pues la finalidad que se persigue (dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes del casino). Este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa. Se trata, en suma, de una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores del casino mantengan entre sí o con los clientes. (FJ 9)[107]

El tratamiento fue desproporcionado porque el grabar las conversaciones de los trabajadores y de los clientes resultaba siendo excesivo para la finalidad perseguida y legítima, afectando otros derechos fundamentales por un indebido o desproporcionado tratamiento del dato de la voz.

e) **Principio de Calidad**

El artículo 8 de la Ley define la calidad de la siguiente manera: “Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.”

La calidad supone cuatro aspectos:

[107] Consultado al 24 agosto de 2020: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4082

- Que los datos sometidos a tratamiento deben ser veraces; lo que implica que deben ser exactos y responder a la situación actual de sus titulares. En este caso si un banco de datos de clientes de una empresa prestadora de servicios de energía eléctrica no tiene actualizada mi dirección domiciliaria o la tiene errada, al no tratar un dato de calidad, por no ser exacto, podrá interrumpir el servicio que me brinda o inclusive llegar a facturar a una persona que no consumió el servicio. El Reglamento[108] de la Ley, señala en atención al principio de calidad, que los datos contenidos en un banco de datos personales deben ajustarse con precisión a la realidad.

Los datos se presumen exactos si son proporcionados directamente por el titular de los mismos[109]. No obstante, este principio no le deja al titular del dato toda la responsabilidad de la veracidad de su información; porque el titular del banco de datos o el responsable del tratamiento está obligado a comprobar la exactitud del dato desde que lo recopila; así como, a adoptar las medidas que le permitan la eliminación de inexactitudes en los datos que ya están bajo su responsabilidad, es decir siendo tratados sea en un banco de datos o sin él.

- Que los datos sean necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Otra vez vemos al principio de finalidad acompañar y delimitar el tratamiento que se haga de los datos personales.

En la resolución de la Autoridad Nacional de Protección de Datos Personales, recaía en el Expediente 40-PTT 2018, se declara fundada una reclamación de una persona que solicitó la supresión de sus datos personales del Sistema de Registro de Organizaciones Políticas (SROP) porque la organización política en la cual se había inscrito nunca llegó a tener reconocimiento como tal, no logrando adquirir personería jurídica ni existencia legal, por lo que el reclamante nunca tuvo la condición de afiliado.

[108] Artículo 9.
[109] Ibidem.

Sin embargo, cuando se ingresaba el número de su DNI en el SROP, aparecían sus datos. Ello configuraba un tratamiento de datos personales por parte del Jurado Nacional de Elecciones para una finalidad diferente para la que recogió dicha información personal.

Tanto la Constitución Política del Estado como la Ley Orgánica de dicho organismo constitucional autónomo le asignan como función mantener y custodiar el Registro de Organizaciones Políticas. La Autoridad sostuvo que:

> […] teniendo en cuenta que no culminó el trámite de inscripción como organización política que le haya otorgado personería jurídica y existencia legal, los datos personales del reclamante contenidos en el "Historial de Afiliación" del SROP a la fecha no son pertinentes ni necesarios para la finalidad para la cual fueron recopilados; asimismo, el reclamado estaría vulnerando el principio de proporcionalidad al realizar un tratamiento excesivo a la finalidad que originó su recopilación. 45. En consecuencia, no corresponde que el Jurado Nacional de Elecciones siga realizando la publicación de los datos personales del reclamante en el "Historial de Afiliación" del SROP.

Culminada la finalidad autorizada para el tratamiento del dato, éste deberá ser suprimido; es decir, dejado de tratar, por carecerse de legitimidad para continuar, en atención a que el consentimiento o, habilitación legal del tratamiento por excepción del artículo 14, ya no existiría ante el agotamiento de la finalidad que lo justificaba.

- La calidad del dato tiene que ver también con el principio de seguridad, que veremos en el siguiente apartado, puesto que una brecha de seguridad puede alterar o eliminar el dato, entre otras incidencias, con lo que la información ya no sería la exacta o ya no habría la información.

- La calidad también tiene que ver con el tiempo de conservación del dato, el mismo que no debe exceder al necesario para cumplir con el fin para el que se lo recogió. Por lo que si el titular del banco de datos o responsable del tratamiento, identifica otra finalidad de utilidad para él, no está habilitado a conservar los datos para esta

última finalidad; y deberá garantizar que no seguirá tratando la información personal, lo que incluye su conservación, más allá del tiempo necesario.

f) **Principio de Seguridad**

El principio de seguridad está regulado en el artículo 9 de la Ley: “El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.”

Las medidas de seguridad, son de tres clases, técnicas, legales y organizativas; y persiguen evitar la alteración, pérdida, tratamiento o acceso no autorizado a la información personal.

Los daños generados por una brecha de seguridad pueden ser de diferente magnitud en los derechos de los titulares de la información. ¿Qué daño causaría si por una brecha de seguridad se alteraran los datos, si se los modificaran?; o ¿si el dato fuera suprimido? dejando al titular del banco de datos sin la información a la que debe acceder para brindar un servicio, por ejemplo.
Asimismo, puede pasar que alguien, que no está autorizado, acceda a los datos personales, no solo algún trabajador de la organización del responsable del tratamiento, sino algún tercero con fines ilícitos; no es extraño a nuestra realidad recibir llamadas extorsionadoras a nuestros celulares, que nos amenazan de diferentes formas, con lo cual ante un indebido tratamiento de la información personal (incumplimiento del principio de seguridad) se estarían además violando otros derechos, como a la libertad y seguridad personales, o a la vida misma.

El artículo 16 de la Ley prescribe una prohibición que pone de manifiesto la seriedad con la que se debe tomar cuenta de la seguridad a la hora de tratar la información

personal “Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.”

Complementando lo señalado, como sabemos, el tratamiento de datos se puede realizar también sin que exista un banco de datos; siendo que el principio de seguridad, como los otros principios, alcanzan a todo tratamiento, exista o no un banco de datos de por medio.

### 1.2. Definición, alcances y contenido del derecho a la protección de datos personales

#### -Definición

La definición del derecho a la protección de datos personales en Perú, si bien es cierto parte de lo que señala el artículo 2, inciso 6) constitucional, ha sido enriquecida y complementada por la labor de la jurisprudencia del Tribunal Constitucional[110], tal como puede apreciarse en lo tratado en el acápite 1.1.5 de la presente investigación; y por la propia Ley de desarrollo constitucional del citado dispositivo, Ley de Protección de Datos Personales, N° 29733; todo lo cual nos sirve de base para entender este nuevo derecho humano reconocido en nuestra Carta fundamental vigente, desde 1993.

---

[110] Sobre el derecho a la autodeterminación informativa, este Tribunal ha establecido que: [e]l derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal. Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen (…). En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera “sensibles” y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos (STCS 04739-2007-PHD/TC, FF.JJ. 2-4 y 0746-2010-PHD/TC, FJ. 4).

Este derecho, que si bien es cierto, nace motivado principalmente para limitar los abusos de la informática o hacer frente a sus intromisiones indebidas, no se restringirá a defender el debido tratamiento de la información personal por medios electrónicos, sino cualquiera sea la forma o medio por el que esta se trate. Definamos al derecho.

El derecho a la protección de datos personales consiste en una serie de facultades que le corresponden a la persona para disponer y controlar la información sobre ella misma, frente a su uso por parte de terceros, con el fin de que sea objeto de un debido tratamiento.

Las facultades que este derecho le otorga a su titular son diversas y amplias y no se restringen a negar o no suministrar informaciones que afecten la intimidad personal o familiar, como reza el artículo 2, inciso 6) de la Constitución. Dichas facultades comprenden:

- La disposición; que se traducirá en el consentimiento, que debe dar para que un tercero pueda realizar el tratamiento de su información personal, desde su recogida hasta su cancelación; salvo los supuestos de excepción al mismo, legalmente establecidos (Art. 14 de la Ley). El principio del consentimiento es la piedra angular que legitima el tratamiento de los datos personales. (Art. 5 de la Ley).

- El control de su información; que se concretará en diversos derechos que se le reconocen al titular de los datos, tales como el de ser informado (Art. 18 de la Ley) sobre las condiciones en que se realizará el tratamiento de su información, previo al otorgamiento de su consentimiento; sumado a los derechos, que limitadamente quedan presentados internacionalmente por el acrónimo ARCO[111], referidos a los derechos de Acceso (Art. 19 de la Ley), para saber quién posee sus datos, desde cuándo, con qué finalidad, por cuánto tiempo y si han sido objeto de transferencia o no; el derecho de Actualización, Inclusión, Rectificación y

[111] Acceso, rectificación, cancelación y oposición, no obstante al titular de la información se le reconocen o pueden reconocer más derechos.

Supresión o Cancelación de la información que le concierna (Art. 20 de la Ley); pudiendo oponerse (Art. 22 de la Ley) a esa posesión, transferencia y uso.

Como puede apreciarse la regulación del derecho a la protección de datos personales no busca impedir el tratamiento de los mismos, pues éste es necesario para el desarrollo de las actividades privadas y públicas, nacional e internacionalmente; sino busca que dicho tratamiento se realice de manera debida a la dignidad y a los derechos de la persona, como titular de la información en el contexto de un Estado Constitucional de Derecho; y en este sentido es que quien trate los datos personales debe observar los principios, respetar los derechos del titular y cumplir las demás obligaciones derivados de la Ley y el Reglamento.

Los terceros frente a quienes el titular de los datos puede ejercer las facultades derivadas de este derecho pueden ser personas naturales y personas jurídicas, del sector privado y del sector público, sea que traten los datos personales de manera automatizada o no.

La información sobre su persona con relación a la que el titular puede ejercer estas facultades o poderes es cualquier información, no solo la referida o relacionada con el ámbito de la intimidad personal o familiar[112] sino a cualquiera que le concierna, pues será el titular quien decidirá qué datos considera oportuno controlar.

**-Alcances**

Analizar los alcances del derecho a la protección de datos personales nos lleva a verlo en dos aspectos propios de su naturaleza de ser un derecho fundamental: como derecho subjetivo y como institución objetiva (Landa 2017: 76).

Como derecho subjetivo, el titular de la información puede ejercer el control sobre el uso que se le dé a la misma por parte de un tercero (Estado o particular), sea que el tratamiento se realice en un banco de datos o fuera del él, de manera automatizada o no.

[112] Art. 2, inciso 6) constitucional.

Control, como ya se refirió, que abarca desde saber quién recopiló los datos, de quién lo hizo; así como conocer las distintas actividades de tratamiento a que haya sido sometida su información y las finalidades de las mismas; incluyendo todos los derechos que la Ley le reconoce y que materializan el control que le es propio sobre la información que le concierne; dentro de lo que se encuentra, la capacidad de oponerse a que se sigan tratando sus datos personales, hasta requerir su cancelación.

El control debe garantizar que el titular de los datos conozca y, como regla, haber consentido a todo tratamiento al que sea sometida su información personal por parte de un tercero.

De lo anteriormente señalado viene aparejada la consideración de ser una institución objetiva; pues la protección de datos, como derecho fundamental, demanda una actividad positiva de los poderes públicos; una serie de obligaciones a cargo de las entidades del Estado así como de las instituciones y personas del sector privado que realicen actividades de tratamiento de los datos personales.

Por ello, corresponde que se establezcan medidas efectivas de garantía del ejercicio del derecho, frente a un indebido tratamiento de los datos personales o un recorte indebido de las facultades, que este derecho le asigna a su titular.

Las medidas de garantía de este derecho son de dos tipos, una jurisdiccional y una administrativa. A través de la garantía procesal específica, que recae en el proceso de Hábeas Data, el titular del dato puede recurrir al Poder Judicial para la defensa de su información personal frente a los tratamientos indebidos o abusos que puedan significar una vulneración o amenaza; sea que provengan de cualquier persona, funcionario o autoridad. Aspectos importantes de lo cual, hemos podido apreciar en el desarrollo del acápite 1.1.5 referida a la jurisprudencia constitucional.

A esa protección judicial y con el fin de hacer más efectivo el derecho, es que se suma una protección de carácter administrativo a través de una autoridad de control, la Autoridad Nacional de Protección de Datos Personales, que fue creada mediante

la Ley N° 29733, dentro del ámbito del Ministerio de Justicia y Derechos Humanos. [113] Dicha autoridad vela por el cumplimiento de las normas sobre la materia y ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.

Cabe resaltar el Derecho de Tutela, que le corresponde al titular del dato personal para dirigirse, en vía de reclamación a la autoridad de control, ante el supuesto de que el titular del banco de datos o responsable del tratamiento le haya denegado total o parcialmente el ejercicio de alguno de los derechos (ARCO) que la Ley le reconoce.

**-Contenido**

El contenido del derecho a la protección de datos personales se delimita a través de los derechos (ARCO) que le corresponden a su titular y de los principios rectores que deben ser observados por los titulares de los bancos de datos o responsables del tratamiento, así como por los encargados del mismo. Si no se reconocieran estos derechos y no se observaran estos principios se desdibujaría este derecho fundamental y autónomo; y al decir de Piñar Mañas, (2005:101) se violentaría el mismo.

La dignidad de la persona está en la base de sus derechos y en nuestro caso en el del derecho a la protección de datos personales. El tratamiento de los datos lo efectúa un tercero; por lo que, al realizar cualquier actividad que constituya tratamiento de datos personales debe hacerlo observando los principios rectores, a los que nos hemos referido en el apartado 1.1.6.2.; es decir, se deben tratar los datos personales conforme a lo establecido en la Ley, principio de Legalidad; debe mediar el consentimiento de tu titular, principio de consentimiento; no puede extenderse a otra finalidad que no haya sido la establecida al momento de su recopilación, principio de finalidad; el tratamiento debe ser adecuado, relevante y no excesivo para la finalidad para la que se recopilaron, principio de proporcionalidad; los datos que se

[113] En la Actualidad y por modificación del Decreto Legislativo N°1353 (2017) la autoridad recae en la Dirección General de Transparencia Acceso a la Información pública y Protección de Datos Personales. Sus funciones están reguladas mediante el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS. Artículos 70-75.

traten deben ser veraces, exactos, actualizados y además adecuados respecto de la finalidad autorizada y solo por el tiempo necesario para cumplir con ella, principio de calidad; estando prohibido el tratamiento de datos que no esté rodeado de las medidas de seguridad técnicas, organizativas y legales adecuadas.

¿Pero, cómo controla el titular, cuyos datos están siendo tratados, que se están observando estos principios en las distintas actividades del tratamiento?; ¿Cómo hace el titular para no perder el control sobre su información personal, después de que esta fue recopilada?

La respuesta es por medio de los derechos que la Ley le reconoce como titular de los datos personales y que están regulados entre sus artículos 18 y 24.

-Así el poder de disposición, que se concreta en el consentimiento, supone que el titular antes de otorgarlo, tiene el derecho y por lo tanto debe ser informado de manera detallada, sencilla, expresa e inequívoca y previamente a su recopilación, sobre la finalidad del tratamiento, la identidad y domicilio del responsable del tratamiento, del encargado y de los posibles destinatarios, las transferencias a realizar, el tiempo de conservación, el carácter obligatorio o facultativo de sus respuestas; así como, la posibilidad de ejercer los derechos que la Ley le reconoce. (Art. 18).

Ahora bien, otorgado el consentimiento, ¿cómo hace el titular para corroborar que se están cumpliendo las condiciones del tratamiento autorizadas?, y en sí; ¿si se están observando, de manera debida, los principios que por Ley deben guiar el tratamiento de sus datos?; preguntas pertinentes, pues el poder que el derecho a la protección de datos personales le da al titular de los mismos, no queda en el otorgamiento de su consentimiento; sino que debe extenderse, para hacer efectivo su control, a todo el tratamiento hasta la finalización de él. Esto requiere de manera indispensable el poder ejercer los derechos ARCO.

-El derecho de Acceso. (Art. 19) sea que se otorgó el consentimiento, o que el dato fue recopilado en virtud a una de las excepciones del mismo; el titular mediante este

derecho, podrá conocer qué datos se están tratando, cómo se recopilaron, las razones que motivaron su recopilación, a solicitud de quién se hizo, así como las trasferencias realizadas o por realizarse; incluyendo todas las condiciones y generalidades del tratamiento de los mismos[114].

- El derecho de Actualización, Inclusión, Rectificación y Supresión. (Art. 20) El titular de los datos, puede actualizar, en vía de rectificación, aquellos datos que hayan sido modificados a la fecha del ejercicio del derecho;[115] asimismo, solicitar la incorporación de la información faltante en atención a la relevancia para el tratamiento.[116] La Rectificación supone también la posibilidad de solicitar que se modifiquen los datos que resulten ser inexactos, erróneos o falsos.[117]

-El derecho de Oposición. (Art. 22). Opera fundamentalmente, cuando el titular no hubiera prestado su consentimiento para su recopilación, en cuyo caso se busca la supresión del dato.[118]

-El derecho a impedir el suministro. (Art. 21) Se refiere directamente a que el titular del dato se opone a que sus datos sean cedidos o transferidos.

-El derecho al tratamiento objetivo. (Art. 23) supone que el titular no debe verse sometido a una decisión con efectos jurídicos sobre él, sustentada solo en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, como parte de un proceso de toma de decisiones, en el que él no tenga participación. [119]

-Derecho a la Tutela. (Art. 24) Derecho a la tutela administrativa (ante la Autoridad Nacional de Protección de Datos Personales) como a la tutela judicial (Hábeas Data)

[114] Art. 61 del Reglamento de la Ley. Aprobado por Decreto Supremo N° 003-2013-JUS, en adelante el Reglamento.
[115] Art. 64.del Reglamento.
[116] Art. 66.del Reglamento.
[117] Art. 65.del Reglamento.
[118] Art. 71.del Reglamento.
[119] Art. 72.del Reglamento.

cuando se le haya denegado el ejercicio de los derechos antes mencionados, por parte del titular del banco de datos o responsable del tratamiento.

Estos derechos (ARCO) no pueden faltar como parte de la protección que el derecho fundamental a la protección de datos le confiere a su titular, pues se encuentran en la base del sistema y solo mediante ellos, el titular del dato puede hacer efectiva su facultad de control sobre su información personal.

### 1.2.1. Naturaleza relacional del derecho a la protección de datos personales

Nos parece importante abordar, con la finalidad de comprender mejor el derecho que nos ocupa y resaltar un aspecto de su importancia, el referirnos a lo que nuestro Tribunal Constitucional ha denominado como derecho relacional.

"Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos […]".[120]

Como podemos apreciar a la luz de lo señalado por el Tribunal Constitucional[121], y que va acorde con la doctrina, es que el derecho a la autodeterminación informativa o a la protección de datos personales comprende una serie de facultades que le corresponden al titular de la información para que éste posea el control sobre la misma, con el fin de evitar extralimitaciones en su uso[122], o un indebido tratamiento de su información, que le pueda afectar o causar un daño, lo que no se restringe a su espera íntima; pues lo que busca este derecho es proteger a la persona misma, en la totalidad de los ámbitos que la conciernen.

[120] STC 04739-2007-PHD/TC. FJ 3
[121] Mucho antes de que se diera la Ley de Protección de datos personales en el 2011, Ley N° 29733.
[122] STC 04739-2007-PHD/TC FJ. 6. Pero el derecho a la autodeterminación informativa también supone que una persona pueda hacer uso de la información privada que existe sobre ella ya sea que la información se encuentre almacenada o en disposición de entidades públicas o de carácter privado. En ese sentido parece razonable afirmar que una persona tiene derecho a obtener copia de la información particular que le concierne, al margen de si ésta se encuentra disponible en una entidad pública o privada

Con esta afirmación se pone de manifiesto la importancia de este derecho, pues su desconocimiento puede estar relacionado con afectaciones a distintos ámbitos de la persona y por lo tanto su violación afectaría a la persona misma.

El Tribunal Constitucional pone énfasis en la naturaleza del derecho a la protección de datos personales, al señalar que es un derecho relacional. Con el fin de llegar a esta afirmación, parte de la naturaleza autónoma del derecho a la protección de datos personales, para poder diferenciarlo de otros derechos, con los que es frecuente verlo vinculado. Uno de los primeros momentos en que el Tribunal Constitucional se pronuncia en este sentido es en la sentencia emitida el 29 de enero de 2003, recaída en el Expediente N° 1797-2002-HD/TC[123] previo a la dación del CPC.

> 3. […] el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen. Tampoco el derecho a la autodeterminación informativa debe confundirse con el derecho a la imagen, reconocido en el inciso 7) del artículo 2° de la Constitución, que protege, básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad. Finalmente, también se diferencia del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad. En ese sentido, por su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, prima facie y de modo general, un derecho de naturaleza

[123] Fj 3.

relacional, pues las exigencias que demandan su respeto se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales. (El subrayado es nuestro).

Nuestro máximo intérprete de la Constitución nos muestra la gran riqueza de este derecho, actor principal en los tiempos de la sociedad de la información en la que nos encontramos en un contexto de la globalización de las comunicaciones, donde el uso de las tecnologías de la información permite transmitir y difundir información en tiempo real con alcances casi ilimitados[124] aumentando exponencialmente los riesgos para la persona (sus derechos) frente a un indebido tratamiento de la información que le concierne. El derecho a la autodeterminación informativa o protección de datos personales, supone el control de toda información sobre una persona que la identifica o hace identificable. Este tipo de información es amplísima[125] y puede estar relacionada con todo ámbito de la vida.

El Tribunal Constitucional Español, en la sentencia 11/1998, de 13 de enero de 1998, puso de manifiesto lo acabado de señalar. Se trataba de un trabajador de la empresa RENFE, afiliado a un sindicado. El comité General de Empresa convocó a huelga apoyada por varios sindicatos, uno de ellos, era al que pertenecía el trabajador recurrente. Pese a que el recurrente no participó en la huelga la empresa aplicó el descuento para los trabajadores que estuvieran afiliados al citado sindicato.
La empresa conocía el dato de la afiliación porque descontaba de los salarios la cuota sindical mediante diversas claves informáticas. La empresa presumió que el trabajador había participado en la huelga por pertenecer a uno de los sindicatos convocantes.

Como señala el alto Tribunal, (FJ 7) el dato de la afiliación, del trabajador recurrente,

[124] Aplicaciones para dispositivos móviles, vigilancia electrónica masiva. Big data, cloud computing, etc. Que permiten, inclusive, controlar conductas de las personas.
[125] Nombre, apellidos, la fecha de nacimiento, la dirección del domicilio, la dirección de correo electrónico; número de teléfono, de ruc, de la placa del vehículo, la huella digital, el ADN, una imagen (fotografía) la voz, el número del seguro social, información crediticia, cuentas bancarias, ingresos, creencias religiosas, afiliación sindical o política, datos de salud, huella digital, datos biométricos, hábitos sexuales, origen racial y étnico, etc.

a determinado sindicato, se facilitó con la única y exclusiva finalidad lícita de que la empresa descontara de la retribución la cuota sindical y la transfiriera al sindicato, no obstante el dato fue objeto de tratamiento automatizado y usó la correspondiente clave informática para un propósito radicalmente distinto, que consistió en retener la parte proporcional del salario relativo al período de huelga.

"[…] estamos ante una decisión unilateral del Empresario que supone un trato peyorativo para el trabajador por razón de su adhesión a un Sindicato (art. 12 L.O.L.S.), que le pudiera perjudicar a causa de su afiliación sindical […]" Se configuró entonces la indebida utilización de "un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de la libertad sindical".

En esta sentencia, el Tribunal Constitucional Español, ratifica lo que ya había señalado en la STC 254/1993 con relación al derecho a la protección de datos personales:

> […] que dicho precepto incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona proveniente de un uso ilegítimo del tratamiento mecanizado de datos. (FJ 6)

Sabemos que la persona es la que tiene el poder de disponer y de controlar sus datos personales y la capacidad decidir sobre los mismos. No obstante, cuando esto no se respeta, puede tener consecuencias de diferente incidencia en la persona, en sus derechos y en su dignidad. Veamos otro ejemplo de la naturaleza relacional del derecho, a través de un indebido tratamiento de la información personal cuya afectación, más allá del derecho a la protección de datos personales, alcanzará a otros derechos fundamentales.

Una cámara de vídeo vigilancia colocada en un ascensor de un hotel capta y graba a una pareja dándose abrazos y besos apasionados, siendo que los protagonistas de esta escena amorosa son casados, pero no entre ellos.

Dicha escena, en lugar de ser eliminada o suprimida, que es lo que el responsable del tratamiento debió hacer, pues dicha escena grabada no era pertinente para la finalidad de seguridad que es lo que justificaba el funcionamiento de la mencionada cámara, es subida a internet y recogida por varias publicaciones escritas y canales de televisión locales.

Este caso da cuenta de un indebido tratamiento, pues la escena no tenía importancia para el tema de seguridad (finalidad de la cámara de vídeo vigilancia), tampoco su difusión por internet fue con el consentimiento[126] de la mujer y el hombre protagonistas de la citada escena. Al haber usado esa información personal (imagen) de estas dos personas, mantenerlas grabadas, subirlas a internet, difundirlas por canales de televisión, se configuró un indebido tratamiento y con ello la violación del derecho a la protección de datos personales; pero la violación de este derecho conllevó la de otros derechos fundamentales en atención a la naturaleza relacional de aquél.

Así por ejemplo, se afectó el derecho a la intimidad, pues el beso apasionado se lo dieron ambas personas protegidas por las cuatro paredes del ascensor, que generaba un entorno íntimo que excluía de su conocimiento a los demás; en ese convencimiento actuaron.
Se afectó el derecho a la imagen, pues no autorizaron que difundieran sus imágenes y, menos en esas circunstancias, por internet ni por ningún medio de comunicación social.

Se afectó su derecho al honor, pues con la difusión de tal escena, la reputación del hombre y de la mujer, casados cada uno por su lado, se vio afectada y la idea que sobre ellos se proyectaba hacia la sociedad, sin duda, cambió y disminuyó. A partir

[126] Ni con su conocimiento, que no es en ningún caso suficiente.

de lo señalado puede analizarse la violación de otros derechos, como pueden ser el derecho a la libertad y al libre desarrollo de su personalidad, entre otros.

Vemos como un uso indebido de la información de una persona, que implica una violación de su derecho a la protección de datos personales o a la autodeterminación informativa, dependiendo de la información indebidamente usada, puede afectar otros derechos fundamentales y generar afectaciones graves a la persona misma.

Es pertinente señalar que el mismo CPC, en su artículo 61, inciso 2) también hace referencia a la naturaleza de derecho relacional de la autodeterminación informativa y lo hace cuando en la última parte del mismo dispositivo señala toda persona puede acudir al proceso de Habeas Data para "[…] hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales."

En igual sentido, lo hace la Ley N° 29733[127], cuando señala que el objeto de la misma es "[...] garantizar el derecho a la protección de los datos personales, […] a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales […]".

En efecto, en muchas ocasiones, el adecuado tratamiento de la información personal garantizará a su vez el respeto a otros derechos de la persona; por lo que, a la inversa, un indebido tratamiento de los datos personales supondrá, en no pocos casos, una afectación a otros derechos fundamentales del titular de la información.

### 1.3. La regulación del derecho a la protección de datos personales geolocalizados de los trabajadores en España

El marco normativo europeo de protección de datos experimentó cambios en aspectos significativos con la aprobación del Reglamento (UE) 2016/679 del

[127] Artículo 1°.

Parlamento Europeo y del Consejo, de 27 de abril de 2016[128] (Reglamento General de Protección de Datos, en adelante, RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE.
En atención a su naturaleza jurídica, el RGPD es una norma de aplicación directa en los Estados.

España, a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, en adelante LOPDGDD, ha pretendido adaptar el ordenamiento jurídico español al RGPD, y completar sus disposiciones; en esa tarea ha introducido algunas novedades importantes a tener en consideración.

Dentro de los cambios que trajo esta nueva normativa europea podemos encontrar algunos en el ámbito de las relaciones laborales, imponiendo mayores deberes a los empleadores, a la hora de tratar los datos de sus trabajadores, como responsables del tratamiento y por ende garantizando en mayor medida los derechos de estos y en especial el referido a la protección de datos personales.

La legislación sobre protección de datos peruana tomó como fuente directa y fundamental la Ley española sobre la materia[129] y a la Directiva 95/46/CE, sustituida por el RGPD; por lo que, resulta pertinente, y especialmente relevante para nosotros, tomar en cuenta estos cambios normativos relacionados con el principal objeto del presente trabajo de investigación, el tratamiento de los datos geolocalizados de los trabajadores con fines de control laboral; además, de constituir un parámetro de mayor garantía para un derecho fundamental y para la dignidad de la persona, lo que corresponde en un Estado Constitucional de Derecho.

Ante el creciente uso de las diversas tecnologías que permiten que los trabajadores puedan ser objeto de controles, que implican seguimiento que traspasan la barrera del horario de trabajo; que posibilitan acceso a más datos de los necesarios para el ejercicio del control laboral; que en muchas ocasiones se usan los datos personales

[128] Que entró en vigencia el 25 de mayo del 2018.
[129] La Ley Orgánica 15/1999 de Protección de Datos de Carácter General, vigente hasta diciembre de 2018.

para otros fines incompatibles con los legítimos dentro de la relación laboral; y siendo que, además, esto suele ocurrir sin que el trabajador, como titular de los datos, esté debidamente informado al respecto; es que desde el RGPD se pretende promover una real protección a los trabajadores.

En el sentido expuesto, el considerando 155 del RGPD señala la posibilidad para que los Estados miembros y en ellos, los convenios colectivos pueden regular de manera específica sobre diferentes aspectos relacionados con el tratamiento de los datos personales de los trabajadores en el ámbito laboral:

> El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

En la línea señalada, el artículo 88 del RGPD, establece, en su inciso 1, que los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de los datos personales de los trabajadores en el ámbito laboral y en particular en los siguientes aspectos:

-Contratación de personal;

-Ejecución del contrato de trabajo (incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo);

-Gestión, planificación y organización del trabajo;

- Igualdad y diversidad en el lugar de trabajo;

-Salud y seguridad en el trabajo;

-Protección de los bienes de empleados o clientes;
-Ejercicio y disfrute individual o colectivo, de los derechos y prestaciones relacionados con el empleo, y
-Extinción de la relación laboral.

El inciso 2, del artículo 88 del RGPD, dispone que las normas que se den según lo acabado de señalar, incluirán medidas adecuadas y específicas para preservar la dignidad humana, los intereses legítimos y los derechos fundamentales, debiendo prestarse especial atención a:

-La transparencia del tratamiento; que implica la debida información sobre los alcances del mismo para el titular de los datos;
-La transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta; y a
-Los sistemas de supervisión en el lugar de trabajo; que conlleva el tratamiento de los datos de los trabajadores por parte del empleador para los fines de control.

Como vemos el RGPD marca y exterioriza la firme voluntad para que se dé una especial atención al tratamiento de los datos personales en el entorno empresarial y específicamente en el ámbito laboral, donde la recopilación y gestión de los datos de los trabajadores debe estar garantizada de manera específica, más aún en el contexto de uso cada vez más intensivo e intrusivo de las Tic, que generan mayores riesgos para los derechos de la persona del trabajador a la hora en que se trata su información personal.

Acogiendo y adaptándose a lo señalado por el RGPD, España, a través de su Ley Orgánica 3/2018, LOPDGDD, incorpora un título, el X, referido a la Garantía de los derechos digitales. En dicho título nos parece, de especial vinculación con el control laboral a través de los datos localizados de los trabajadores, lo regulado en los artículos 87, “Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral; 88, “Derecho a la desconexión digital en el ámbito laboral” y el 90, “Derecho a la intimidad ante la utilización de sistemas de geolocalización”.

Por medio del artículo 87, el legislador español reconoce el derecho a la intimidad de los trabajadores cuando éstos usen los dispositivos digitales puestos a disposición por el empleador. Señala que dos son los fines que podrían legitimar el acceso a los contenidos derivados del uso de los medios digitales: controlar el cumplimiento de las obligaciones laborales o estatutarias y garantizar la integridad de dichos dispositivos.

La Ley manda que los empleadores deben establecer, con participación de los representantes de los trabajadores, los criterios de utilización de los dispositivos digitales que se ponen a disposición de los trabajadores, debiendo respetar los estándares mínimos de protección de la intimidad de acuerdo con los usos sociales y los derechos que las leyes y la Constitución reconocen. Medida sin duda saludable y equilibrada, pues tratándose de criterios que no derivarán de una ley sino del empleador, que es una parte de la relación laboral, es preciso que intervenga, de alguna manera, la otra parte que es la que representará a los trabajadores.

El artículo 90, regula el uso de los sistemas de geolocalización en el ámbito laboral en torno al derecho a la intimidad. Deja en claro que la función de control de los trabajadores es el fin legítimo que habilitaría a los empleadores a tratar los datos de sus empleados; siempre claro, que dicha función se ejerza dentro del marco legal y los límites inherentes al mismo. Lo señalado obliga a tener particular cuidado con este sistema tecnológico que, por la naturaleza de su funcionamiento, es una forma de seguimiento del trabajador que puede permitir el acceso a mayor información de la necesaria, para que el empleador cumpla su facultad de control legítimo, pudiendo resultar intrusivo para otros derechos y la dignidad el empleado.

Merece resaltar que este mismo dispositivo normativo, establece la obligación por parte de los empleadores de cumplir con el deber de informar de forma expresa, clara e inequívoca a los trabajadores, y en su caso, a sus representantes, acerca de la existencia y las características de estos dispositivos; así como de la posibilidad del ejercicio de los derechos de acceso, rectificación y supresión del tratamiento. Sin lo señalado, se dejaría sin contenido al derecho a la protección de los datos personales.

Como condición indispensable en el contexto laboral, donde el cumplimiento de las obligaciones del trabajador abarca parte importante de su jornada y de su vida, pero que de ninguna manera puede absorberlo por completo, ni en su tiempo ni en su atención, ni tampoco disminuirle en sus derechos, o por lo menos no debería hacerlo, menos fuera del tiempo de la jornada laboral, es que España, regula como otra importante novedad, en el artículo 88 de su Ley, el derecho a la desconexión digital en el ámbito laboral. Como lo señala Moreno, citando a Sotomayor, sobre la aplicación de las Tic en el ámbito laboral

> […] produce una intrusión del trabajo a la vida privada, la confusión entre lugar y tiempo de trabajo y vida privada e intimidad del trabajador y da lugar a un incremento del poder de control del empresario mediante el uso de las TIC, en detrimento - o incluso vulneración- de los derechos a la dignidad y a la intimidad de los trabajadores. A través de las TIC (correos electrónicos, móviles o teléfonos inteligentes, tabletas, etc.) el empleador puede dar órdenes o instrucciones a los trabajadores cualquier día de la semana y del año y a cualquier hora del día y de la noche, provocando, además de la vulneración de los derechos al descanso, la aparición de importantes riesgos laborales (fatiga informática, estrés laboral...) y la invasión de la vida personal y familiar del trabajador. (Moreno 2019: 172).

La ley Española señala que el derecho de los trabajadores a la desconexión digital tiene como fin garantizar fuera del tiempo de trabajo el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.
Las modalidades del ejercicio de este derecho deberán tener en cuenta la naturaleza y objeto de la relación laboral y potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar. Si ponemos de ejemplo el sistema de geolocalización instalado en el móvil del trabajador, sin desactivar una vez que terminó la jornada laboral, o durante una visita a una atención de salud, por medio de un permiso, etc. el empleador podría conocer aspectos de su comportamiento o de su vida privada o social a la que no tiene derecho y a lo que no está legitimado en virtud del control laboral que le corresponde.

Asimismo, la ley española manda al empleador que elabore una política interna en la que se defina las modalidades de ejercicio del derecho a la desconexión digital; así como las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. Esta política debe ser elaborada por el empleador, pero previa audiencia de los representantes de los trabajadores.

Los trabajadores no tienen por qué conocer el funcionamiento técnico de los dispositivos digitales que el empleador pone a su disposición para el cumplimiento de sus funciones; tampoco conocer los alcances ni capacidades ni los resguardos frente a los mismos; es el empleador quien es el primer y principal responsable de la formación y sensibilización para un uso razonable de estos dispositivos que, siendo de su propiedad los entrega a sus trabajadores para que cumplan sus obligaciones laborales, que permitan el logro de los fines de la relación laboral y, en lo que corresponda, los fines empresariales legítimos.

La introducción de las nuevas Tic en el contexto laboral, en términos de infraestructura, aplicaciones y dispositivos inteligentes, permite nuevos tipos de tratamiento de datos sistemáticos y potencialmente intrusivos. Permiten acceso a mayor cantidad de datos y a procesarlos o tratarlos de diversas maneras, que combinados entre sí, y con datos provenientes de otras fuentes como las redes sociales, internet, etc., pueden desarrollar un perfil de la persona del trabajador, pero no solo como tal, sino un perfil que comprenda diversos aspectos de su vida íntima, personal y familiar, e inclusive social, que es parte de su libre desarrollo de la personalidad; pero a la que no alcanza, ni está legitimado el empleador, con su facultad de control.

## **Capítulo 2**: **El control laboral por medio del GPS y su impacto en el tratamiento de los datos personales**

La evolución tecnológica y la globalización han planteado nuevos retos para los derechos y la dignidad de las personas, frente al objetivo de alcanzar un debido tratamiento de la información personal en cualquier contexto donde éste se realice, sea en el ámbito público como en el privado, se trate de una gran empresa como de una pequeña empresa, nos encontremos en internet como fuera de él; ya el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo [130] (RGPD) en su considerando 6, lo señala:

> La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

Así como en muchos ámbitos, el de la relación laboral, ha sido significativamente afectado y modificado por el uso de las Tecnologías de la información y comunicación (Tic) en el ejercicio del poder de dirección del empresario y de su correlativa facultad de control, supervisión o vigilancia.

Las empresas suelen buscar implementar una política de innovación tecnológica con

[130] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

diferentes objetivos como, mejorar la organización, aumentar la productividad y reducir costos. Los procesos de tecnificación se están introduciendo en todos los aspectos de la vida de una empresa, lo que incluye y tiene particularidades, necesarias de atender, cuando se trata del control laboral con el fin de verificar el cumplimiento adecuado de la prestación del trabajo a cargo del trabajador.

Esta situación genera un reforzamiento del poder de control del empleador sobre las tareas e incluso sobre la persona del trabajador. Como lo señalan Fernández y Rodríguez-Rico

> […] junto a las técnicas de reproducción de la imagen y el sonido, de monitorización de ordenadores, o de supervisión de conexión a internet y correspondencia electrónica mediante la instalación de programas espía, emergen otras nuevas como las propias de geolocalización (el sistema de posicionamiento global o GPS permite conocer la situación exacta de los usuarios a través de satélites) o de control biométrico de los trabajadores. El avance tecnológico permite, por tanto, que el control empresarial gane en cantidad y en calidad, pues habilita un mayor número de instrumentos capaces de fiscalizar más aspectos de los controlables mediante la vigilancia tradicional, siendo además más precisos y detallados, al tiempo que abren un gran número de posibilidades de almacenamiento y de reproducción (2016: I.47).

Esta situación hace más sutiles los límites entre la vida privada y la vida laboral del trabajador (De Vicente 2005:19), lo que muchas veces lo lleva a estar constantemente vigilado, controlado, frente a un poder de control empresarial que tiene hoy ya múltiples manifestaciones o modalidades para realizar su vigilancia por medio de distintos instrumentos, herramientas, horarios, lugares y modalidades. Esto es el origen de conflictos que requieren ser solucionados y encontrar un equilibrio entre los distintos intereses o derechos en juego, tanto por el lado del empresario o empleador, como por el lado del trabajador.

Para el desarrollo de sus actividades empresariales y en específico para el mantenimiento de las relaciones laborales, el empresario trata diversos datos personales de sus trabajadores: recoge, almacena, organiza, transfiere, graba,

suprime, etc. diversa información concerniente a su personal; información necesaria para el mantenimiento de la relación laboral, para la planificación y organización del trabajo, o para cumplir con obligaciones legales en virtud de normas tributarias, sobre pensiones, sobre régimen del sistema nacional de salud, entre otras.

No obstante, no siempre el empleador trata solo los datos personales que son necesarios para los objetivos señalados, pues las herramientas tecnológicas que utiliza tienen la capacidad de captar más información que la estrictamente necesaria; por lo que ámbitos extra laborales propios de la esfera personal del trabajador se pueden ver afectados e invadidos por el laboral, poniéndose en riesgo la intimidad y el debido tratamiento de los datos personales, generándose muchos interrogantes y conflictos jurídicos que es menester atender.

En el Perú no ha existido una norma específica sobre protección de datos personales aplicables al ámbito laboral y menos que regule el tratamiento de los datos personales de los trabajadores sometidos al control empresarial; por lo que se hace necesario conocer en qué medida la legislación, y la jurisprudencia han atendido esta situación de desequilibrio entre el derecho de los trabajadores a la protección de sus datos personales[131] y la facultad de control del empresario, quien usa para el ejercicio de dicha potestad de las Tic; dentro de las cuales merecerá particular atención el del Sistema de Posicionamiento Global, GPS.

### 2.1. La libertad de empresa y el poder de dirección empresarial

Analizar el derecho a la libertad de empresa nos brindará criterios que favorezcan a la comprensión e interpretación de la pugna que existe, dentro de la organización empresarial, a nivel de la relación laboral entre los derechos de los trabajadores y los poderes del empresario.

La libertad de empresa está consagrada en el artículo 59 de la Constitución Política de 1993: “Artículo 59. El Estado estimula la creación de riqueza y garantiza

[131] Y por su naturaleza relacional puede implicar la violación de otros derechos.

la libertad de trabajo y la libertad de empresa, comercio e industria. El ejercicio de estas libertades no debe ser lesivo a la moral, ni a la salud, ni a la seguridad públicas. El Estado brinda oportunidades de superación a los sectores que sufren cualquier desigualdad; en tal sentido, promueve las pequeñas empresas en todas sus modalidades."

Nuestro máximo intérprete constitucional, el Tribunal Constitucional, ha definido a la libertad de empresa y señalado sus limitaciones básicas de la siguiente manera:

> […] la facultad de poder elegir la organización y efectuar el desarrollo de una unidad de producción de bienes o prestación de servicios, para satisfacer la demanda de los consumidores o usuarios. Tiene como marco una actuación económica autodeterminativa, lo cual implica que el modelo económico social de mercado es el fundamento de su actuación y, simultáneamente, el que impone los límites de su accionar. Consecuentemente, dicha libertad debe ser ejercida con sujeción a la Constitución y la ley —siendo sus limitaciones básicas aquellas que derivan del interés público, el bien común, la seguridad, la higiene, la moralidad o la preservación del medio ambiente—, y su ejercicio debe respetar los diversos derechos de carácter socio-económico que la Constitución reconoce[132]

La libertad de empresa comprende un derecho de autodeterminación frente al Estado, al mercado y a sus componentes. Por eso, comporta una serie de libertades que forman parte de su contenido especialmente protegido:

a) La libertad de creación de empresa y acceso al Mercado. Lo que supone la libertad para emprender actividades económicas, en el sentido de libre fundación de empresas y concurrencia al Mercado.
b) La libertad de organización. Contiene la libre elección: del objeto, nombre, domicilio, tipo de empresa; de las facultades a los administradores, políticas de precios, créditos y seguros, contratación de personal y política publicitaria, entre otros.
c) La libertad de competencia; y

[132] EXP. N.° 003-2006-AI/TC. Fundamento 62. Ver también otros expedientes tales como: EXP. N.° 7339-2006-AA/TC. EXP. N.° 3455-2014-AA/TC.

d) La libertad de disponer el cierre o cesación de las actividades de la misma cuando se considere oportuno.[133]

Al ser estas cuatro libertades parte del contenido esencial de la libertad de empresa estamos frente a lo que hace reconocible este derecho; es decir facultades que permitirán a su titular satisfacer los intereses para cuya obtención el derecho se otorga y que deberán ser respetados tanto por el Estado como por la colectividad. (García 2016: 34).

Como se desprende del contenido esencial del derecho a la libertad de empresa, como derecho fundamental, y específicamente lo que el Tribunal Constitucional denomina como libertad de organización, está la libertad de establecer los objetivos de la empresa que decida crear; dirigir y planear su actividad en atención a sus recursos y a las condiciones del mercado[134], contratar al personal y la política de personal en general; para cumplir los fines empresariales que comprenden los de producción.

La libertad de empresa comprende entonces no solo la facultad de crear una empresa sino de organizarla y dirigirla, lo que sirve de base jurídica para el poder de dirección que le corresponde al empresario, y que se debe complementar con su poder de controlar el cumplimiento de las directrices u órdenes que emita para la ejecución adecuada de la relación laboral; y por tanto también del poder disciplinario que le servirá de mecanismo para garantizar los fines empresariales establecidos. Así, "el poder disciplinario y el directivo constituyen dos caras de una misma moneda, dos medios para defender el interés del empresario" (Poquet 2013:20).

Es pertinente hacer referencia al derecho a la propiedad reconocido constitucionalmente por los artículos 2, inciso 16) y el 70. Derecho que tiene dentro de sus características el de ser uno pleno, que le confiere a su titular amplias atribuciones (usar, disfrutar, disponer y reivindicar) que puede ejercer dentro de las limitaciones que establece el ordenamiento jurídico y los derechos de terceros; lo que

[133] EXP. N.° 003-2006-AI/TC. Fundamento 63.
[134] STC Español 225/1993, de 8 de julio.

incluye el derecho a defender la propiedad contra todo acto que tenga efectos de privación en la integridad de los bienes protegidos.[135] En este orden de ideas, Barría (2009: 9) [136] señala:

> Además del principio constitucional antes mencionado[137], el poder de dirección se fundamenta en el principio-derecho constitucional de propiedad, al ser el empresario el dueño de los recursos productivos y de las herramientas que pone al servicio de la consecución de sus fines empresariales. Como propietario de los medios de producción en su empresa, el empleador necesita tener un cierto control sobre el uso que se hace de ellos, razón por la cual el legislador le concede tal facultad, e incluso consagra ciertos medios para llevar a cabo el control referido.

En consecuencia el derecho a la libertad de empresa junto con el derecho a la propiedad constituyen la base constitucional del poder de dirección del empresario. Poder que nace a partir de la existencia del contrato de trabajo; si como señala Montoya (1965: 38) entendemos que el contrato de trabajo es un presupuesto jurídico para su ejercicio.

### 2.1.1. Poder de dirección y facultad de control laboral

La configuración legal del poder de dirección del empresario está recogida en el Texto Único Ordenado del Decreto Legislativo Nº 728, Ley de Productividad y Competitividad Laboral, artículo 9: “Por la subordinación, el trabajador presta sus servicios bajo dirección de su empleador, el cual tiene facultades para normar reglamentariamente las labores, dictar las órdenes necesarias para la ejecución de las mismas, y sancionar disciplinariamente, dentro de los límites de la razonabilidad, cualquier infracción o incumplimiento de las obligaciones a cargo del trabajador.”.
Del texto citado, así como de varios pronunciamientos del Tribunal Constitucional se desprende que el poder de dirección comprende la facultad de dirigir, fiscalizar y

[135] EXP. N.º 3455-2014-AA/TC. Fundamento 5.

[136] Consultado al 20 de enero de 2021en: http://repositorio.uchile.cl/bitstream/handle/2250/106908/de-barria_d.pdf?sequence=3&isAllowed=y

[137] Aludiendo la autora a la libertad de empresa.

sancionar al trabajador[138]. Este poder está conformado por una serie o conjunto de facultades que le permitirán al empresario garantizar la satisfacción del legítimo interés propio de su organización empresarial. Dentro de las facultades que conforman el poder de dirección, siguiendo a De Vicente (2005: 23-24) y a Poquet (2013: 31-32) pueden mencionarse las siguientes:

a) Dictar instrucciones generales sobre la organización y el funcionamiento de la empresa y sobre la prestación laboral en ésta.
b) Dictar órdenes e instrucciones particulares a los trabajadores sobre el contenido y las circunstancias del trabajo.
c) Vigilar y controlar para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.
d) Disciplinaria como consecuencia de la comprobación de incumplimientos laborales del trabador que habilitan a la imposición de las sanciones correspondientes.

La facultad disciplinaria, no es incluida por la totalidad de la doctrina dentro del poder de dirección, (Poquet 2013: 32), al considerarla una autónoma pero ligada íntimamente el poder de dirección con carácter complementario. No obstante, otro importante sector de la doctrina, así como se desprende de la legislación peruana y por reiterados pronunciamientos del Tribunal Constitucional peruano, la facultad disciplinaria es propia del poder de dirección "Como se observa, dentro de este poder de dirección encontramos la potestad disciplinaria del empleador para sancionar cualquier infracción o incumplimiento de obligaciones laborales del trabajador. Se advierte, además, que dicha potestad disciplinaria emana de la subordinación a la que está sometido el trabajador frente a su empleador, es decir, no se podría sancionar a una persona que no está subordinada laboralmente a un empleador." [139]

[138] EXP. N.° 1112-2012-AA/TC. Fundamento 7. EXP. N.º 3001-2014-AA/TC. Fundamento 2. EXP. N.º 4539-2012-AA/TC. Fundamento 28.

[139] EXP. N.° 3001-2014-PA/TC. Fundamento 2. EXP. N.° 1112-2012-AA/TC. . EXP. N.° 4539-2012-AA/TC.

El poder Directivo es la manifestación más clara de uno de los elementos esenciales y distintivos del contrato de trabajo, que es la subordinación a que está sometido el trabajador. La subordinación o dependencia del trabajador, como lo señala Poquet (3013: 28) viene a ser comprendida como la otra cara de la moneda del poder de dirección del empleador, en la medida que no puede ser entendido uno sin el otro.

La dependencia o subordinación propia de la relación laboral tiene expresión en un doble aspecto, o puede señalarse que son dos elementos los que la componen (De la Cueva citado por Blancas 2007: 97) "[…] una facultad jurídica del patrono en virtud de la cual puede dictar los lineamientos, instrucciones u órdenes que juzgue conveniente para la obtención de los fines de la empresa, y una obligación igualmente jurídica del trabajador de cumplir esas disposiciones en la prestación de su trabajo".

El trabajador tiene una posición muy débil desde que se incorpora a una organización previamente diseñada por el empleador y donde sus funciones están ya fijadas o pueden irse acomodando, según corresponda, por voluntad del empleador y en el marco de la relación laboral generada por el contrato de trabajo; el mismo que opera como frontera fundamental tanto para el ejercicio del poder del empresario como de la subordinación del trabajador.
Para que el poder de dirección sea efectivo y real es que está intrínsecamente unido a la facultad de fiscalización, de vigilancia o control; de la que puede derivarse el ejercicio del poder disciplinario cuando corresponda y con las debidas garantías del caso. La facultad de fiscalizar se denomina también como facultad de control reconocida así tanto a nivel doctrinario como en la legislación interna.[140] Por lo que utilizaremos dichas denominaciones indistintamente.

En efecto, si en virtud al poder de dirección el empleador puede y debe dictar instrucciones y órdenes, por lo mismo, debe poder verificar el cumplimiento correcto de las mismas. Pero este poder de fiscalización, vigilancia o control va más allá de lo específicamente ordenado dirigiéndose al conjunto de la prestación laboral. García

[140] CAS. N.º 14614-2016 LIMA. Considerando Décimo quinto. Publicada en el Diario oficial El Peruano el martes 30 de mayo de 2017.

Ninet lo señala en el sentido de que es “algo más amplio que el mero verificar si se ejecutan o no cada una de las ordenes o instituciones cursadas. Se trata de controlar el cumplimiento total de las obligaciones, o mejor de la prestación de trabajo de todos y cada uno de los trabajadores en todas y cada una de sus fases de ejecución¨ (1981: 164) ; o tal como lo pone de relieve Goñi “la actividad de vigilancia alimenta una idea que se sustenta en una mayor y más constante atención a la ejecución de la prestación, y en el fortalecimiento de los elementos comunes de vigilancia contrastables en cualquier relación contractual, lo que hace sin duda el poder de control empresarial una facultad mucha más intensa , penetrante, continua y minuciosa” (1998: 110-111).

Si a esto le sumamos la incorporación de los elementos tecnológicos que vienen a reforzar, a multiplicar y a potenciar la facultad de control empresarial, sin que la legislación haya adoptado una posición al respecto, la asimetría que por naturaleza existe en la relación laboral, en desventaja del trabajador, se acentúa y eso puede generar efectos negativos en la persona el trabajador y en su actitud hacia su compromiso con la empresa de cumplir adecuadamente sus obligaciones laborales, como pieza importante en el logro de los objetivos empresariales; a cuya consecución justamente está dirigida, en última instancia, la potestad de fiscalización.

Las nuevas tecnologías vienen reforzando el “ojo electrónico” del empleador haciéndolo “penetrante, dominante y ubicuo” como lo expresa Rodríguez:

> La tecnificación e informatización de la empresa, como instrumento de vigilancia, conceden al empresario – por vía directa o indirecta- una “fuerza de choque” superior a la derivada de su poder tradicional de dirección o disciplinario e introducen un elemento nuevo en el sinalagma contractual capaz de provocar la ruptura en el necesario equilibrio de intereses […] si en el pasado el control aparecía centrado en los resultados del trabajo, en la actualidad es la propia ejecución y el cumplimiento de los operarios los que a él quedan sometidos en el afán de favorecer una mayor exigencia empresarial y un mayor rendimiento […]. Es preciso destacar, en este contexto, el doble control producido en el interior de la

> empresa dotada de avances tecnológicos: de un lado, el clásico, jerárquico o vertical, acentuando la omnipresencia de los superiores; de otro, el control horizontal, pues los datos son utilizados en distintos departamentos de la empresa simultáneamente, con la consiguiente pérdida tanto en la delimitación de la intimidad en el propio puesto como del "espíritu de cuerpo", que llevaba - no obstante posibles desavenencias internas- a la tradicional cooperación y dependencia entre quienes formaban parte de una sección o departamento. Con las innovaciones técnicas y la integración de sistemas informatizados "son otros, extraños a la sección o al departamento, los que pueden juzgar ahora el rendimiento (2006: 86-88).

En efecto, el uso de las nuevas tecnologías para ejercer la facultad de control, permiten recoger y tratar datos personales de los trabajadores, por distintas áreas de la empresa tanto, la que corresponde a los encargados de la parte técnica o tecnológica, como de los directivos o jefes de áreas, quienes en virtud a los datos recogidos pueden verificar el cumplimiento de los deberes laborales, en el mejor de los casos; así como también, y, dependiendo de la tecnología utilizada, asomarse y entrar en el conocimiento de aspectos de la vida extra laboral del trabajador, abarcando información relacionada con su intimidad personal o familiar, así como otros ámbitos a los que el empleador no está legitimado para conocer en su calidad de tal.

El tratamiento bastante general que hace la Ley de Productividad y Competitividad Laboral sobre el poder de dirección puede entenderse en un sentido positivo, si consideramos que permitirá adecuarse a situaciones nuevas como la introducción de los avances tecnológicos dentro de la empresa; pero por otro lado, la interpretación podría ser negativa ante la inexistencia de regulación específica del tema, y la inexistencia de límites necesarios en atención a los intereses legítimos en juego: el empresarial y los derechos y la dignidad del trabajador.

Surgen interrogantes, sobre el nivel de discrecionalidad del que puede hacer uso el empleador, por ejemplo, a la hora de elegir un determinado sistema o particular medida técnica de vigilancia o control; y en su caso, hasta dónde puede llegar de

manera legítima dentro de la relación de trabajo sin afectar a la persona del trabajador, por ley subordinado a aquél.

Será preciso complementar el ejercicio de esta amplia gama de facultades que se desprenden del poder de dirección del empleador, con otras normas, que están fuera del ámbito laboral, como la Ley N° 29733, Ley de Protección de Datos Personales.

Sobre lo señalado, ya el Grupo de trabajo del Artículo 29[141], en lo sucesivo GT29, ponía en relevancia en su Dictamen sobre el tratamiento de datos personales en el contexto laboral 8/2001, la interacción existente entre la legislación laboral y la legislación sobre protección de datos personales. En efecto, la legislación sobre protección de datos no se aplica de forma independiente del derecho del trabajo y las prácticas laborales; y éstos, a su vez, no pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos. Esta interacción es necesaria y valiosa y debería contribuir al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores.

#### 2.1.1.1. Límites

Hemos visto que los dos principales fundamentos del poder de dirección del empleador son la libertad empresarial y el derecho a la propiedad, reconocidos por el texto constitucional de 1993.

De igual manera el principal y explícito límite al poder de dirección y a su correspondiente facultad de control empresarial está claramente reconocido por la Constitución Política, que señala en su Artículo 23: "[…] Ninguna relación laboral puede limitar el ejercicio de los derechos constitucionales, ni desconocer o rebajar la dignidad del trabajador […]".

Disposición del más alto nivel del ordenamiento jurídico que tiene por fin proteger la

[141]El Grupo de Trabajo del Articulo 29 era el órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46(CE, en la actualidad ha sido sustituido por el Comité Europeo de Protección de Datos.

dignidad y los derechos de los trabajadores, y que si bien, es clara su relevancia al estar en la norma fundamental del Estado, no ha sido objeto de mayor desarrollo; no obstante, no por ello la empresa puede constituirse en un espacio de inobservancia del cumplimiento de lo que en buena cuenta ilumina todo el ordenamiento jurídico: la defensa y el respeto de la dignidad de la persona.

> […] en cuanto el valor central de la persona impone que sus derechos fundamentales proyecten también su efecto regulador al ámbito de la sociedad y de la propia autonomía privada. La dignidad de la persona trae así consigo la proyección universal, frente a todo tipo de destinatario, de los derechos fundamentales, de modo que no hay ámbito social que se exima de su efecto normativo y regulador, pues de haber alguno, por excepcional que fuese, significaría negar el valor normativo del mismo principio de dignidad. En consecuencia, los derechos fundamentales vinculan, detentan fuerza regulatoria en las relaciones jurídicas de derecho privado, lo cual implica que las normas estatutarias de las entidades privadas y los actos de sus órganos deben guardar plena conformidad con la Constitución y, en particular, con los derechos fundamentales" (sentencia emitida en el Expediente 06730-2006-PA/TC, fundamento 9). [142]

La jurisprudencia, a nivel del Tribunal Constitucional, ha recurrido al precepto constitucional mencionado, en los contados casos, que han llegado ante dicha instancia, conflictos sobre el ejercicio de la facultad de control y/o del poder disciplinario; específicamente relacionados con el uso del correo electrónico corporativo o programas de mensajería instantánea proporcionados por el empleador.[143] La amplia mayoría de estos pronunciamientos han utilizado como base lo desarrollado en la sentencia recaída en el expediente N° 01058-2004/AA, y lo ha ratificado como colegiado[144]. De dicha sentencia podemos extraer los siguientes criterios importantes relacionados con límites a la facultad de control[145]:

---

[142] EXP. No 01413-2017-AA/TC. Fundamento 6.
[143] EXP. N.º 3001-2014-PA/TC. EXP. N.º 4539-2012-AA/TC. EXP. N.º 0114-2011-PA/TC. EXP. N.º 1058-2004-AA/TC.
[144] Aunque en algunos votos singulares se hayan alejado de algunos de sus fundamentos específicamente relacionados con lo que en doctrina se denomina “expectativa de privacidad” como es el caso de los votos singulares de los Magistrados Álvarez Miranda y Urviola Hani en la sentencia recaída en el EXP. N.° 3599-2010-AA/TC.
[145] EXP. N.º 1058-2004-AA/TC Fundamentos 19 y 20.

-En el marco de la relación laboral el trabajador no deja de ser titular de los atributos y libertades que como persona la Constitución le reconoce. Por lo que resulta inobjetable que la relación de trabajo debe respetar el contenido esencial de los derechos de los trabajadores.

-El empleador no solo puede, sino que debe hacer uso de su poder fiscalizador e, incluso, disciplinario. La forma de determinar la validez, o no, de una medida de fiscalización o disciplinaria es respetar las limitaciones establecidas por la Constitución y, a su vez, implementar mecanismos razonables que permitan, sin distorsionar el contenido de los derechos involucrados, cumplir los objetivos laborales a los que se encuentran comprometidos los trabajadores y las entidades empleadoras a las que pertenecen.

Por lo que se debe entender que el empleador no carece de medios adecuados para controlar la labor del trabajador y la eficiencia de las responsabilidades que se le encomienden a éste; sino que la implementación de tales medios no puede hacerse de manera arbitraria en contra de los derechos de la persona, sino de manera razonable, de modo que se permita satisfacer los fines de toda relación laboral sin perjudicar los ámbitos propios de autodeterminación que en todo momento deben estar sujetos a lo establecido en la Constitución.[146]

La razonabilidad, prescrita como actuación razonable, por el artículo 9 de la Ley de Productividad y Competitividad Laboral; y utilizada por el Tribunal Constitucional, aparece como un límite o prohibición a la actuación arbitraria del empleador; nuestro más alto intérprete de la Constitución define este principio señalando que:

> Por virtud del principio de razonabilidad se exige que la medida restrictiva se justifique en la necesidad de preservar, proteger o promover un fin constitucionalmente valioso. Es la protección de fines constitucionalmente relevantes la que, en efecto, justifica una

[146] EXP. N.º 1058-2004-AA/TC Fundamento 23.

> intervención estatal en el seno de los derechos fundamentales. Desde esta perspectiva, la restricción de un derecho fundamental satisface el principio de razonabilidad cada vez que ésta persigue garantizar un fin legítimo y, además, de rango constitucional.[147]

Es cierto que en la relación laboral los derechos de los trabajadores también pueden en determinas circunstancias ser modulados en atención a la condición de trabajador, en condición de subordinación, que es parte de una organización con determinados fines; los cuales vinculan tanto al trabajador como al empleador, siempre y cuando ambos estén sometidos a los límites que impone el ordenamiento jurídico.

Lo señalado nos lleva a entender que hay intereses que pueden contraponerse a la hora en que el empleador fiscaliza al trabajador, y que se debe buscar una forma de satisfacer de manera ponderada tanto los intereses de la parte trabajadora como de la empleadora para que puedan alcanzarse los legítimos objetivos empresariales en un clima de respeto a los derechos de los trabajadores. Claro que esta labor le corresponde al empresario quien es el que tiene la autoridad en la relación laboral y quien determinará los medios de fiscalización a emplear. Lo que no debe perder de vista es que una decisión que transgreda los derechos fundamentales de sus trabajadores acarreará la nulidad de dicha medida.

Para esta tarea, cobra importancia la aplicación de la técnica jurídica del principio de proporcionalidad, que será de particular pertinencia cuando el empleador ejerza su potestad de control a través de mecanismos que puedan afectar los derechos fundamentales del trabajador.

De otro lado, la Corte Suprema, en una sentencia de casación N° 14613-2016 Lima,[148] señaló en su fundamento décimo quinto, dos tipos de límites a la facultad de control empresarial. Así, esta facultad encontrará límites en su ejercicio: funcional y

[147] EXP. N.° 0045-2004-AI/TC Fundamento 23.
[148] Publicada en el Diario Oficial El peruano el 30 de mayo de 2017. Citando a su vez a Samuel Oswaldo M. “Derechos y obligaciones en el contrato de trabajo”.

racional. El límite funcional está relacionado al contexto empresarial, por lo que el empleador no puede controlar la esfera privada del trabajador; y en cuanto al límite racional, parte de la idea de que el control debe ser resultado de un proceso intelectual que lo justifique y que dé razón al proceso de toma de decisiones.

Con lo señalado, se ratifica que el empleador cuando ejerce su facultad de control, no podrá invadir esferas de la vida del trabajador que excedan a su condición de tal y; que sus decisiones para la conducción, ejecución y mantenimiento de la relación laboral, no pueden ser arbitrarias.

Existen dos elementos generales necesarios de considerar cuando del ejercicio de la facultad de control empresarial se trata: el respeto a los derechos fundamentales y dignidad de los trabajadores; y el test de proporcionalidad; especialmente si el empleador recurre a la tecnología como instrumento de vigilancia o fiscalización; lo que deberá garantizar la racionalidad en el ejercicio funcional de la potestad empresarial.

#### 2.1.1.2. El derecho a la protección de datos personales como derecho laboral inespecífico

Los derechos fundamentales de la persona están reconocidos por la norma fundamental de un Estado y deben ser garantizados[149]; y por ende respetados por él (eficacia vertical de los derechos fundamentales); pero también deben ser respetados y, por lo tanto, ser oponibles frente a los particulares (eficacia horizontal de los derechos fundamentales); como en el contexto de la relación laboral entre el empleador y el trabajador.

Esto constituye un deber impuesto por la Constitución "Artículo 38. Todos los peruanos tienen el deber de honrar al Perú y de proteger los intereses nacionales, así como de respetar, cumplir y defender la Constitución y el ordenamiento jurídico de la Nación.";

[149] Su garantía constituye uno de los deberes primordiales para el Estado. Artículo 44 de la Constitución Política de 1993.

pero también, el respeto a los derechos humanos constituye un deber de nuestra civilización; más aún si nos encontramos en un Estado Constitucional de Derecho.[150]

Los derechos fundamentales son atribuibles a la persona en base a su dignidad, por lo que su titularidad es de la persona, en su condición de tal, independientemente de cualquier otra consideración.
En el ámbito laboral, la doctrina suele clasificar en dos los derechos fundamentales cuya titularidad le corresponden al trabajador: derechos fundamentales específicos del trabajador; y derechos fundamentales inespecíficos del trabajador.

Los derechos fundamentales específicos del trabajador o derechos fundamentales laborales, son aquéllos que le corresponden al trabajador en su calidad de tal y se ejercen dentro del ámbito de las relaciones laborales; dentro de ellos podemos mencionar los constitucionalmente reconocidos: derechos de sindicación, negociación colectiva y huelga (artículo 28); los derechos a una jornada ordinaria de trabajo; al descanso semanal y anual remunerados (artículo 25); etc.

Pero como sabemos los derechos fundamentales son atributos inherentes a la persona en su calidad de tal y no por ser parte de una organización o corporación; por lo que hay muchos derechos que no tienen un contenido exclusivamente laboral pero que se ponen de manifiesto y tienen importantes repercusiones en este ámbito. Estos son los derechos fundamentales inespecíficos del trabajador. Palomeque señalará que, además de los derechos laborales o específicos del trabajador están los:

> […] otros derechos constitucionales de carácter general y, por ello, no específicamente

[150] EXP. 01413-2017-AA/TC. Fundamento 5.“En principio, cabe recordar que "[...] el Estado social y democrático de Derecho implica que los derechos fundamentales adquieren plena eficacia vertical —frente a los poderes del Estado- y horizontal —frente a los particulares-. Ello excluye la posibilidad de que existan actos de los poderes públicos y privados que estén desvinculados de la eficacia jurídica de los derechos fundamentales, toda vez que éstos no sólo son derechos subjetivos de las personas sino también instituciones objetivas que concretizan determinados valores constitucionales —justicia, igualdad, pluralismo, democracia, entre otros- recogidos, ya sea de manera tácita o expresa, en nuestro ordenamiento constitucional" (Cfr. sentencia emitida en el Expediente 10087-2005-PA/TC, fundamento 3).”

> laborales pueden ser ejercitados, sin embargo, por los sujetos de las relaciones de trabajo (los trabajadores en particular) en el ámbito de las mismas, por lo que en tal caso adquieren un contenido o dimensión laborales sobrevenidos. Se produce así una "impregnación laboral" de derechos de titularidad general o inespecífica por el hecho de su utilización por trabajadores asalariados a propósito y en el ámbito de un contrato de trabajo. […] se trata por ello, de derechos que, no obstante de ser atribuidos a las personas con carácter general, […] son ejercitados en el seno de una relación jurídica laboral por ciudadanos que, al propio tiempo, son trabajadores y, por lo tanto, se convierten en verdaderos derechos laborales por razón de los sujetos y de la naturaleza de la relación jurídica en que se hacen valer, en derechos constitucionales inespecíficos (1991: 31-32).

Dentro de los derechos fundamentales inespecíficos del trabajador podemos mencionar los derechos a: la intimidad; al honor; a la propia imagen; a la libertad de expresión; a la libertad religiosa; a la libertad ideológica; a la igualdad; a la inviolabilidad y al secreto de las comunicaciones, y al derecho a la protección de datos personales.

Como lo señalan Hernández y Zamudio:

> Es necesario que en el seno de la relación laboral se consideren ciertos derechos fundamentales, denominados de la libertad, no específicamente laborales para contrarrestar el poder económico y social del empleador, expresado en sus facultades como tal, sin que esa función se agote en la eficacia ante éste de los derechos fundamentales específicamente laborales; se trata de los derechos que siendo atribuidos a las personas con carácter general, son ejercidos en el seno de la relación laboral por sujetos que son trabajadores, pero que se requiere para que el empleador no ejercite un poder omnímodo y hagan de la empresa una isla al margen de los derechos y la dignidad del trabajador, lo cual es inadmisible en un Estado de Derecho (2019: p. 39).

El derecho a la protección de datos personales, como derecho laboral inespecífico del trabajador, como derecho fundamental autónomo de la persona, se instituye como un límite preciso y acorde en el contexto de la sociedad de la información y del

conocimiento, que tiene como una de sus características el uso creciente de los avances tecnológicos y de internet, como herramientas y plataformas usadas cada día de manera más intensa para el ejercicio de la facultad de control empresarial.

Son muchos los datos personales que el empleador recaba por parte de sus trabajadores por medio de: las computadoras; del correo electrónico; del internet; la mensajería instantánea laboral; del celular corporativo, cámaras de videovigilancia con o sin fines explícitos de control laboral; los sistemas de geolocalización colocados en los celulares, en los vehículos, laptop o tabletas digitales puestos a disposición por el empleador; sistemas de fichaje o biométricos de control horario; entre otros, cada día más potenciados.

Abundante información que el empleador recaba sobre sus trabajadores que puede ser usada no solo para el fin legítimo de vigilancia laboral; sino de manera indebida para perfilar a su personal, para conocer aspectos para los que no está habilitado y con fines extra laborales o incompatibles con su poder de dirección.

Pero los trabajadores ¿son conscientes de esta situación?; por lo menos saben que su información personal, ¿está en poder de otro u otros?; conocen ¿Qué actividades de tratamiento se realizan con sus datos personales?, ¿Por cuánto tiempo?, ¿Con qué medidas de seguridad? , ¿Para qué finalidades?, ¿Cuál es el plazo de conservación de los mismos? ¿A quiénes han sido cedidos? ¿Cuáles son los límites para el uso de su información personal en la relación laboral?, etc.

Son preguntas legítimas del titular del dato personal y que responden al objetivo de no perder el control sobre la información que le concierne, lo que es parte del contenido esencial del derecho a la protección de datos personales de los trabajadores; quienes, si bien en cierto, en virtud del contrato de trabajo deben estar sometidos a un control laboral, dicho control se ve potenciado por el uso de la tecnología. Lo acabado de señalar, hace que la subordinación, a la que está sometido el trabajador frente al empleador, se acentúe muchas a veces de manera indebida cuando este realiza un tratamiento de los datos personales de sus trabajadores, al

margen de la legislación sobre la materia.

En Perú no hay un tratamiento legislativo sobre los derechos fundamentales inespecíficos del trabajador; lo cual frente al avance e incorporación de las nuevas tecnologías en las relaciones laborales se hace preciso atender; siguiendo a Toscani y Valenciano (2016:13-14); se hace necesario una atención legislativa que dote de contenido y efectividad a estos derechos y limite de manera objetiva los poderes de vigilancia y control empresarial.

En el caso de la legislación sobre la materia de protección de datos personales en el Perú, no hay un desarrollo del tratamiento de datos en el ámbito laboral, por lo que se debe recurrir a la legislación general sobre la materia para ayudar a mitigar el impacto negativo que puede suponer el uso de la tecnología en el control laboral.

#### 2.1.1.3. El principio de proporcionalidad

Los derechos fundamentales no son absolutos, ni responden a una jerarquía entre ellos que permita justificar el sacrificar unos sobre otros. Los derechos coexisten y se espera el mayor grado de satisfacción en su ejercicio para cada uno. No obstante, en el ámbito laboral, pueden darse circunstancias en las que algunos puedan entrar en conflicto; como el derecho a la libertad de empresa, del empleador, y alguno de los derechos fundamentales del trabajador, como podrían ser los derechos a la protección de datos personales, a la intimidad, o al libre desarrollo de la personalidad, entre otros. Como lo manifiesta García (2016: 51) en la relación laboral, los derechos de una de las partes no pueden menoscabar de forma indebida los derechos de la otra parte. El empresario no puede ampararse en la libertad de empresa para volver ilusorios los derechos de los trabajadores; pero por otro lado, tampoco los derechos fundamentales de los trabajadores pueden implicar una modificación unilateral de las obligaciones asumidas mediante el contrato de trabajo.

Cuando el empleador ejerce su potestad de control debe buscar implementar mecanismos razonables que le permitan, sin distorsionar los derechos involucrados de

los trabajadores, cumplir los objetivos laborales a los que se encuentran comprometidos ambas partes por el contrato de trabajo. En general, no quedará violado un derecho fundamental porque se impongan a su titular limitaciones como consecuencia de deberes y relaciones jurídicas que el ordenamiento regula[151]; en esta línea; la eventual limitación del derecho será constitucionalmente legítima, siempre que se encuentre suficientemente justificada en la tutela de otros intereses y bienes jurídicos de relevancia constitucional; sin que se exijan sacrificios desproporcionados a la finalidad perseguida.[152]

Como lo expresa el Tribunal Constitucional Español: [153] "la efectividad de los derechos fundamentales del trabajador en el ámbito de las relaciones laborales debe ser compatible, por tanto, con el cuadro de límites recíprocos que pueden surgir entre aquellos y las facultades empresariales, las cuales son también expresión de derechos constitucionales reconocidos". Se necesita que se actúe con equilibrio.

Para que el equilibrio caracterice una decisión empresarial que afecte un derecho del trabajador, como cuando elige una herramienta de control laboral y la forma o procedimiento en que la usará, será preciso que el empleador recurra al principio de proporcionalidad; "la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad"[154]. Herramienta de la que los tribunales constitucionales[155], como el nuestro, hacen uso para evaluar la constitucionalidad de una medida restrictiva de derechos. [156]

En la estructura del principio de proporcionalidad se encuentran tres subprincipios, los mismos que deben ser aplicados de forma sucesiva, de tal manera que no será

[151] España: STC 170/1987, de 30 de octubre.
[152] España: STC 142/1993, de 22 de abril.
[153] España: STC 151/2004, de 20 de septiembre.
[154] España: STC 98/2000, de 10 de abril.
[155]Es más, en la sentencia recaída en el expediente EXP. 01413-2017-AA/TC., en el voto singular, fundamento 14, del Magistrado Calle Hayen, se señala que el empleador " podrá aplicar las medidas correctivas del caso siguiendo los principios constitucionales de pro hominem, in dubio pro operario, derecho al debido proceso, racionalidad y proporcionalidad establecidos por el Tribunal Constitucional.
[156] EXP. 01413-2017-AA/TC. Fundamento 14.

necesario pasar a aplicar el siguiente si no se supera el que lo antecede.[157]

a) Subprincipio de idoneidad.[158] Consiste en la relación de causalidad de medio a fin. Supone dos cosas: primero, la legitimidad constitucional del objetivo; y segundo, la idoneidad de la medida utilizada para el logro del objetivo.
   Lo primero que este subprincipio exige es determinar si los fines y los medios identificados son razonables, es decir que sean legítimos y que no se encuentren prohibidos por la Constitución.[159] En lo que respecta al fin perseguido, no basta que no esté prohibido sino que sea uno constitucionalmente válido; para luego evaluar si la medida utilizada es idónea para lograr el objetivo o fin perseguido.

b) Subprincipio de necesidad. Importa el análisis de dos aspectos:
   Primero: la identificación de si hay otros medios alternativos (a la medida adoptada) que sean idóneos para la consecución del objetivo y que estén disponibles. Supone la comparación entre dos medios idóneos.
   Segundo: si tales medios idóneos revisten menor intensidad o grado de intervención o restringen menos el derecho fundamental afectado.
   En consecuencia, si del análisis resulta que existe al menos un medio disponible igualmente idóneo que es más benigno con el derecho afectado, deberá elegirse ese, para superar el test de necesidad.[160]

c) Subprincipio de proporcionalidad en sentido estricto. Consistirá en una comparación entre el grado de realización u optimización del fin constitucional y la intensidad de la intervención en el derecho afectado.
   La comparación de estas dos variables ha de efectuarse según la denominada ley de ponderación “Cuanto mayor sea el grado de la no satisfacción o de la afectación de un principio, tanto mayor tiene que ser la

[157] EXP. 01413-2017-AA/TC. Fundamento 13.
[158] Examen de idoneidad o de adecuación. EXP. 048-2004-AI/TC. Fundamento 65.
[159] EXP. 00540-2016-AA/TC. Fundamento 8.

[160] EXP. 048-2004-AI/TC. Fundamento 65. EXP. 045-2004-AI/TC. Fundamento 39.

importancia de la satisfacción del otro".

Por lo que para que una injerencia en los derechos fundamentales sea legítima, el grado de realización del objetivo de intervención debe ser por lo menos equivalente o proporcional al grado de afectación del derecho fundamental.[161]

Por lo señalado, toda medida o sistema de control que implemente el empleador, en ejercicio de su poder directivo, que pueda afectar derechos fundamentales del trabajador, se entenderá, en principio, adecuada y lícita si cumple el principio de proporcionalidad; es decir, si resulta idónea, indispensable y equilibrada.

No obstante lo señalado, hay autores como Goñi, que consideran que la aplicación del principio de proporcionalidad no sería suficiente; porque no atendería los problemas derivados de la afectación del derecho a la protección de datos personales del trabajador, "Este principio se detiene en una simple consideración de los límites a la actividad de indagación del empresario; no atiende más allá de los peligros provenientes de la intrusión sobre la conducta de la persona del trabajador. Y no comporta directriz alguna sobre los límites a la posibilidad del empresario de tratamiento de las informaciones recabadas en las actividades de control ni sobre los derechos del trabajador frente a los riesgos de manipulación y utilización de esas informaciones" (2009: 19).

Uniendo las dos posiciones, consideramos que, tratándose del derecho a la protección de datos personales, cuando el empleador elija una medida de control laboral (como el de la geolocalización) que afecte derechos fundamentales, deberá en primer lugar someterla al principio constitucional de proporcionalidad; para luego de superado el mismo, evaluar su implementación definitiva previa adecuación a la normativa del derecho a la protección de datos personales.

Si hecho lo señalado, se produce la afectación del derecho a la protección de datos

[161] EXP. 048-2004-AI/TC. Fundamento 65. EXP. 045-2004-AI/TC. Fundamento 40.

personales, se deberá garantizar la implementación o activación de todos los mecanismos, que la Ley le provee al trabajador, como titular de la información, para que ésta deje de ser tratada indebidamente y él recobre el control sobre la misma, para mitigar de la mejor manera posible, los daños de los que puede o pueda seguir siendo víctima.[162]

### 2.2. Dispositivo de geolocalización GPS y su uso empresarial

Las empresas en el contexto globalizado, interconectado y competitivo actual, buscan mayor eficiencia y productividad; para lo cual desarrollan diversas estrategias que comprenden la incorporación de variada tecnología que les permita el mejor logro de sus objetivos empresariales. Como un recurso, que va en la línea de lo señalado, en los últimos años se ha hecho más frecuente el uso del Sistema de Posicionamiento Global, conocido por sus siglas GPS (Global Positioning System)[163].

El Sistema de Posicionamiento global es un servicio diseñado por el Departamento de Defensa de los Estados Unidos[164] que proporciona a los usuarios información sobre posicionamiento, navegación y cronometría; brindando informaciones precisas de posición, velocidad y tiempo.

El Sistema está constituido por tres segmentos básicos: el segmento espacial, referido

---

[162] En la línea de la pertinencia de realizar este test de proporcionalidad, como también se le suele referir al principio de proporcionalidad, se refieren los Estándares de la Red Iberoamericana de Protección de Datos, al ocuparse de la ponderación del derecho a la protección de datos personales señalando que :

> **7.1.** Los Estados Iberoamericanos podrán exentar, en su derecho interno, el cumplimiento de los principios y derechos previstos en los presentes Estándares, exclusivamente en la medida en que resulte necesario conciliar el derecho a la protección de datos personales con otros derechos y libertades fundamentales.
> **7.2.** Esta exención deberá requerir de un ejercicio de ponderación con la finalidad de determinar la necesidad, idoneidad y proporcionalidad de la restricción o excepción conforme a las reglas y criterios que establezcan los Estados Iberoamericanos en su derecho interno.

[163] Cuando el dispositivo GPS se encuentra acoplado a un terminal telefónico móvil o red Wi-fi se denomina GMS (Global System for Mobile Communications), pero en la presenta investigación nos referiremos a la denominación genérica GPS.

[164] Información oficial del Gobierno de los Estados Unidos relativa al Sistema de Posicionamiento Global y temas afines. Consultado al 17 de octubre de 2020 en: GPS.gov:https://www.gps.gov/systems/gps/spanish.php

a una constelación formada por 24 satélites operativos que transmiten señales unidireccionales que proporcionan la posición y la hora de cada satélite del GPS; el segmento de control, formado por estaciones de seguimiento y control distribuidas por todo el mundo a fin de mantener los satélites en la órbita apropiada, las que realizan el seguimiento de los satélites del GPS, y garantizan el funcionamiento adecuado de la constelación de satélites; y el segmento usuario, que es el equipo receptor del GPS que recibe las señales de los satélites del GPS y las procesa para calcular la posición tridimensional y la hora precisa.

Para la Autoridad Nacional de Protección de Datos Personales peruana, "la geolocalización debe entenderse como la ubicación geográfica de un objeto en el espacio, el cual es medido en coordenadas, en otras palabras, es un concepto que hace referencia a la situación que ocupa un objeto en el espacio y que se mide en coordenadas de latitud (X), longitud (Y) y altura (Z)."[165]

Las empresas pueden utilizar el GPS para el logro de diferentes objetivos. Si desean mejorar la productividad y eficiencia pueden usar el GPS para monitorear la mercadería enviada rastreando dónde se encuentra en tiempo real y proporcionando al cliente información exacta sobre la entrega de su producto; o para acortar las rutas y hacer una mejor y más rápida distribución y envío de los productos o brindar el servicio -por ejemplo de taxi-de manera oportuna.

Si la finalidad es la seguridad, el GPS colocado en los vehículos de la empresa permitirá conocer dónde se encuentra el mismo ante un posible robo del vehículo o de la mercadería que transporta -dinero o joyas-; podrá enviarse alertas sobre el exceso de velocidad, sobre choques cercanos; o dependiendo del tipo de actividad puede ser útil en circunstancias de emergencia o urgencia, como para el caso de conductores de ambulancias, asistencia en carreteras; personal de seguridad, personal minero o de buceo, entre muchos otros.

[165] Expediente 14-2016-RD 08-2007-DGPDP. Análisis 3.4.

Pero lo que es objeto del presente trabajo es el uso del GPS como mecanismo de control de las obligaciones laborales del trabajador. Convirtiéndose este sistema en uno muy eficaz y apto para dicho cometido, brindando información para verificar el cumplimiento de dichas obligaciones.

Esto se produce normalmente cuando no es posible realizar un control presencial de los servicios o tareas concretas que se le asignan a los trabajadores. Los tipos de actividad o puestos, donde se suele utilizar este sistema, están referidos a los comerciantes o vendedores a domicilio; servicios técnicos como los de mantenimiento; visitadores; repartidores (como empresas Rappi, Glovo); transportistas; conductores de servicios de transporte, de ambulancias, de asistencia, de taxis; personal de vigilancia; servicios de mensajerías; monitores de servicios; trabajadores de campo, entre otros.

Para estos fines descritos, el GPS puede estar incorporado a un vehículo o a cualquier medio de transporte; o en un dispositivo electrónico móvil como puede ser un Smartphone, una lap top, una Tablet; o en los llamados wearable device, a través de dispositivos de geolocalización diseñados para ser llevados en las prendas de vestir o de trabajo, como pulseras o relojes, entre otros.

Si hablamos del GPS en el vehículo conoceremos no solo la ubicación del mismo sino, como es lógico, la ubicación del conductor; lo que será de utilidad en transporte de mercaderías o de pasajeros pues facilitará planificar o rediseñar las rutas, para asignación de tareas en atención a la cercanía del objetivo del servicio o producto. Puede también usarse en la ubicación de trabajadores que realizan actividades dinámicas en un espacio geográfico con instalaciones separadas, como centros comerciales o locales de fábricas como depósitos, almacenes, obras de infraestructura, etc.

Como lo señala González (2019: 47) los datos que suministra el GPS son muy variados y completos, pues no solo realizan la función básica de brindar la posición

en cada momento del dispositivo, lo que se llama geolocalización estática; sino también sus movimientos, el trayecto realizado, el tiempo invertido en cada ruta, el de espera, lo que se denomina geolocalización dinámica, entre otros. Señalemos como ilustración las funciones principales del GPS en un vehículo, colocado por una empresa y que fue materia de un proceso que mereció la sentencia del Tribunal Superior de Justicia del Principado de Asturias, Sala de lo Social, Sentencia 3058/2017 de 27 Dic. 2017, Rec. 2241/2017:

> Las funciones principales del dispositivo son: localización en tiempo real, visualización de trayectos con posición segundo -a segundo, visualización de tramos conducidos con exceso de velocidad, detección de vehículo más cercano a un punto / calle, cuentakilómetros basado en GPS y creación de alertas, datos que a su vez permitirán elaborar informes de distancia por día o por periodos, ralentí, recorridos, (reconstrucción de recorridos duración, kilometraje, recorridos efectuados fuera de horario), exceso de velocidad, localización, detalle de actividad (número de paradas, duración de la parada, retrasos).
>
> El dispositivo permitirá también configurar alertas, entre otras, de hora de arranque y aparcamiento del vehículo, hora de aparcamiento, exceso de velocidad, paradas no autorizadas, duración excesiva de las paradas, puntos de paso y paradas, entre otras.

Como estamos viendo, este mecanismo de control, permite también el acceso a información sobre el comportamiento del trabajador; por ejemplo el conductor, ¿cómo es al volante?; y si supone una monitorización continua, se podrá conocer no solo el paradero del vehículo sino del conductor mismo, o del personal que lleve el GPS en su móvil o en su Tablet o laptop, con lo cual el empleador podrá recopilar información sobre la conducta o hábitos del trabajador. Por ejemplo, su presencia en lugares donde venden comida, o en un gimnasio, iglesia, hospital, local sindical, partido político, asociación de determinado perfil, etc., con lo cual se pueden estar revelando datos de su vida privada que salen del espacio laboral y a los que no tiene derecho de conocer el empleador; y si el trabajador no fue informado de la colocación del GPS, o si lo lleva o debe llevar encendido todo el día, el riesgo de la invasión a su privacidad y a un indebido tratamiento de sus datos personales se concretará.

“La geolocalización arrastra mala fama por su especial impacto en la privacidad. Sin embargo, es una de las tecnologías más usadas en las empresas. Con la digitalización laboral, las empresas han visto aumentados sus riesgos de incumplir la normativa de protección de datos y vulnerar la intimidad de los trabajadores […] ahora más que nunca hay que poner el foco en la protección de esos datos”(Pardo de Vega 2020) [166].

Asimismo, puede presentarse otro riesgo; sobre quiénes tienen acceso a toda esa información personal geolocalizada; son ¿Sólo las personas autorizadas de la organización? ¿Se han implementado las medidas adecuadas de seguridad frente a accesos no autorizados? ¿Cuánto tiempo se conservarán dichos datos?.

De otro lado, puede ocurrir que dicha información excesiva, sea utilizada para finalidades diferentes o incompatibles con el control laboral para la que fue recogida.

El Tribunal Europeo de Derechos Humanos (TEDH)[167], declaró prima facie y de manera general, asunto: Uzunc. Alemania; que la vigilancia mediante GPS, así como el tratamiento y la utilización de los datos resultantes, supone una injerencia en la vida privada de la persona, aun cuando el dispositivo esté instalado en un objeto, como en un vehículo.

En otra oportunidad el alto tribunal con ocasión de la sentencia, recaída como definitiva en el caso Barbulescu V. Rumania[168], expone un criterio claro sobre los límites al poder de control del empresario cuando señala que “…las instrucciones de un empleador no pueden reducir la vida social privada en el lugar de trabajo a cero”.

Entra a tallar aquí, la legislación sobre protección de datos personales, la que deberá ser observada por el empleador, como responsable del tratamiento y en su caso también por el encargado del mismo, para que no se produzca un abuso y un control desproporcionado por invasivo o excesivo, del tratamiento de la información personal de los trabajadores, controlados mediante el GPS.

[166] Consultado al 23 de enero de 2020 en: https://www.eleconomista.es/opinion-legal/noticias/10316565/01/20/Geolocalizacion-riesgos-limites-y-oportunidades.html

[167] Parlamento Europeo. Consejo de Europa, El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado. Asunto: Uzunc. Alemania. Página 34. 2 de septiembre de 2010

[168] 5 de setiembre de 2017.Gran Sala. FJ. 80.

### 2.2.1. Los datos de localización como datos personales

La presente investigación se centra fundamentalmente en el tratamiento de los datos geolocalizados o localizados[169] de los trabajadores que realiza el empleador en ejercicio de su facultad de control, supervisión o vigilancia. Por ello es importante analizar si este tipo de datos obtenidos por el sistema GPS son datos personales; con ello, el sometimiento de su tratamiento a la legislación sobre protección de datos personales que existe en el Perú, será inobjetable e ineludible.

La Ley, Nº 29733, define a los datos personales en el numeral 4, de su artículo 2 como: "Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados".

El Reglamento de la Ley da, a su vez, una definición de los datos personales mencionando, a modo de ejemplo, algunos tipos de los mismos "Datos personales: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados."

La Autoridad Nacional de Protección de Datos Personales, en adelante la Autoridad, considera que una persona es identificada, cuando "[…] dentro de un grupo de personas, se la distingue de todas las demás. El identificador más común de una persona es el nombre (nombre propio o nombre de pila y nombre patronímico o apellido) por lo tanto, constituye un dato personal y convierte a la persona en "persona identificada", en algunos casos directamente y en otros con medios fácilmente utilizables" 3.4. Del análisis del Expediente 14-2016-RD 08-2007-DGPDP.

En la misma Resolución Directoral citada, se entiende que una persona es "identificable" directa o indirectamente cuando, aunque no se le haya identificado aún,

[169] Usaremos ambos términos de manera indistinta.

“sea posible hacerlo, porque para establecer la identidad habrá que combinar el nombre con otros atributos (fecha de nacimiento, dirección domiciliaria, fotográfica, documento nacional de identidad, entre otros).” Con relación a la identificación indirecta o individualización, la Autoridad, señala que se refiere a una persona que “puede ser identificada dentro de un grupo colectivo de datos, lo que permite que se tome decisiones que afecten a esa persona”.

Para la autoridad española, la Agencia Española de Protección de Datos, la persona será considerada identificable, cuando se pueda determinar su identidad, de manera directa o indirecta, en particular mediante un número de identificación o uno u otros elementos propios o particulares de su identidad “física, fisiológica, psíquica, económica, cultural o social” debiéndose tener en cuenta para este proceso de identificación los medios que puedan ser “razonablemente utilizados por el responsable del tratamiento o por cualquier persona, para identificar a dicha persona”.

Por lo tanto, no será una persona identificable, aquella cuya “identificación requiere plazos o actividades desproporcionados”. No siendo “imprescindible para que exista un dato personal una plena coincidencia entre el dato y una información concreta”, bastará con que dicha identificación pueda realizarse sin esfuerzos desproporcionados. Recurso N.º A/00128/2013.

Como ya lo vimos, la geolocalización permite la ubicación o posición geográfica de un objeto en tiempo real, sus movimientos, los tiempos de desplazamiento de un punto a otro, los momentos en que se está en parado o en pausa; por lo que permitirá saber dónde y cuándo estuvo la persona que lleva el GPS incorporado ya sea en su vehículo, celular, Tablet, reloj o inclusive en una prenda de vestir. Esta asociación no supondrá esfuerzos desproporcionados y menos tratándose de la relación laboral en la que el empleador sabe quién es el trabajador que usa alguno de los objetos o dispositivos, proporcionados por él, a los que se ha incorporado el sistema GPS; tratándose por lo tanto de datos personales, aquella información que brinda el uso de esta tecnología.

Así también ha concluido la Autoridad, en los pocos pronunciamientos que ha tenido

sobre datos geolocalizados, aunque no referidos al ámbito laboral, “la identificación de una persona que se da a través de la información generada por la ubicación de un teléfono móvil inteligente o dispositivo electrónico de naturaleza similar constituye un dato personal” Expedientes 14-2016-RD 08-2007-JUS/DGPDP/ 15-2016-RD-29-2017-JUS/DGPDP.

Por lo señalado, en la medida que los datos geolocalizados se refieren siempre a una persona física identificada o identificable son datos personales y le son de aplicación las disposiciones de la Ley de Protección de Datos Personales y su Reglamento.

En el ámbito europeo, el artículo 2 de la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas define los datos de localización como “cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de comunicaciones electrónicas disponible para el público”.

Asimismo, ya el Grupo de Trabajo del artículo 29, que era el órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, en el Dictamen 5/2005, sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido indicaba: “ Habida cuenta de que los datos de localización se refieren siempre a una persona física identificada o identificable, les son de aplicación las disposiciones sobre la protección de los datos personales establecidas en la Directiva 95/46/CE de 2410/1995.”[170]

La legislación, sobre protección de datos, más moderna de Europa ya incluye a los datos geolocalizados en sus textos normativos. El Reglamento (UE)2016/679 del Parlamento Europeo y del Consejo, los incluye desde la definición de datos personales: “ toda información sobre una persona física identificada o identificable (“el interesado”); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un

[170] Directiva que fue sustituida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

España, por su parte, en su reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, reconoce el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

Nuestra autoridad peruana, la Autoridad, concluye "Por tanto, los datos de geolocalización son datos personales". Análisis 3.4. Expediente N.º 14-2016-RD 08-2007-JUS/DGPDP.

Por lo expuesto, los tratamientos de los datos geolocalizados de sus trabajadores que realice el empleador, en ejercicio de su facultad de control, son datos personales y deberán someterse a las disposiciones de la Ley de protección de datos personales y de su Reglamento.

### 2.3. Nivel de tratamiento judicial y administrativo de la utilización de dispositivos GPS para vigilancia y control laboral en Perú

En el Perú, la legislación sobre protección de datos personales no se pronuncia sobre los datos geolocalizados; tampoco hace alusión alguna sobre las actividades de tratamiento de datos con el uso de la tecnología GPS. Asimismo, dentro de los tratamientos específicos de datos, regulados en la Ley o en el Reglamento, no se encuentra el tratamiento de los datos personales de los trabajadores en el ámbito laboral.

Tenemos un contexto de carencia legislativa sobre el uso de la tecnología del GPS para el tratamiento de datos personales en el contexto laboral en general y en específico para controlar a los trabajadores.

Por lo expuesto, consideramos importante, con el fin de tener una visión integral sobre

el tratamiento de nuestro tema en el Perú, conocer la atención que ha merecido el uso de la tecnología del GPS como mecanismo de tratamiento de los datos de los trabajadores; tanto por parte de los la jurisdicción constitucional, como por la labor administrativa desarrollada por la Dirección General de Transparencia Acceso a la Información Pública y Protección de datos personales, que es la autoridad de control sobre la materia.

Con el objetivo señalado se ha procedido a realizar la búsqueda en los portales del Tribunal Constitucional, del Poder Judicial, y del diario oficial El Peruano[171]; así como en la página web de la Autoridad Nacional de Protección de Datos personales.

### 2.3.1. Resoluciones judiciales

#### 2.3.1.1. Tribunal Constitucional

El tratamiento del GPS como mecanismo de control laboral no ha sido materia de ninguna sentencia del Tribunal Constitucional; de ello da cuenta la búsqueda realizada al 05 de noviembre del 2020, en el portal electrónico de este organismo Constitucional autónomo.[172]

#### 2.3.1.2. Poder Judicial

De las búsqueda realizada en el portal electrónico del Poder judicial[173], se han podido identificar 05 sentencias de casación y un Pleno Jurisdiccional Regional Laboral realizado en Chiclayo; asimismo en el Diario Oficial El Peruano[174], se ha encontrado

[171] Se ha buscado en las publicaciones que se realizan mensualmente con el nombre " Sentencias de Casación", hasta el mes de octubre del 2020 en el siguiente https://busquedas.elperuano.pe/

[172] La búsqueda se ha realizado hasta el 05 de noviembre del 2020 en el portal institucional del Tribunal Constitucional por medio de las palabras claves: GPS, sistema de posicionamiento global, sistemas de control satelital, protección de datos personales y autodeterminación informativa. http://181.177.234.7/buscarRes/public/resolucionjur

[173] Al 5 de noviembre del 2020, se ha buscado en las Salas Supremas, pues al ser la máxima instancia, las casaciones son publicadas.

[174] Se han buscado las casaciones laborales con las palabras claves: GPS, sistema de posicionamiento global, sistemas de control satelital, protección de datos personales y

una sentencia de casacón; en todas ellas se menciona o alude al uso del GPS o al sistema satelital como herramienta de control laboral.

### a. Pleno Jurisdiccional Regional Laboral realizado en Chiclayo, 06 de junio de 2009[175]

El segundo tema abordado por el Pleno jurisdiccional fue sobre la "Jornada extraordinaria de trabajo de choferes". El tema debatido fue con el objetivo de determinar si se encuentran los choferes excluidos de la jornada máxima legal, según los supuestos contenidos en el artículo 5 del Decreto Supremo No 007-2002-TR, Texto único Ordenado del Decreto Legislativo N.º 854, Ley de jornada de trabajo, horario y trabajo en sobretiempo, modificado por la Ley N.º 27671.

Conforme al artículo 5 citado, no se encuentran comprendidos en la jornada máxima laboral los siguientes trabajadores: los de dirección; los que no se encuentran sujetos a fiscalización inmediata y los que prestan servicios intermitentes de espera, vigilancia o custodia.

Una de las utilidades de tomar una posición sobre la interpretación del artículo 5 citado, es determinar la procedencia o no del pago de horas extras a los choferes, especialmente a los de transporte interprovincial; porque una posición considera que están excluidos de la jornada máxima legal y otra posición sostiene que, en determinadas circunstancias, no se encuentran excluidos de aquella.

En el Pleno jurisdiccional se presentaron dos ponencias:

-Primera ponencia. Sostuvo que los choferes están excluidos de la jornada máxima legal por encontrarse en los supuestos de falta de fiscalización inmediata y por

autodeterminación informativa. La búsqueda se ha realizado hasta el 5 de noviembre del 2020 en el siguiente https://jurisprudencia.pj.gob.pe/jurisprudenciaweb/faces/page/laboral.xhtml

[175] Participaron los doctores: Marco Antonio Pérez Ramírez, Vocal de la Corte superior de Justicia de Lambayeque, quien lo presidió; y los siguientes magistrados participantes: Eduardo Alonso Pacheco Yépez de la Libertad, Francisco Cunya Celi de Piura, Juan Manuel Alván Rivas de Cajamarca y Percy Elmer León Dios de Tumbes.

intermitencia de los servicios.

-Segunda ponencia. Sostuvo lo siguiente:

> Existen algunas situaciones de hecho que determinan que en casos particulares los choferes no se encuentran excluidos de la jornada máxima legal; ello por cuanto los adelantos tecnológicos (sistema de posicionamiento global-GPS, entre otros) permite una fiscalización directa y constante de su empleador; y, su tiempo de descanso en la prestación de la jornada debe considerarse como efectivamente trabajado en aplicación del Convenio OIT N.º 67.

La conclusión plenaria fue adoptada por unanimidad, y enuncia lo que sostuvo la segunda ponencia precedentemente citada.

Lo que podemos resaltar, en relación al tema que nos ocupa, es haber identificado y reconocido el uso del GPS como mecanismo de control del empleador sobre los trabajadores. El Pleno Jurisdiccional identifica al GPS como un mecanismo de fiscalización directa y constante del empleador; no obstante, esta herramienta tecnológica que cada día se usa más en el ámbito laboral, no es analizada desde el punto de vista del derecho a la protección de datos personales de los trabajadores, no se lo reconoce como actividad de tratamiento de la información personal de los empleados; sino como un supuesto que haría que los trabajadores, sujetos a ese tipo de control, sí estarían comprendidos dentro de la jornada máxima legal.

**b. Sentencias de casación laboral**

El análisis que vamos a realizar, de las sentencias encontradas, es en aquéllos aspectos relacionados con el control laboral y desde la perspectiva del derecho a la protección de datos personales, por lo que nos enfocaremos en los aspectos de las resoluciones que nos permitan, de manera directa o indirecta, lograr el objetivo señalado.

Se han identificado cinco sentencias de casación Laboral en las que se menciona, o alude, al GPS o sistema satelital como un mecanismo de control laboral. Vamos a

dividirlas en dos grupos.

**-Primer grupo: sentencias que fueron motivadas por el reclamo del pago, entre otros, de horas extras a choferes de transporte interprovincial**

Son las casaciones laborales: N.º 03780-2014. N. º 507-2015. N. º 15969-2015. Las tres del departamento de La Libertad, emitidas por la Segunda Sala de Derecho Constitucional y Social Transitoria de la Corte Suprema de Justicia de la República.

El punto de análisis de fondo, de las tres sentencias, se refiere, a la correcta interpretación y aplicación del artículo 5 del Decreto Supremo No 007-2002-TR, Texto Único Ordenado del Decreto Legislativo N. º 854, Ley de jornada de trabajo, horario y trabajo en sobretiempo; mediante el cual se dispone que no se encuentran comprendidos en la jornada máxima laboral los trabajadores incursos en los siguientes tres supuestos:

-Los de dirección;

-Los que no se encuentran sujetos a fiscalización inmediata y;

-Los que prestan servicios intermitentes de espera, vigilancia o custodia.

-De la sentencia de casación N. º 03780, se desprende que la resolución de vista, consideró que el demandante, chofer de transporte interprovincial, no obstante realizar labores de naturaleza intermitente[176] y que por lo tanto estaría excluido de la jornada máxima de trabajo; sin embargo, en aplicación del principio de razonabilidad, determinó que el demandante realizó labores por encima del límite de doce horas diarias, y que por lo tanto se le debe reconocer el pago de horas extras.

Por su lado, los jueces supremos, concluyeron que el actor no estaba comprendido en la jornada máxima de trabajo, pues, realizó labores intermitentes; hecho que

[176] El artículo 10 del Decreto Supremo Nº 008-2002-TR, en su literal b) define a los trabajadores que prestan servicios intermitentes como aquellos que regularmente prestan servicios efectivos de manera alternada con lapsos de inactividad.

tampoco fue cuestionado por el trabajador; por lo que desestimaron la pretensión referida al pago de horas extras.

Con relación al voto en minoría, que es el que reviste particular importancia para nuestro tema, primero se señala que la actividad de conducción de vehículos interprovinciales no puede ser considerada actividad intermitente, pues dicha actividad relativa al transporte masivo de pasajeros es permanente y no es discontinua. Con lo cual discrepa de lo decidido en mayoría.

Asimismo, señala que "el tiempo de descanso de los choferes […] no es de conducción pero tampoco es tiempo libre o de refrigerio pues el chofer no puede disponer libremente de su tiempo sino que se encuentra en el vehículo de su empleador. Esto es, se encuentra en el centro de trabajo a disposición de su empleador" por lo que el tiempo de descanso intercalado debe ser considerado para efectos del cálculo de la jornada máxima semanal y, de ser el caso debidamente retribuido. "Por tanto, el tiempo efectivo de trabajo de los conductores será el tiempo dedicado a la conducción, a los descansos intercalados y a otros trabajos durante el tiempo de circulación del vehículo y los trabajos auxiliares que se efectúen en relación con el vehículo, los pasajeros o la carga".

El voto en minoría analiza, más bien, si se aplica o no, otro de los supuestos de exclusión de la jornada máxima, no considerado en los pronunciamientos anteriores; es el referido a los trabajadores que están sujetos a fiscalización inmediata; señalando dentro de los mecanismos de control laboral al sistema de control satelital, de la siguiente manera:

> En el caso de los trabajadores que laboran fuera del centro de trabajo, debe de cumplirse el siguiente presupuesto para que no se encuentre presente la fiscalización inmediata: no deben de estar sujeto a vigilancia en la prestación de sus labores; presupuesto que no se cumple en el caso de los conductores de vehículos de transporte interprovincial, ya que normalmente los choferes cuentan con inspectores, sistemas de control satelital, tacómetro, hoja de ruta y otros medios que permiten la fiscalización y supervisión del trabajo que realizan.

Añadiendo que “La no presencia en el vehículo del piloto y copiloto puede dar lugar a responsabilidad disciplinaria para el trabajador y administrativa para la empresa”.

Por consiguiente, el voto en minoría considera que el trabajador demandante si se encuentra dentro de la jornada máxima de trabajo y debe pagársele horas extras, por estar bajo fiscalización inmediata, utilizándose para dicho fin, entre otros mecanismos, el del control satelital.

-La casación 507-2015, desarrolla básicamente el mismo razonamiento de la casación 3780-2014. Tanto la primera instancia, como la segunda señalaron que la labor del demandante, el conductor profesional especializado- chofer interprovincial-, desarrollaba labores de naturaleza intermitente; y por lo cual debería estar excluido de la jornada máxima de trabajo; sin embargo, en aplicación del principio de razonabilidad, determinaron que realizó labores por encima del límite de doce horas diarias, por lo cual se le debía reconocer el pago de horas extras.

La Corte Suprema coincide con las dos instancias previas en la idea de que los choferes realizan labores de naturaleza intermitente (en el caso de los choferes es un servicio intermitente de espera porque dichos trabajadores permanecen en el mismo vehículo aunque no pueden manejar en ese tiempo); pero señala que justamente por ello, se encuentran excluidos legalmente de la jornada máxima de trabajo, por lo que el empleador no tiene obligación de pagar horas laboradas en sobretiempo, conclusión contraria a la arribada por las instancias inferiores.

Igual a lo sucedido en la casación anterior, la 380-2014, el voto en minoría discrepará con los pronunciamientos anteriores pues considerará que los servicios que prestan los choferes interprovinciales no son de naturaleza intermitente, sino permanentes; pues dichos trabajadores permanecen al servicio de la empresa demandada, bien ejerciendo de manera alternada las funciones de chofer o como de copiloto de la misma unidad de transporte.

Además optará por analizar otra causal, como sustento del pago de horas extras, descartando otro supuesto de exclusión del artículo 5 del Decreto Supremo N.º 007-2002-TR. que se refiere a los trabajadores que no están sujetos a fiscalización inmediata; justamente porque los choferes interprovinciales, si están sujetos a ese tipo de fiscalización y por lo tanto puede ser objeto del pago de horas extras.

Dentro de los mecanismos de control, permanente e inmediato, mencionados, al que están sujetos los conductores de vehículos de transporte interprovincial, se nombran: "inspectores, sistemas de control satelital, tacómetro, hoja de ruta y otros medios que permiten la fiscalización y supervisión del trabajo que realizan. La no presencia en el vehículo del piloto y copiloto puede dar lugar a responsabilidad disciplinaria para el trabajador y administrativa para la empresa".

-La casación 15969-2015; al igual que en las dos sentencias de casación precedentes, la demanda se analiza desde la naturaleza de los servicios prestados por el chofer interprovincial demandante, para determinar si corresponde o no el pago de horas extras, entre otros.

La primera instancia deniega el pago de horas extras. La segunda instancia revoca la sentencia apelada en lo relacionado al pago de horas extras, amparando dicha pretensión, por considerar que el chofer interprovincial estuvo sujeto a lapsos de intermitencia, y que si bien es cierto que por ello se encuentra excluido de la jornada máxima laboral, no obstante declara fundada dicha pretensión.

La Corte Suprema considera que la sentencia de vista ha realizado un razonamiento incongruente y no contiene una debida motivación. Razón por la cual declara nula la sentencia de vista.

De la misma forma en que las dos casaciones precedentes, en los pronunciamientos de las dos primeras instancias así como en el de la Corte Suprema no se alude al sistema satelital o de GPS como mecanismo de control laboral. Lo hace también, en esta ocasión, el voto en minoría.

Así cuando analiza la normativa respecto a la jornada de trabajo de los choferes interprovinciales, señala que el actor, al estar de manera permanente al servicio de la empresa demandada, ejerciendo de manera alternada sus funciones de chofer como copiloto de la misma unidad de transporte, queda determinado el tiempo de espera como de trabajo efectivo para el caso de los choferes de transporte interprovincial de pasajeros; no cumpliéndose la labor intermitente y no siéndole de aplicación las consecuencias normativas del artículo 5 del Decreto Supremo N.º 007-2002-TR.

Asimismo, analiza que a este tipo de trabajadores no se le puede aplicar la exclusión de la jornada máxima regulada en el artículo 5 citado; pues ellos, laborando fuera del centro de trabajo, están sujetos a fiscalización inmediata, a través, entre otros medios, del uso de los sistemas de control satelital; en la misma línea de lo señalado en los votos singulares de las dos sentencias de casación precedentes.

En este primer grupo de sentencias de casación, podemos apreciar que el sistema satelital o el GPS, solo es mencionado en los votos singulares. Además su mención es para considerarlo como un mecanismo de control, supervisión o fiscalización inmediata y permanente de los trabajadores; que en los supuestos de los casos analizados son trabajadores que cumplen sus funciones fuera del centro de trabajo, en su calidad de choferes interprovinciales. Pero, no se analiza el uso de la información personal de los trabajadores que proporciona el GPS al empleador, es decir el impacto y la pertinencia de usar esa tecnología con relación a la persona de un trabajador.

**-Segundo grupo: sentencias que reclaman por un despido arbitrario**

-Casación laboral No 3776-2015. La Libertad. Segunda Sala de Derecho Constitucional y Social Transitoria de la Corte Suprema de Justicia de la República.

La demanda de fondo es sobre impugnación de despido fraudulento y otros. La

sentencia de primera instancia declara infundada la demanda porque considera que existe prueba razonable de la existencia de los hechos imputados al demandante, para adoptar la decisión de despido.

La Sentencia de segunda instancia revoca la apelada porque sostiene que los hechos imputados al trabajador accionante no han sido acreditados. De la sentencia se desprende que al trabajador se le imputó incumplimiento de sus obligaciones laborales por no encontrarse en el lugar donde debía prestar sus servicios en virtud a la información proporcionada por el Sistema de Posicionamiento Global o GPS. Dicha sentencia sustenta su fallo señalando que:

> Los hechos imputados al accionante no han sido acreditados en el decurso del proceso, pues no se ha comprobado que se haya encontrado en la localidad de Casa Grande los días dos y tres de marzo de dos mil doce; ello debido a que la empresa emplazada ha sustentado tales imputaciones en la información proporcionada por el Sistema de Posicionamiento Global (GPS), el cual no se encontraba homologado[177]; por lo tanto se desconoce si al momento de acaecidos los hechos la información proporcionada por dicho sistema era optima [sic]; máxime si se encuentra probado que el actor prestó servicios el dos de marzo de dos mil doce en la localidades de Compín, pernoctando en dicho lugar, para posteriormente regresar a la ciudad de Trujillo al día siguiente; razón por la cual concluye que el demandante ha sido objeto de un despido fraudulento.

La Corte Suprema coincide, en el extremo acabado de señalar, como sustento del fallo de la Corte Superior.

Como podemos apreciar se admite, la utilización del GPS como mecanismo de control laboral, sin cuestionar o analizar las condiciones de su uso como mecanismo de supervisión que trata datos localizados de los trabajadores. Se desprende que la

[177] La homologación consiste en verificar que el modelo del equipo fue fabricado para la correcta operación en el país. ... Si encuentra el modelo exacto de su teléfono, quiere decir que ya está homologado y puede hacer el registro con su operador. consultado al 06 de noviembre de 2020 en: https://www.google.com/search?rlz=1C5CHFA_enPE872PE872&q=que+significa+que+un+equipo+est%C3%A1+homologado&spell=1&sa=X&ved=2ahUKEwiNvafygPTsAhUzC9QKHX3kCkIQBSgAegQIGBAt&biw=1440&bih=821.

información proporcionada por un GPS, que hubiera estado homologado, no hubiera tenido objeciones para ser admitida como prueba.

El análisis del GPS, desde la primera instancia, pudo hacerse desde la perspectiva del derecho a la protección de datos personales y de otros derechos como el de la intimidad, o el disfrute del tiempo libre. Pues aunque se esté ante la información que proporcione un GPS homologado, puede resultar que la información que dicho sistema proporcione, en efecto pueda ser exacta e incuestionable técnicamente; pero eso no implica que no pueda ser cuestionada jurídicamente, a la luz de los límites que el poder del empresario tiene frente a los derechos de sus trabajadores, como los que le impone el de la autodeterminación informativa.

Supongamos que en efecto el trabajador, por información del GPS en perfecto funcionamiento estuvo en otro lugar diferente al del lugar donde debía prestar sus obligaciones laborales; pero el trabajador no fue informado de los alcances y las condiciones en que se iban a tratar sus datos personales que iba a proporcionar dicha tecnología ni las consecuencias que podrían derivarse de la misma, para su persona; por ejemplo, por la que se le podría aplicar sanciones que podían llegar al despido.

A la luz de la Ley de Protección de Datos Personales, el empleador, como responsable del tratamiento, debe informar de manera clara, expresa e indubitable de las condiciones del tratamiento al que serán sometidos los datos personales, en este caso los datos localizados de los trabajadores, incluyendo las consecuencias que dicha información podría acarrear para el trabajador; de lo contrario no podría ser utilizada válidamente, en la medida que como titular de sus datos, el trabajador habría perdido su control; y es más bien otra persona, el empleador, el que controla y dispone de una información de manera indebida porque se trataría de un tratamiento ilegal que dejaría vacío de contenido el derecho fundamental mencionado de su trabajador, en el supuesto descrito.

Por lo dicho si se hubiera analizado el uso debido del GPS, como mecanismo de

control del trabajador que trata datos personales, es muy probable por ejemplo, ante la ausencia de la comunicación de la información debida, no sólo que no se hubiera podido admitir como prueba de incumplimiento de obligaciones laborales; sino que, a la vez, se hubiera constituido una violación del derecho a la protección de datos personales, ante el desconocimiento de las condiciones de tratamiento a las que se sometían los datos geolocalizados del trabajador.

Además en virtud del tratamiento indebido de sus datos personales y, en atención a la naturaleza relacional del derecho, también se hubiera producido, la violación al derecho a la intimidad, en atención a que se presenta en la sentencia la ubicación de los lugares donde había pernoctado el trabajador; poniendo de manifiesto el control de una conducta extra laboral y por lo tanto fuera del contexto en el que el empleador puede ejercer su poder de dirección, con su correlativa facultad de control.

-Casación laboral No 17968-2017. Junín. Segunda Sala de Derecho Constitucional y Social Transitoria de la Corte Suprema de Justicia de la República.

El tema de fondo del presente proceso es la pretensión de indemnización por supuesto despido arbitrario contra la empresa Mi Banco, interpuesta por uno de sus gerentes zonales. La imputación es haber realizado mal uso de la camioneta fuera del horario de trabajo sin autorización de los superiores, incumpliendo sus obligaciones laborales.

La prueba presentada es que el mismo trabajador en su calidad de Gerente Zonal, remitió vía correo electrónico un cronograma de uso del vehículo de la empresa, indicando que dicha camioneta estaría en uso a partir del 06 de abril de 2016; sin embargo, de acuerdo al reporte de GPS se verificó que la camioneta fue utilizada el día 05 de abril del mismo año desde las 10:41 am, hasta las 05.51 pm, no habiéndose informado de tal hecho a sus superiores.

La sentencia de primera instancia declaró infundada la demanda del trabajador. La

sentencia de la Sala laboral de la Corte Superior de Huancayo revocó la sentencia de primera instancia y declaró fundada la demanda.

La sentencia de la Corte Suprema, declara nula la sentencia de vista considerando que no tomó en cuenta, principalmente, los siguientes fundamentos: no se habría vulnerado el derecho de defensa del demandante, pues pese a que la demandada le habría convocado en reiteradas oportunidades a aquél para que concurra a la agencia con el fin de visualizar el correo electrónico institucional, donde supuestamente tendría las pruebas fehacientes que sustentarían sus descargos ante la falta imputada, el trabajador habría renunciado a dicha citación; que el demandante habría reconocido en la audiencia de juzgamiento el uso del vehículo asignado fuera de la jornada de trabajo y en días no laborables; y que se debió tomar en cuenta que por la envergadura del cargo, del demandante, como Gerente Zonal, supondría que tendría total conocimiento de la normatividad y de todas las políticas del Banco.

Como puede otra vez apreciarse, en el presente caso, del texto de la resolución publicada, se ha utilizado el GPS con la finalidad de controlar laboralmente al trabajador y no con la finalidad de seguridad del vehículo. Esto queda claro, porque el despido se sustenta básicamente en el reporte del seguimiento satelital, dando cuenta que el trabajador usó el vehículo, que la empresa le asignó, fuera de la jornada de trabajo y en días no laborables.

Por lo expuesto, lo que se ha realizado, es un seguimiento a la persona del trabajador y un control sobre el mismo, a través de sus datos personales geolocalizados. Sin embargo, este análisis no ha sido tomado en cuenta en ninguna de los tres pronunciamientos de las diferentes instancias del Poder Judicial, en un caso cuyos hechos acaecieron en el año 2016.

Por lo que a la luz de lo que manda la Ley de protección de datos personales que data del 2011, así como su Reglamento, surgen varios interrogantes que consideramos debieron ser abordados a lo largo del proceso para determinar si hubo un debido y por tanto legal uso de los datos personales localizados del demandante; pero que no

se hicieron, a la luz de lo detallado en la sentencia de casación.

En la línea de lo señalado, debió determinarse si el trabajador fue informado de manera clara, expresa e indubitablemente con lenguaje sencillo de: la finalidad o finalidades del tratamiento al que iban a ser sometidos sus datos personales de localización; así como de las consecuencias incluyendo las posibles sanciones; de la existencia del banco de datos geolocalizados en que se almacenarían los mismos, entre otras informaciones que el responsable del tratamiento, en este caso el empleador, debió hacerle saber al titular de los datos, su trabajador, en cumplimiento de los artículos 18 de la Ley y 12 del Reglamento.

Pero, además, resulta ineludible reflexionar y evaluar los debidos alcances del control del empleador en ejercicio de su facultad de fiscalización sobre las actividades laborales a cargo del trabajador demandante.

Se entiende que el poder de dirección le faculta al empresario a fiscalizar a sus trabajadores en el marco que da la relación laboral; porque fuera de la relación laboral el empleador ya no tiene el poder de dirección que le habilita fiscalizarlos. Por ello, para tratar los datos personales de sus trabajadores, al margen de la relación laboral, como fuera del horario de trabajo o en días no laborables, como se ha producido en el presente caso, necesitaría, considerando las salvaguardas debidas, del consentimiento de sus trabajadores, tal como manda el artículo 5 de la Ley.

Es evidente que el empresario, no requiere solicitar el consentimiento de nadie para geolocalizar el vehículo fuera del horario de trabajo, con fines de seguridad; no obstante, cuando el vehículo de la empresa es usado por un trabajador, lo que se recopila y trata son datos personales de la persona que usa el vehículo, y para eso el empleador no puede ir más allá de su poder de dirección, abarcando espacios extra laborales, avasallando los derechos del trabajador, realizando un indebido tratamiento de los datos personales de su persona, afectando además su intimidad, el disfrute del descanso y de su tiempo libre.

Entonces, en la presente casación, el empleador debió contar con el consentimiento del trabajador para controlarlo más allá del contexto de la relación laboral, y debió cumplir con el deber de informarle al mismo, sobre las condiciones, finalidades y alcances del tratamiento al que iban a ser sometidos sus datos geolocalizados; no obstante esto no ha sido objeto de pronunciamiento ni de análisis en el presente supuesto.

Sin embargo, en el presente caso, ¿cuándo podría haber sido considerado claro que el empleador aplique el despido basándose en los datos de geolocalización?; para tratar de verlo desde la perspectiva del empleador en relación a su interés legítimo de velar por la seguridad del vehículo asignado al trabajador; creemos que lo sería si se le informó adecuadamente a éste, que el uso del vehículo fuera del horario laboral y/o para fines personales, mediante el reporte del GPS, sería una falta grave con la consecuencia del despido.

Esto no habría ocurrido, por lo menos desde la normativa de protección de datos personales, pues dentro de los fundamentos que reconoce la Corte Suprema se ha señalado que el demandante habría reconocido el uso del vehículo asignado fuera de la jornada de trabajo y en días no laborables; y que "se debió tomar en cuenta que por la envergadura del cargo, del demandante, como Gerente Zonal, supondría que tendría total conocimiento de la normatividad y de todas las políticas del Banco". Las mismas, que por lo menos a este nivel, no han merecido una mayor mención o descripción.

La Corte Suprema valida la suposición de que el trabajador por el cargo que desempeña debía conocer que el reporte del GPS sobre el uso del vehículo fuera del horario de trabajo supondría un despido. Para la Ley y el Reglamento de protección de datos personales, la prueba de la información adecuada, que de manera previa debe darse a conocer al trabajador sobre el tratamiento de sus datos geolocalizados, le corresponde al empleador, como responsable del tratamiento de los datos personales, y no se admitiría una suposición al respecto, sino un análisis sobre no sólo si hubo información, sino de la adecuación de las condiciones y alcances de la

misma a la Ley y al Reglamento.

Como señala la Agencia Española de Protección de Datos: “La información previa y su prueba es esencial, ya que estos tratamientos no requieren el consentimiento del trabajador y son manifestación de los poderes de control del empresario.” (Resolución de archivo de actuaciones recaída en el Expediente Nº: E/06036/2014).

Esto nos lleva a tener que recordar que la legislación y las prácticas laborales no pueden aplicarse al margen de la legislación sobre protección de datos.

Como resultado de lo analizado en el presente acápite, y al tratar de buscar una interpretación ante la prescindencia del derecho a la protección de los datos personales (geolocalizados) de los trabajadores en los casos presentados; consideramos que nos encontramos en una situación de desconocimiento de esta materia.

Desconocimiento, no solo por parte de los titulares de los datos (trabajadores), de los responsables del tratamiento (empleadores) sino; parecería también, por parte de las autoridades encargadas de la aplicación de justicia constitucional laboral, frente a un derecho fundamental; el mismo, que ha sido reconocido constitucionalmente desde el año 1993 y que cuenta con una norma de desarrollo constitucional desde el año 2011. Situación que nos debe llevar a una mayor reflexión; pues estamos en un Estado Constitucional de Derecho.

### 2.3.2. Autoridad Nacional de Protección de Datos Personales

Con el fin de determinar si la Autoridad Nacional de Protección de Datos Personales se había pronunciado sobre el tratamiento de los datos geolocalizados de los trabajadores, en el contexto de la facultad de control que realiza el empleador, se procedió a realizar la búsqueda en la página web de la Dirección General de Transparencia Acceso a la Información Pública y Protección de datos Personales, como autoridad de control peruana en la materia, en los siguientes apartados; los

que corresponden a los diversos pronunciamientos de la Autoridad:

- Absolución de consultas. Que incluyen las: Opiniones consultivas[178], las opiniones técnicas[179] y los Informes jurídicos.[180]

- Procedimientos Trilaterales de Tutela.[181] A los que se dirigen los titulares de los datos personales a quienes, el titular del banco de datos o responsable del tratamiento, les ha denegado total o parcialmente el ejercicio de un derecho que le corresponde en su calidad de titular del dato. (por denegación de un Derecho ARCO).

- Procedimientos Administrativos Sancionadores[182]. Que se instauran para determinar una infracción a la Ley o al Reglamento; así como la sanción que pueda corresponder.

De la búsqueda realizada en los links correspondientes a todos los

[178] 2013 https://www.minjus.gob.pe/consultas-absueltas/
2014 https://www.minjus.gob.pe/consultas-absueltas/
2015 https://www.minjus.gob.pe/consultas-absueltas/
2016 https://www.minjus.gob.pe/consultas-absueltas/
2017 https://www.minjus.gob.pe/consultas-absueltas/
2018 https://www.minjus.gob.pe/consultas-absueltas-opiniones-consultivas/
2019 https://www.minjus.gob.pe/consultas-absueltas-opiniones-consultivas-2019/
2020 https://www.minjus.gob.pe/ultimas-noticias/consultas-absueltas-opiniones-consultivas-2020/

[179] 2018 https://www.minjus.gob.pe/consultas-absueltas-opiniones-tecnicas/

[180] 2018 https://www.minjus.gob.pe/consultas-absueltas-informes-juridicos/

[181] 2013 https://www.minjus.gob.pe/ptt-dgpdp/
2014 https://www.minjus.gob.pe/ptt-dgpdp/
2015 https://www.minjus.gob.pe/ptt-dgpdp/
2016 https://www.minjus.gob.pe/ptt-dgpdp/
2017 https://www.minjus.gob.pe/ptt-dgpdp/
2018 https://www.minjus.gob.pe/ptt-dgpdp/
2019 https://www.minjus.gob.pe/ptt-dgpdp/

[182] 2015 https://www.minjus.gob.pe/procedimientos-administrativos-sancionadores/
2016 https://www.minjus.gob.pe/procedimientos-administrativos-sancionadores/
2017 https://www.minjus.gob.pe/procedimientos-administrativos-sancionadores/
2018 https://www.minjus.gob.pe/procedimientos-administrativos-sancionadores/

pronunciamientos señalados, hemos podido determinar que la Autoridad[183] solo se ha pronunciado sobre el GPS, en tres Resoluciones Directorales recaídas en dos procedimientos trilaterales de tutela; pues la tercera es la que corresponde a la resolución de una reconsideración de uno de los dos expedientes previos. Dichas resoluciones son:

-RESOLUCIÓN N. ° 008-2017-JUS/DGPDP (EXP 14)[184]

-RESOLUCIÓN N. ° 002-2017-JUS/DGPDP (EXP 15)[185]

-RESOLUCIÓN N. ° 029-2017-JUS/DGPDP (EXP 15) [Reconsideración][186]

No obstante lo señalado, las tres resoluciones acabadas de citar, son solicitudes de tutela en ejercicio del derecho de acceso por parte de los titulares de los datos (usuarios) en el contexto de los servicios de telefonía que brindan distintos operadores de servicios públicos de Telecomunicaciones.

Si bien es cierto en dichas resoluciones se aborda de manera general, que los datos geolocalizados son datos personales, así como algunos usos del sistema de geolocalización; no analizan[187] el tratamiento de los datos geolocalizados de los trabajadores en general, ni el referido al tratamiento de dichos datos en ejercicio de la facultad de control laboral; sino que se solo se refieren al tema de una manera básica en atención a la materia solicitada.

Por lo que podemos afirmar que a nivel de la Autoridad Nacional de Protección de Datos Personales no ha habido pronunciamiento sobre el tema de los datos geolocalizados de los trabajadores en general, ni en el ejercicio de la facultad de control por parte del empleador.

Por lo expuesto, podemos señalar que en el Perú, el tratamiento de los datos geolocalizados de los trabajadores no ha merecido pronunciamiento de la legislación,

[183] Al 05 de noviembre de 2020.
[184] https://www.minjus.gob.pe/wp-content/uploads/2019/03/EXP-14-2016-RD-08-2017-DGPDP.pdf
[185] https://www.minjus.gob.pe/wp-content/uploads/2019/03/EXP-15-2016-RD-02-2017-DGPDP.pdf
[186] https://www.minjus.gob.pe/wp-content/uploads/2019/03/EXP-15-2016-RD-29-2017-DGPDP.pdf
[187] Resolución Directoral Nº008-2017-JUS/DGPDP. Punto de análisis 3.4

ni de la Autoridad Nacional de Protección de Datos Personales; ni del Tribunal Constitucional.

En lo que respecta al Poder Judicial, en tres sentencias de casación, la alusión al GPS como mecanismo de control laboral lo ha hecho el voto dirimente; un pleno regional laboral; y dos sentencias de procesos sobre despido arbitrario, pero que no analizaron el uso del GPS como mecanismo de control laboral, desde la perspectiva y lo que manda la Ley y el Reglamento de protección de datos personales.

Lo descrito, nos indica que la Ley y el Reglamento sobre la materia, con sus disposiciones generales, son lo único que puede guiar hasta el momento, a los empleadores cuando ejercen su facultad de control mediante el uso de los datos geolocalizados de sus trabajadores; situación que evidencia un riesgo real para éstos, en relación con un uso de su información personal, en el contexto de la relación asimétrica en la que se encuentran, y mediante la tecnología de los sistemas satelitales de rastreo, como lo es el GPS, cuyos alcances y usos son cada día más dinámicos e invasivos.

Ante esta situación, y en tanto se den regulaciones específicas, los principios rectores de la protección de datos, su conocimiento e interpretación adecuada a las distintas actividades de tratamiento de los datos personales en el contexto laboral, se constituyen en el apoyo y guías básicas para, la actuación conforme a derecho, de las partes que integran lo que llamamos la triple base (pilares) de la protección de datos personales: el titular del dato ( trabajador) , el responsable del tratamiento ( empleador) y la Autoridad, sea la administrativa como la judicial.

## Capítulo 3: Los principios rectores de la protección de datos personales y sus alcances al control laboral de los datos geolocalizados

El tratamiento de los datos personales que se da en el contexto de la relación laboral, no cuenta en el Perú, a nivel de la Ley ni del Reglamento, con normas específicas que lo regulen; sin embargo, en el año 2020, la ANPDP, emitió la Directiva Nº 01-2020-JUS/DGTAIPD, aprobada mediante la Resolución Directoral Nº 02-2020-JUS/DGTAIPD, denominada "Tratamiento de datos personales mediante sistemas de videovigilancia", la misma que incluye un apartado sobre la videovigilancia para el control laboral. Con lo que contamos por primera vez, con algún tipo de normativa que se introduce al ámbito laboral, específicamente para guiar al empleador, pero solo cuando utiliza el sistema de videovigilancia para controlar a sus trabajadores.

Sin embargo, no existe regulación sobre el tratamiento de los datos geolocalizados en general y menos alguna normativa que guíe las actividades de tratamiento que realiza el empleador a la hora de controlar a sus trabadores, en ejercicio de su poder de dirección, mediante la tecnología del GPS.

Esta situación descrita, de ausencia de regulación específica, se replica en la inexistencia de criterios sobre el particular tanto en los pronunciamientos de los órganos jurisdiccionales como en los de la autoridad administrativa de control sobre la materia.

Lo señalado exige que los empleadores apliquen la normas sobre protección de datos personales, que son la Ley de Protección de Datos Personales y su Reglamento, interpretando sus disposiciones generales al contexto de la relación laboral y específicamente a la hora de realizar las actividades de tratamiento con los datos geolocalizados de los trabajadores; aunque dichas normas no vayan a dar todas las respuestas a los conflictos que puedan presentarse a la hora de tratar la información personal de los trabajadores en la relación laboral.

Por ello, para esta labor, es fundamental conocer, interpretar y observar adecuadamente los principios rectores de la protección de datos personales.

Sobre los principios rectores, ya tratamos de manera general en el primer capítulo de la presente investigación, por lo que vamos a tomar como base, lo desarrollado en él para aplicarlo al ámbito laboral y en específico al objeto fundamental de este trabajo.

El artículo 12 de la Ley, señala el valor y utilidad de los principios rectores. Dicho dispositivo, parte de decretar y, por lo tanto de resaltar, que los titulares de los bancos de datos, o encargados de tratamiento, y en general todos los que intervengan en alguna actividad de tratamiento de datos personales, deben adecuar su actuación a los principios rectores; esto no es solo una recomendación, es una obligación cuya inobservancia afectaría el contenido esencial del derecho a la protección de datos personales de los empleados y constituiría una infracción sancionable.

Dentro de las utilidades que la Ley le asigna a los principios rectores hay una que debe ser aplicada con intensidad al tratamiento de los datos personales de los trabajadores, y es la que dice que: “Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento”; esto significa que, ante la anemia de criterios y regulación específica, la ayuda más importante que tienen los empleadores a la hora de cumplir con la Ley y el Reglamento, cuando gestionan la información personal de sus empleados, son los principios rectores.

En este sentido, García-Coca anota lo siguiente:

> Como es lógico, es preciso identificar y distinguir los principios de la protección de datos para poder aplicarlos a las relaciones laborales y constatar si la utilización de datos de los trabajadores es acorde con la normativa sobre protección de datos. Con este sentido […] se justifica la descripción genérica de los mismos, profundizando en el contenido del principio de calidad, información y consentimiento. Aun sí, la mayor

parte de la doctrina muestra insatisfacción respecto de la aplicación de la LOPD a las relaciones de trabajo, por la dificultad de conectar el régimen genérico de la protección de datos con la dinámica existente en cualquier relación laboral, lo que podría justificar la promulgación de una normativa específica para resolver los problemas que se pueden generar en el centro de trabajo (2000: 85).

El grupo de Trabajo sobre Protección de Datos del Artículo 29, en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo[188], señalaba que los empresarios deben tener siempre presentes los principios fundamentales de protección de datos, independientemente de la tecnología utilizada, más aun tratándose de tecnologías como la del GPS, que al igual que otras, permiten un tratamiento más sistemático de los datos personales de los trabajadores en el entorno laboral.

Los principios rectores deben observarse y cumplirse en todo el ciclo de vida de los datos personales y en cada una de las actividades de su tratamiento, desde su recogida hasta su cancelación.

Como lo señala Emilia Zaballos "Es básico entender que no nos encontramos ante una serie de principios abstractos, sino que su inobservancia por el responsable del tratamiento constituye una infracción que acarrea, de forma posterior, una sanción" (2013:176).

### 3.1. Principio de Consentimiento

#### 3.1.1 Legitimidad del empleador para el tratamiento de datos geolocalizados de sus trabajadores

La base jurídica que constituye la piedra angular que habilita el tratamiento de los datos personales en el Perú, es el consentimiento de su titular. La Autoridad Nacional de Protección de Datos Personales, ha señalado en su Opinión Consultiva N.º 35-2019-JUS/DGTAIPD, sobre el particular lo siguiente: " […] el eje central para el

[188] Adoptado el 18 de junio de 2017.

tratamiento de los datos personales es el consentimiento. En ese sentido, es importante precisar, que el límite para el tratamiento de datos personales es la autorización del titular del dato personal, es decir, no se puede tratar la información más allá de lo que el titular consintió"[189] .

Frente a lo señalado, es legítimo preguntarse si en el contexto de la relación laboral cabe asumir que el consentimiento del trabajador, como titular del dato, pueda ser considerado pacíficamente, como regla válida, frente al tratamiento de su información por parte del empleador, teniendo en cuenta la relación asimétrica que los une; donde la posición del trabajador es la subordinada y por ende, la característica de libertad, que es esencial para el consentimiento válido, puede no ser cumplida a cabalidad.

El grupo de Trabajo sobre Protección de Datos del Artículo 29, en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, señalaba que: "es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas".

El considerando 43 del RGPD europeo, señala que no se puede considerar que el consentimiento se haya dado libremente cuando "exista un desequilibrio claro entre el interesado y el responsable del tratamiento", como ocurre en la relación generada por el contrato de trabajo entre empleador y trabajador; donde la situación de desventaja del empleado debe suponer, en todo caso, la adopción de mayores salvaguardas en el tratamiento de sus datos personales; pues se da en un contexto donde el que ejerce la posición de ascendencia, el empleador, por la necesidad de la ejecución del contrato de trabajo, accede a importante información de sus trabajadores y realiza diversas actividades de tratamiento con ellos, sin requerir el consentimiento de los mismos.

[189] Pág. 12.

Como señalan Hernández y Zamudio:

> […] los empresarios deben ser conscientes de que muchas actividades realizadas de forma rutinaria en el ámbito del empleo implican el tratamiento de datos personales de los trabajadores, a veces de información muy delicada. Cualquier actividad de recopilación, uso o almacenamiento de información sobre los trabajadores por medios electrónicos entrará casi con toda seguridad en el ámbito de aplicación de la legislación sobre protección de datos (2020: 5).

En la línea de lo señalado, lo que legitima al empleador a realizar el tratamiento de los datos personales de sus trabajadores, no es el consentimiento de éstos, sino la excepción considerada en el artículo 14, inciso 5) de la Ley, cuando dispone que: "No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento […] 5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte […]".

Por lo tanto, en el contexto de la relación laboral, la base que legitima el tratamiento de los datos personales de los trabajadores por parte del empleador no es el consentimiento de los trabajadores, sino la necesidad que surge de la celebración y ejecución del contrato de trabajo.

Entonces, en la relación laboral el empleador puede, sin el consentimiento de sus trabajadores, tratar sus datos personales para ejercer sus facultades derivadas de su poder de dirección: dirigir, fiscalizar y sancionar.

No obstante, no se debe de perder de vista nunca, que esta habilitación legal, solo alcanza el tratamiento de los datos estrictamente necesarios para ejercer su poder de dirección, y en el caso bajo análisis, su facultad de control a través del sistema GPS.

La facultad de fiscalizar, supervisar o controlar mediante GPS, en atención a sus alcances y naturaleza, no podrá aplicarse para controlar a todos los trabajadores de una empresa, sino a aquéllos que realicen una función o cumplan sus servicios de tal forma que solo se posible lograr el objetivo legítimo de control por medio de esta tecnología.

Dentro de los trabajadores que podrían ser objeto de fiscalización por el GPS podemos mencionar a los que realizan sus servicios fuera de las instalaciones de la empresa (vendedores, técnicos de asistencia, repartidores, supervisores, choferes, trabajadores de campo, enfermeros, etc.); o a los que los realizan en un local de gran dimensión, que exige ubicarlos en atención a demanda del servicio, como vigilantes de un centro comercial o personal de seguridad de instalaciones; entre otros.

Parece justo que, el empleador que no puede realizar un control laboral directo, en persona, por no encontrarse el trabajador prestando sus servicios en las instalaciones u oficinas de la empresa pueda, en principio, optar por la vigilancia por medio del GPS; tecnología que le permitirá saber en qué lugar se encuentra en un momento exacto el trabajador, durante la jornada laboral, y siempre, respetando los principios como el de proporcionalidad, calidad y seguridad de los datos.

En este punto consideramos oportuno tomar en cuenta lo señalado, en la Recomendación CM/Rec (2015) 5 del Comité de Ministros del Consejo de Europa[190], sobre el tratamiento de datos personales en el contexto del empleo, en relación a que no debería permitirse el uso de sistemas que tengan por principal finalidad la monitorización de la actividad y el comportamiento de los empleados. Sin embargo, cuando dicha monitorización responda a fines legítimos como puede ser, el control laboral, deberán adoptarse garantías adicionales.

[190] Punto 10. Consultado el 22 de noviembre del 2020 en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

#### 3.1.1.1. Transparencia e información

Si bien está claro que para que el empresario o empleador, realice el tratamiento de los datos geolocalizados de sus trabajadores con fines de control, no necesita el consentimiento de éstos, en atención a la excepción al consentimiento del artículo 14º, inciso 5), la no exigencia del consentimiento es de lo único de lo que se lo exime con relación a la normativa sobre protección de datos; por lo que en obediencia del deber (para el responsable del tratamiento) y derecho (para el titular del dato) de la información, el empleador deberá cumplir con lo dispuesto por el artículo 18 de la Ley y 12 del Reglamento.

Así lo reconoce la misma ANPDP, en diversos pronunciamientos; como el contenido en la absolución de consulta OC 9 del 2017[191] "[…] es preciso tener en cuenta que en los casos en los que no se requiere el consentimiento para el tratamiento se deben cumplir las demás obligaciones señaladas en la LPDP y su Reglamento, entre ellas, la de informar a los titulares de los datos personales sobre los detalles del tratamiento que se va a realizar de acuerdo a lo señalado en el artículo 18º de la LPDP".

Tratándose del tratamiento de los datos de los trabajadores en el ámbito laboral, como el caso de los datos geolocalizados con fines de control, el cumplimiento del deber de información debe ser más cuidadosamente observado. Lo señalado es porque no se requiere el consentimiento del trabajador, para que el empleador trate sus datos personales, y además por la naturaleza asimétrica de la relación laboral que los une.

Teniendo en cuenta los artículos 18 de la Ley y 12 del Reglamento, así como la Resolución Directoral N.º 43-2018-JUS/DGTAIPD que aprueba un modelo de cláusula informativa con las condiciones de tratamiento; el empleador, que actúa en virtud a su poder de fiscalización, deberá informar a sus trabajadores objeto de control laboral, a través de sus datos geolocalizados, lo siguiente:

-La identidad del empleador como titular del banco de datos o responsable del

[191] Oficio N.º 252-2017-JUS/DGPDP.

tratamiento; su domicilio o dirección.

-La existencia del banco de datos personales en que se almacenarán los datos geolocalizados.

-La finalidad de control laboral descrita detallada y adecuadamente.

-La identidad de quienes puedan ser sus destinatarios.

La Autoridad, en la resolución directoral en la que aprueba la cláusula informativa, señala que en caso de no realizarse la transferencia de datos personales, esa información debe quedar indicada de la siguiente manera: “Los datos personales no se transmitirán a terceros, salvo obligación legal”, en consonancia con la transparencia y lealtad que deben guiar todo tratamiento de datos personales.

En el caso de los datos geolocalizados para fines de control laboral, podríamos encontrar supuestos de encargos de tratamiento, como pueden ser otras personas, naturales o jurídicas, con quienes mediante una relación jurídica, el empleador se vincula, para un encargo de tratamiento de este tipo de datos. Si bien en este caso no se considerará una transferencia de los datos personales geolocalizados, conforme al artículo 36 del Reglamento, si deberá informarse de dicha circunstancia al trabajador; es decir, informarle sobre la identidad del encargado del tratamiento.

-El plazo durante el cual se conservarán sus datos geolocalizados.

En este punto, entendemos que cumplida la finalidad de control laboral, es decir si se verificó el cumplimiento adecuado de los deberes del trabajador, debe procederse a la cancelación de los datos geolocalizados. De otro modo, si en virtud a ellos, se descubre un incumplimiento de las funciones laborales, la conservación durará hasta que se agote el procedimiento sancionatorio correspondiente y los plazos para una posible impugnación de los resultados del mismo ante las instancias establecidas. No obstante; en esta caso, consideramos que los datos deberán permanecer bloqueados para cualquier uso diferente a hacer frente a la impugnación que pueda activarse ante la medida sancionatoria del que haya podido ser objeto el trabajador.

-La posibilidad de ejercer los derechos que le corresponden al trabajador como titular de los datos geolocalizados, así como los medios previstos para ello. La resolución directoral que aprueba la cláusula informativa en este punto señala:

> […] como titular de sus datos personales el usuario tiene el derecho de acceder a sus datos en posesión de (indicar el titular del banco de datos personales); conocer las características de su tratamiento, rectificarlos en caso de ser inexactos o incompletos; solicitar sean suprimidos o cancelados al considerarlos innecesarios para las finalidades previamente expuestas o bien oponerse a su tratamiento para fines específicos.

Esto supone que el trabajador pueda ejercer con libertad sus derechos como titular de los datos geolocalizados, para seguir en el control de los mismos, sin represalias de ningún tipo[192].

-Asimismo, el empleador deberá señalar que ha adoptado los niveles de seguridad y de protección de datos personales legalmente requeridos, y ha instalado todos los medios y medidas técnicas a su alcance.

Toda esta información detallada, sobre las condiciones del tratamiento, se podrá dar en dos oportunidades tratándose del control laboral mediante el sistema del GPS.

Si el empleador, antes de contratar a un trabajador para un puesto, ya tiene decido y previsto controlarlo por medio del GPS, podrá cumplir con el deber de información a la hora de la celebración del contrato de trabajo. De otro lado, si la decisión de implementar el control mediante el GPS se da durante el desarrollo de la relación laboral, es decir, es un mecanismo de control nuevo a implementar, deberá hacerlo antes de comenzar a recopilar los datos geolocalizados.

Cualquiera sea la circunstancia en que se implemente el uso del GPS para tratar datos

[192] El capítulo IV del Regalamiento establece las disposiciones para el ejercicio de los derechos que le corresponden a los titulares de los datos personales.

geolocalizados de los trabajadores con fines de control; siempre la información deberá ser dada al trabajador, objeto de este tipo de control, de manera previa a la recopilación de sus datos geolocalizados. Esto en cuanto a su oportunidad de informar; pero, además, en cuanto a cómo debe informar, el Reglamento señala que la información será comunicada en forma clara, expresa e indubitable y con lenguaje sencillo.

El titular del dato debe ser informado con transparencia, por parte del empleador de todas las condiciones del tratamiento de su información, para que el trabajador conozca qué clase de información suya recogen; cómo la gestionan; cómo la analizan; con quién la comparten; qué decisiones se toman a partir de ella y con base en qué factores; así como las consecuencias que de ella pueden derivarse para él.

Veamos criterios sobre el derecho- deber de información esgrimidos por la Agencia Española de Protección de Datos, esbozadas en procedimientos administrativos sancionadores sobre el tratamiento de datos geolocalizados de trabajadores. No existe un procedimiento similar todavía seguido ante nuestra Autoridad de control peruana.

Mediante la Resolución R/03010/2016 emitida por la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00275/2016, contra la empleadora U.T.E. MADRID SUR MOVILIDAD LOTE IV, en adelante la empresa denunciada, la autoridad de control española impuso una sanción contra la empresa denunciada por violación a la Ley de Protección de Datos Personales.

La empresa denunciada había procedido a dotar a sus trabajadores de unos dispositivos móviles denominados PDA al objeto de controlar su actividad. Dichos equipos contaban con localización mediante GPS. La empresa denunciada contaba con unos 120 controladores y 6 inspectores a los que había dotado de dichos terminales móviles PDA´s con línea telefónica móvil y GPS. El uso de esos terminales se estableció como obligatorio ya que proporcionaba una serie de funcionalidades necesarias para el desempeño del trabajo.

Dentro de las finalidades del servicio GPS incluidos en la PDA se encuentran: el Fichaje del personal al inicio y final de la jornada laboral; la introducción de las matriculas para la verificación de la autorización del vehículo correspondiente, el envío de las detecciones del vehículo lector de matrículas al controlador.

En el presente caso, la información al comité de empresa se realizó por parte de la empresa denunciada en fecha de 19/5/2015, trasladando con posterioridad la información a cada uno de los trabajadores, cuando la recogida de los datos de geo-localización de los trabajadores se venía realizando desde el comienzo de la actividad de la empresa en fecha de 1/11/2013.

Como lo afirma la Agencia Española de Protección de Datos, “la información sobre la finalidad del sistema implantado, sus usos, y el establecimiento del procedimiento para el ejercicio de derechos a los mismos datos constituyen parte esencial no solo del marco de protección de datos de carácter personal sino también relevante en el ámbito de los derechos y deberes laborales relacionados con los derechos a la intimidad personal y a la propia imagen”.

Quedó demostrado que la empresa denunciada puso en funcionamiento en noviembre de 2013 un sistema de geolocalización de sus empleados que permitía la monitorización de los datos de localización. Por lo que el empleador debió cumplir con un tratamiento de los datos “no sólo legal, sino también leal, e implícito en dicho deber de lealtad se encuentra el de prestar una información adecuada al afectado o interesado, de forma que conozca el alcance real del consentimiento que presta o caso de no precisarse, los fines de la recogida y el modo de ejercitar los derechos”.

Pero así como una ausencia de información previa sobre las condiciones del uso del GPS con fines de control invalida una sanción basada en lo que reporte dicho dispositivo; de igual, manera una información previa y adecuada de las condiciones de uso y tratamiento de los datos personales geolocalizados a los trabajadores, habilitan el ejercicio de los poderes de control y disciplinario que le corresponden al

empleador. Esto lo podemos ver en el siguiente pronunciamiento de la Autoridad de control española.

Mediante una resolución de archivo de actuaciones recaída en el Expediente N.º: E/06036/2014, entre los trabajadores denunciantes, y la empresa denunciada EULEN SEGURIDAD, S.A.; los trabajadores manifestaron que los habían despedido utilizando un sistema de control de flotas con dispositivo GPS; cuando la utilización de dicho dispositivo no fue comunicado debidamente a los trabajadores, y por lo tanto, desconocían el uso que la empresa estaba haciendo de este sistema de control.

Se demostró que los trabajadores sí tenían conocimiento de que en el vehículo de la empresa, con el que prestaban sus servicios, se había instalado un sistema de GPS. Asimismo que "[…] la empresa demandada informó al actor de que sus datos serían incorporados a los ficheros de datos personales incorporados a la Empresa y que serían tratados con la finalidad de permitir el ejercicio de los derechos y el cumplimiento de las obligaciones derivadas de su relación laboral […]".

La Resolución analiza que se cumplió el principio de proporcionalidad, cuando se decidió establecer la presente medida de control laboral señalando que:

> puede ser perfectamente razonable dotar de un dispositivo de geolocalización en tareas como, en el presente caso, mantener la seguridad en las instalaciones del transporte por ferrocarril y para las que resulte relevante conocer donde se encuentra el vehículo dotado de localizador y, por ende los trabajadores, en qué momento se están llevando a cabo las obligaciones derivadas de la realización de labores de la seguridad, sin que ello pueda suponer pues no sería proporcional que se facilite un dispositivo de esta naturaleza a todos los trabajadores de la empresa cuando su tipo de prestación no lo haga necesario.

El Jefe de Seguridad en el ejercicio de las funciones, realizó una inspección rutinaria del servicio que presta EULEN en las líneas de alta velocidad de ADIF. Para localizar el lugar donde se encontraba la patrulla a inspeccionar, utilizó el GPS. En dicha inspección se constató que dos vigilantes armados, que deberían estar patrullando a

lo largo de las vías del AVE, se encontraban en su casa particular y con signos evidentes de haber consumido alcohol.

Dichas irregularidades dieron lugar a la apertura de una investigación para comprobar la correcta prestación del servicio de vigilancia de la línea de alta velocidad, con el resultado del despido a los trabajadores involucrados.

Concluyendo la Autoridad de España que “la prueba obtenida mediante la utilización de un sistema de GPS es lícita puesto que, en el presente caso, la empresa informó previamente al trabajador, tanto de la existencia del sistema de GPS como de la posibilidad de utilizar sus datos para controlar el cumplimiento de sus obligaciones laborales”. Por lo que quedó acreditado, que los trabajadores de EULEN, estaban informados previamente y de buena fe de la instalación de dichos dispositivos. Conducta empresarial que observó las prescripciones previstas en la normativa sobre protección de datos personales.
Reiterando que “La información previa y su prueba es esencial, ya que estos tratamientos no requieren el consentimiento del trabajador y son manifestación de los poderes de control del empresario.”

Por lo señalado, el empleador no podría realizar una vigilancia por medio de la geolocalización de forma oculta, sin que el trabajador haya sido informado.

¿Podría darse el caso de que se considere legal de maneara excepcional una vigilancia oculta de los datos geolocalizados de los trabajares que están bajo control laboral?

No tenemos en Perú pronunciamientos o criterios sobre la posibilidad de vigilancia oculta, como supuesto de excepción, a un tratamiento de datos geolocalizados de los trabajadores; por lo que una respuesta incuestionable a la luz de nuestra legislación tendría que ser negativa, pues no sería admisible frente al deber de información regulado en la Ley.

No obstante, y teniendo en cuenta que el mundo de la realidad práctica puede presentar supuestos que no están previstos por la norma, lo que se torna más posible cuando interviene la tecnología; hemos querido traer a modo de reflexión algunos criterios jurisprudenciales que se han dado en el ámbito europeo, aunque con relación al uso de otras tecnologías que también se emplean para el control laboral como es el caso de la videovigilancia; a pesar de no ser una tecnología equivalente al GPS; podría iluminarnos ante un supuesto excepcional donde se entienda que solo con una vigilancia oculta, se podría obtener un objetivo o fin legítimo para el empleador que, además, haya también observado el principio de proporcionalidad.

La evaluación de dichos criterios para su excepcional posible aplicación no podría dejar de tener en cuenta la naturaleza y alcances de la tecnología que nos ocupa, y el supuesto concreto que debería reunir características extraordinarias, puesto que no nos estaríamos refiriendo a un control laboral normal.

El Caso de López Ribalda y otros versus España, resuelto por la Gran Sala del Tribunal Europeo de Derechos Humanos, (TEDH) (17 de octubre de 2019)[193], puso de manifiesto la posibilidad de una videovigilancia oculta cuando estaban en juego intereses del empleador, y el derecho a la intimidad de los trabajadores[194].

Los hechos se refieren a un supermercado en el que se detectaron diferencias entre el inventario de productos y lo facturado en las cajas; por lo que se instalaron cámaras de control de dos tipos: cámaras visibles para grabar posibles robos de clientes (de lo cual fue informada la representación de los trabajadores y los propios empleados), y cámaras ocultas para grabar posibles robos de los empleados, que enfocaban la zona de las cajas. Tras un período de grabación, la compañía citó a los empleados que aparecían implicados en los robos, y todos ellos reconocieron su participación en los hechos. Los despidos disciplinarios fueron impugnados ante la jurisdicción social,

[193] Sentencia consultada, al 14 de diciembre de 2020, en: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-197098%22]}

[194] Convención para la Protección de los Derechos Humanos y de las Libertades Fundamentales. CEDH. “Artículo 8. “Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto a su vida privada y familiar, de su domicilio y de su correspondencia. […]”

siendo el principal argumento de las demandantes que la videovigilancia oculta había vulnerado el derecho a la protección de su intimidad.

Los criterios fundamentales que, a partir del análisis, hizo la gran sala del TEDH, para justificar en el presente caso la videovigilancia oculta y fallar que no hubo violación al derecho a la intimidad de los trabajadores, fueron los siguientes:

- "La medida estaba limitada en lo que respecta a las áreas y el personal que están supervisando […]" En opinión del Tribunal, esta evaluación no puede considerarse irrazonable. Señala que el monitoreo no cubrió todo el taller, sino que se centró en las áreas alrededor de las cajas, donde probablemente se cometieron robos" (párr. 124).
- "La vigilancia por video y las grabaciones no fueron utilizadas por el empleador para ningún otro propósito que no sea rastrear a los responsables de las pérdidas registradas de bienes y tomar medidas disciplinarias contra ellos" (párr. 127).
- "Sobre el alcance de la medida a lo largo del tiempo; si bien el empleador no había establecido de antemano la duración de la videovigilancia, en realidad duró diez días y cesó tan pronto los empleados responsables habían sido identificados. Por lo tanto, la duración de la monitorización no parece excesiva en sí misma" (párr. 126)
- "La existencia de sospechas razonables de que se ha cometido una mala conducta grave comprometida y el alcance de las pérdidas identificadas en el presente caso puede parecer una justificación importante (para la falta de información previa)".
- "Si bien no puede aceptar la proposición de que, en términos generales, la más mínima sospecha de apropiación indebida o cualquier otro delito por parte de los empleados podría justificar la instalación de videovigilancia encubierta por parte del empleador, la existencia de sospechas razonables de que se ha cometido una mala conducta grave […] y el alcance de las pérdidas identificadas en el presente caso puede parecer una justificación importante

(para la falta de información previa) [...] Esto es aún más cierto en una situación en la que el buen funcionamiento de una empresa está en peligro no solo por la sospecha de mal comportamiento de un solo empleado, sino más bien por la sospecha de una acción concertada por parte de varios empleados, ya que esto crea una atmósfera general de desconfianza en el lugar de trabajo".

Cabe señalar, sin embargo, que el año anterior a la sentencia de la Gran Sala, la Sección Tercera del TEDH, el 09 de enero del 2018, falló en sentido contrario, es decir señalando que si se había violado el derecho a la privacidad de los trabajadores, basándose entre otras consideraciones, en que: "los derechos del empresario podrían haberse salvaguardado, al menos hasta cierto punto, por otros medios, en especial informando previamente a las demandantes, incluso de manera general, de la instalación de un sistema de videovigilancia y proporcionándoles la información establecida en la Ley de protección de datos personales" (párr. 69).

En consecuencia, entendemos que la posición preponderante en Europa es a permitir, dependiendo del caso concreto y solo como medida excepcional, una vigilancia oculta, y bajo la exigencia de que se cumplan determinadas condiciones de proporcionalidad y razonabilidad, como las señaladas por la Gran Sala; no obstante, como hemos señalado, el criterio ha merecido variantes.

Lo que sí es indudable, es que los principios rectores de la protección de datos están prestos a ayudar en esta tarea a los responsables de tratamiento, no solo como orientadores sino como normas de ineludible cumplimiento en cada caso.

### 3.2. Principio de Finalidad

El principio de finalidad conforme el artículo 6º de la Ley supone que: "los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o

científico cuando se utilice un procedimiento de disociación o anonimización”
Para poder aplicar correctamente dicho principio, con fines metodológicos, vamos a dividirlo en dos momentos:

-Previo a la recopilación de los datos geolocalizados:

Cuando el empleador va a recopilar los datos geolocalizados de los trabajadores, partiendo de que no requiere su consentimiento; dentro de la información que les dé a éstos, deberán quedar clara o claras las finalidades para las que se tratarán dichos datos. ¿Cómo? Cumpliendo las tres características que deben reunir las finalidades según la Ley: determinadas, explícitas y lícitas.

La finalidad determinada, supondrá que debe ser una finalidad concreta y explícita, como la de señalar que se utilizarán los datos para control laboral, verificando el cumplimiento debido y oportuno de las funciones o actividades que le corresponden al trabajador, el cumplimiento de las instrucciones dadas periódicamente, el tiempo en que las cumpla, durante el horario de trabajo.

La licitud de la finalidad, supondrá que la finalidad deberá ser válida a la luz de la legislación; cumpliendo con dicha licitud el ejercicio del poder de fiscalizar o vigilar del empleador, el que se basa en su poder de dirección, que a su vez se basa en la libertad de empresa y en el derecho de propiedad, cuando corresponda.

Sin embargo, podrían darse supuestos donde se vulnere el principio que estamos analizando, al señalar una finalidad que no sea determinada o explícita, como por ejemplo, cuando el empleador, sumando a los fines de control laboral, señale frases como las siguientes: “ y el cumplimiento efectivo de los fines de la organización del trabajo”; o “ para otros fines análogos” o “para fines similares”.
¿Qué podrán implicar las frases entrecomilladas? ¿qué actividades de tratamiento podrán entrar en ellas?; tal redacción no podría entenderse como una finalidad determinada ni explícita; puesto conforme al artículo 8º del Reglamento, se

considera que una finalidad está determinada “cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales […]”

-Posteriormente a la recopilación de los datos geolocalizados que se venía realizando para una finalidad diferente a la del control laboral:

Esto puede darse en el supuesto en el que el empleador había informado que se ha instalado el GPS en la herramienta de trabajo con fines de seguridad de la misma; en efecto, por ejemplo, se venía tratando los datos de geolocalización del vehículo para poder enfrenar una situación de robo; pero luego decide también tratar dicha información con fines de control laboral. Es decir para una nueva finalidad; lo que podrá hacerlo, previo análisis del caso concreto, pero habiendo señalado adecuadamente y con anticipación la nueva finalidad para la que se tratarán los datos de geolocalización.

Luego de la recopilación de los datos geolocalizados de los trabajadores con fines de control laboral, las actividades de tratamiento a las que estos datos sean sometidos, solo pueden ser aquellas necesarias para cumplir con la verificación de si el trabajador está cumpliendo con las obligaciones derivadas del contrato de trabajo.

El GPS, como lo señala, San José Gras (2020)[195] “como máquina que controle a una máquina (coche/camión/móvil), no cabría plantearnos mayores dudas; el problema está en si el control se realiza sobre la persona del trabajador, entonces podemos incurrir en la intromisión a la intimidad del trabajador”.

Debemos tener en cuenta que al ser el GPS una tecnología invasiva que monitorea permanentemente el lugar y el momento exacto en que el trabajador se encuentra,

[195] Consultado al 05 de noviembre de 2020 en: https://www.agmabogados.com/el-gps-como-mecanismo-de-control-laboral/

va a proveer, por lo general, al empleador de más información a la que está legitimado para la finalidad de control laboral.

Entonces, la conservación o almacenamiento, la organización y el uso en general que le dé el empleador a los datos geolocalizados de los trabajadores, solo podrá realizarse para fines de control y no podrá utilizarlos, por ejemplo, para transferirlos a otras personas naturales o jurídicas que no tengan que ver o participar, legítimamente, con el fin de control laboral. No podrá así transferir dichos datos, a otra persona natural o jurídica, porque el control le corresponde a él, salvo que se trate de un encargo de tratamiento. Situación que ha debido de informar al trabajador[196].

Pero, el GPS en atención a la naturaleza de su funcionamiento y al dispositivo donde se haya colocado, por ejemplo en el vehículo o el celular proporcionados por la empresa, podrá darle al empleador información sobre determinadas conductas y hábitos del trabajador, como podrían ser el conocimiento de los lugares donde come o toma su refrigerio; si almuerza en un lugar público o privado; lugares de paso; frecuencia en que para y va a determinado lugar; si para periódicamente frente a determinado comercio; por ejemplo, la "casa del tabaco", o escoge una ruta donde pasa por una iglesia y hace periódicamente una breve parada frente a determinado local, o suele hacer una parada en una dirección que ha registrado como el colegio de su hijo o el lugar de trabajo de su esposa, etc.

Toda esta información sale del ámbito laboral y tiene que ver con aspectos de su vida íntima o privada, y que pueden abarcar la fe, hábitos alimenticios, relaciones personales, participación en determinadas asociaciones sindicales, políticas, religiosas, defensoras de determinados intereses, etc.

Frente a esto, ¿es lícito que el empleador recoja esta información? y si lo hace por la capacidad del sistema, ¿la debe descartar, es decir suprimir?; desde la protección de los datos personales, con respecto a la primera pregunta la respuesta, en

[196] Como lo dispone el artículo 18 de la Ley.

principio, es que no es lícito, porque se refieren a conductas extra laborales; salvo que esa información se produzca durante la jornada laboral, en cuyo caso deberá, luego de analizada su pertinencia o no para la finalidad de control laboral, suprimirla, según corresponda.

Conservar información personal que no es relevante para la finalidad del control laboral supondría un tratamiento al que no está legitimado y por ende para una finalidad no conocida y, por lo tanto, tampoco autorizada.

Supongamos que el empleador asume que el trabajador al parar con periodicidad frente a la casa del tabaco, es fumador; siendo que a la vez tiene un seguro oncológico donde ha señalado que es no fumador ( quienes pagan una prima más baja con relación a los fumadores). Si el empleador transfiere dicha información de sus trabajadores, a la empresa aseguradora, no constituyendo esta finalidad una autorizada; no solo vulneraría el derecho a la protección de datos personales de su trabajador, sino que podría estar afectando otros derechos, como el de acceder a un seguro de salud y a la intimidad.

¿Podría el empleador usar esta información u otra información geolocalizada para transferirla a otras personas si cuenta con el consentimiento de sus trabajadores?

La respuesta inmediata y en principio sería sí; siempre que cuente con el consentimiento de sus trabajadores. No obstante, nos parece pertinente, el cuestionamiento sobre si ese consentimiento se ha dado libremente o no, teniendo en cuenta la subordinación del empleado en la relación laboral. Podría considerarse que sí, si el empleador le dio la posibilidad de rechazar el consentimiento, sin consecuencias adversas para el trabajador. Consideramos que, de ser necesario, habrá que analizar cada caso.

Sostenemos lo señalado, aunque nuestra legislación peruana sobre la materia, no hace ninguna excepción o exige mayores garantías para otorgar el consentimiento del trabajador, en el ámbito de la relación laboral, para el tratamiento de sus datos

personales para otras finalidades adicionales o no directamente relacionadas con la celebración y ejecución del contrato de trabajo. No obstante, si atendemos a una de las características del consentimiento, como es el de la libertad, y nos encontramos en la asimetría propia de la relación laboral, creemos que de requerirlo las circunstancias, habrá que analizar cada caso concreto.

El empleador recogerá datos geolocalizados pertinentes para ejercer su facultad de control, debiendo usarlos solo para dicha finalidad y no para otra u otras finalidades; sin embargo, por las capacidades del GPS, también recogerá datos geolocalizados que den cuenta de aspectos extra laborales a los que el empleador no podrá darles tratamiento para ninguna finalidad, pues su poder de dirección no lo habilita a tratarlos más allá de la supervisión respectiva. En cuyo caso, de no poder impedir su recopilación, deberá suprimirlos.

Otro supuesto que puede significar la violación del principio de finalidad se puede dar cuando la finalidad legítima e informada se refiere, por ejemplo a la mejora de la productividad, y no a la de control laboral, pero el empleador utiliza los datos geolocalizados legítimamente recogidos para la mejora de la productividad con otra finalidad, que sería la fiscalización o control laboral.

La mejora de la productividad, por ejemplo, para el servicio que presta el personal técnico; así, cuando se rastrea a los técnicos que prestan servicio de asistencia a domicilio y, la empresa según la cercanía de su personal al lugar de la prestación del servicio requerido, lo va asignando o reasignando (en tiempo real) conforme se vayan presentando las situaciones con el fin de brindar una atención más oportuna.

La finalidad del uso de los datos geolocalizados del trabajador no ha sido el del control laboral; no obstante, el empleador ha ido recogiendo datos por ejemplo, de los lugares donde el trabajador va regularmente a almorzar y recoge información que manifiestan que su preferencia culinaria se inclina por la comida mexicana, por lo que va con regularidad, con el vehículo o el celular que tiene asignado por la

empresa durante su hora de refrigerio, a un restaurant del tipo de comida señalado, pero que, por el lugar de la ubicación de dicho comercio, le exige alejarse un poco más de la zona donde está asignado a prestar sus servicios técnicos durante el horario de la jornada, sin constituir esto un incumplimiento laboral.

El empleador, que conoce por la geolocalización donde almuerza el trabajador, considera que sería más conveniente, para cualquier eventualidad, como la de congestión vehicular, que el trabajador escoja restaurantes más cercanos a la zona (ruta) de atención que le corresponde, y le envía una comunicación "memorándum" haciéndole dicha recomendación, dándole inclusive opciones de restaurantes, con el fin de prevenir y evitar un posible incumplimiento de sus funciones. El empleador habría accedido a información personal íntima (preferencias culinarias) que implicarían un control del comportamiento del trabajador para prevenir una posible afectación en la productividad. Tratamiento que excedería a la finalidad de mejora de la productividad explicitada.

Es preciso recordar que la definición del principio de finalidad, exige que se trate también de una finalidad que sea lícita; por lo que se desprende que este principio también esté relacionado con el de legalidad, y por ende con el respeto de todos los derechos fundamentales del trabajador.

Vamos viendo como un tratamiento indebido de los datos personales de los trabajadores por medio del GPS , puede afectar diversos derechos de la persona del trabajador, aunque lo que se pretenda controlar no sea a la persona del mismo, sino al cumplimiento de sus deberes laborales; pero al hacerlo, con la tecnología señalada, en una herramienta (o dispositivo) de trabajo que usa el empleado, se va a captar más información sobre su persona; y con ello, en el proceso de recopilación y tratamiento de sus datos personales geolocalizados pueden quedar afectados otros derechos.

En tal sentido, la afectación para el trabajador podrá ser más amplia, como lo señala

González Ortega:

> No es solo el derecho a la intimidad personal y familiar y a la propia imagen sino, más ampliamente, a la reserva de todo dato mediante el cual se pongan de manifiesto hábitos, comportamientos, actitudes personales, relaciones y actividades; es decir, circunstancias que pertenecen al espacio de privacidad que debe ser tutelado frente a invasiones no consentidas. Mucho más cuando el hecho de que tales datos personales puedan ser tratados digitalmente incrementa la agresividad de la obtención del dato en la medida en que ese tratamiento puede contribuir de forma decisiva, merced a su capacidad de acumulación y de combinación de la información, a ofrecer una imagen, extremadamente detallada de la persona de que se trate . Imagen que así obtenida, invade sin duda los espacios protegidos por el derecho a la intimidad, o si se quiere, de la vida privada. Todo ello como una manifestación de respeto al más genérico valor de la dignidad humana, constitucionalmente reconocido […] como soporte y condensación de todos los derechos fundamentales. (2019: 58)

Por eso, los datos geolocalizados deben recopilarse limitándose a lo estrictamente necesario para lograr la finalidad legítima de control laboral.

El principio de finalidad va a acompañar todo el ciclo de vida del dato geolocalizado desde la recogida hasta su supresión. Por ello, cuando el dato geolocalizado haya cumplido la finalidad de verificar el cumplimiento de las obligaciones laborales de los trabajadores deberá suprimirse, sin que el empleador, como titular del banco de datos requiera que el trabajador, como titular del dato, ejerza su derecho de cancelación. Esto supone que el empleador ha debido de establecer los lineamientos, pautas o protocolos para que esto se ejecute. Cumplida la finalidad del tratamiento del dato localizado, queda agotada la legitimidad del empleador para seguir con su tratamiento.

Otro aspecto importante con relación a la finalidad, que es la que se estableció en la información que el empleador debió dar a su trabajador antes de proceder a recopilar sus datos geolocalizados, es determinar si por medio de los datos geolocalizados se ha confirmado que el trabajador ha incumplido sus funciones laborales y merecerá

ser sometido a un procedimiento disciplinario que podría traer como consecuencia una sanción; pudiendo llegar a ser una falta grave que justifique su despido.

¿Cuándo el empleador podrá aplicar una sanción al trabajador en virtud de los datos geolocalizados?; cuando ello se ha establecido como una de las finalidades del tratamiento; es decir ha debido quedar claramente especificado que los datos geolocalizados podrán ser utilizados para identificar infracciones y de ser el caso sancionar conforme a la ley laboral.

La descripción de la finalidad de fiscalizar para sancionar, debe quedar claramente determinada para que el empleador pueda tratar la información geolocalizada del trabajador con ese fin. El tratamiento queda vinculado a las finalidades determinadas, explicitas y lícitas de las que se informó previamente al trabajador y además dicha información ha debido darse de una manera clara, expresa, indubitable y con lenguaje sencillo, como lo señala el Reglamento en el artículo 12.

El conocimiento cabal de la finalidad con la que se van a tratar nuestros datos personales es fundamental para ejercer la facultad de control que le corresponde al titular del dato; facultad que está en el contenido esencial del derecho a la protección de datos personales.
Una información deficiente o incompleta sobre la finalidad del tratamiento puede convertir en ilegal y abusiva la gestión de la información por parte del responsable del tratamiento.

Lo señalado, se pone de manifiesto en el Procedimiento sancionador N.º: PS/00112/2015 llevado a cabo por la Agencia Española de Protección de Datos. La empresa VALMICS 2000 SL realizó el despido disciplinario por falta muy grave, fundamentado en datos recogidos por un dispositivo GPS instalado en el móvil de un trabajador.

La empresa informó que el denunciante, en su calidad de Jefe de Explotación y Ventas de VALMICS, tuvo conocimiento de la instalación del sistema GPS instalado en su

teléfono móvil y en el del resto de trabajadores.
El sistema estaba operativo únicamente durante la jornada laboral; y la información e instalación de éste tuvo lugar en reunión celebrada al efecto en la que se encontraban presentes los trabajadores de la empresa, entre ellos el propio denunciante, y en la que por el técnico que instaló dicha aplicación, se explicó a todos ellos la instalación y funcionamiento de la misma, a fin de facilitar su labor de comercialización con los clientes. En la referida reunión, se firmó un documento por todos los asistentes, incluido el propio denunciante, en el que se les informaba sobre el sistema de localización GPS.
La aplicación fue instalada en cada uno de los móviles de los trabajadores tras facilitar todos ellos al técnico instalador el PIN o clave de acceso a su teléfono móvil.

Asimismo, se señala que de todo ello fue perfecto conocedor tanto el denunciante como su esposa, que también trabajaba en la empresa y conocía la existencia del dispositivo GPS; pues además, era la encargada de llamar a los trabajadores tras ser localizados con dicha aplicación para dar instrucciones sobre determinadas peticiones de clientes, facilitando así las labores de comercialización.

En el procedimiento, se determinó que dicho documento no contenía relación alguna del posible uso para el control laboral, ámbito de control, o efectos disciplinarios, sus consecuencias, o el modo de ejercicio de derechos sobre dichos datos. Según manifiesta la denunciada; la finalidad del geolocalizador era la de facilitar su labor de comercialización con los clientes.

El denunciante no tenía conocimiento de que mediante el sistema de geolocalización se permitiría un continuo y permanente seguimiento del dispositivo móvil que portaba como empleado, en sus trayectos; facilitando no sólo el posicionamiento de éste por razones de fácil contacto con clientes o comunicación de labores en el momento, sino también el lugar exacto en donde se hallaba como trabajador y, a su vez, del posterior tratamiento de los datos obtenidos con una finalidad no informada al afectado denunciante y que sirvió, en parte, para formular y apoyar su despido disciplinario

La autoridad española no cuestiona el poder de vigilancia y control del empresario sobre el cumplimiento de las obligaciones del trabajador ; pero recuerda que su ejercicio, de igual modo que, incluso, el de los derechos fundamentales no es absoluto, sino que tiene límites que no pueden traspasarse so pena de resultar abusivo e ilícito.

El tratamiento de los datos geolocalizados puede resultar lícito al estar, en principio, amparado en la Ley; inclusive puede resultar eventualmente, en el caso específico de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, no obstante, deberá asegurar también la debida información previa.

La AEPD señala que “la prestación laboral de servicios no entraña la inmunidad de la facultad de control de que dispone el empresario a la ineludible necesidad de garantizar los derechos fundamentales y libertades públicas del trabajador”.

El sistema GPS instalado en el móvil que la empresa cedió al denunciante por teóricas razones de facilitar el contacto y las labores, se utilizó, en realidad, sin previo aviso, ni información al afectado, para conocer y tratar luego los datos relativos a los lugares en que estuvo en cada momento mientras se movía por las zonas de las visitas programadas.

El hecho de que al denunciante se le instalara un sistema de geolocalización y conociera o permitiera dicha instalación no supone que haya sido informado de los fines de control laboral a que iba a ser sometido. Si no se tiene la información que los datos van a ser utilizados para control laboral, pudiendo llegar a ocasionar un despido o expediente disciplinario, no hay modo de que los empleados sepan a qué atenerse. Igualmente, como ocurrió en el presente caso, se acreditó que la información a efectos de autodeterminación informativa (quién tiene los datos, con qué finalidad y usos) no daba cuenta sobre el mecanismo de ejercicio de derechos a los empleados, con lo cual se le impidió el control sobre su la información que le concernía.

### 3.3. Principio de Proporcionalidad

El principio de proporcionalidad establece límites con relación a los datos personales que el titular del banco de datos vaya a usar; así como para las actividades del tratamiento a realizar con dichos datos; estos límites están en función a la finalidad o a las finalidades autorizadas desde antes de la recopilación de los mismos.

¿Cómo debería delimitarse el uso de los datos personales geolocalizados de los trabajadores y las actividades de tratamiento para ejercer el control laboral a cargo del empleador?,

La Ley utiliza tres calificativos, señalando que debe ser: adecuado, relevante y no excesivo a la finalidad.

Por la proporcionalidad el empleador deberá tener como norte de su actuación, en su calidad de responsable del tratamiento, la finalidad autorizada: que es la de ejercer su facultad de control laboral, la que ha debido estar detallada de manera determinada y explícita en la información que ha dado a sus trabajadores, previo a la recopilación de sus datos localizados.

Para los efectos señalados, deberá actuar no sólo a la luz del principio de proporcionalidad, sino también del de legalidad y el de finalidad, puesto que otra vez, en el caso de éste último, viene explicitado y vinculado con el de proporcionalidad.

El empleador deberá tener en cuenta, lo siguiente:

-La información personal que le proporcione el GPS debe ser la estrictamente necesaria para controlar a los trabajadores, que es la finalidad legítima establecida. Por lo que solo deberá tratar la información que sea apropiada e importante para el control laboral.

Pero por la tecnología utilizada, si el GPS está en el vehículo de la empresa asignado al trabajador para el cumplimiento y por ende el control de su actividad laboral; el empleador sabrá en todo momento dónde se encuentra el vehículo y por ende la persona del trabajador que lo posee y usa. Podría, además, conocer conductas del trabajador al volante; tales como el número de paradas, el tiempo de las mismas, los lugares de las paradas, la velocidad, etc.

Si el GPS está en el celular del trabajador, podrá saber con mayor exactitud los lugares en los que ha estado, independientemente de aquéllos que son parte de su recorrido formal del servicio; el GPS, brindará información sobre los lugares visitados, y el tiempo en ellos, pudiendo referirse a los lugares donde el trabajador realiza actividades que pertenecen a su espera privada o íntima, como podría ser: lugares de comida, centro de salud, locales de culto, comercio específico, edifico o dirección particular que puede corresponder a una oficina de una asociación sindical, partidaria, ambientalista, de diversa ideología, etc.

Supongamos que dentro de los datos localizados, el empleador ha almacenado, una dirección particular donde el empleado suele ir a la hora de refrigerio con regularidad, no apareciendo esta dirección como la del domicilio que ha dado el trabajador al empleador desde el inicio de la relación laboral y que aún mantiene como vigente. Ocurre que estando el trabajador de vacaciones, y no encontrándose nadie en su domicilio consignado en la empresa, el empleador opta por dejarle al trabajador una comunicación escrita en esa dirección que obtuvo del sistema GPS instalado en su celular, pero que no es la que ha proporcionado el trabajador.

Independiente de lo que contesten en esta dirección, indebidamente usada para dejar comunicaciones para el trabajador, eso demostraría que el empleador está no solo recopilando datos excesivos por la geolocalización con fines de control laboral, sino que los está usando para una finalidad distinta a la establecida; con lo cual no sólo se afecta el derecho a la protección de dato personales, sino que también la intimidad del trabajador y eventualmente la violación del derecho a la protección de datos personales del propietario de esa dirección usada como domicilio del

trabajador, sin serlo.

Ante esta información excesiva debe establecerse la desactivación del GPS, en horas fuera de la jornada laboral; o de ser otro el caso, es decir, que el trabajador tiene permitido la realización de actividades privadas con límites dentro de la jornada laboral, establecerse el procedimiento adecuado para que esta información sea suprimida, porque es excesiva con relación a la finalidad de control y por ende desproporcionada.

Si el trabajador pidió permiso para una atención de salud, para recoger a un hijo del colegio o de otra actividad, o para cualquier otro tema personal, el empleador podrá, en virtud al GPS, saber el lugar y la hora del día en donde se encontraba durante ese tiempo extralaboral. Lo cual es una información excesiva y no relevante, para la finalidad de control, siendo que además es obtenida fuera de la jornada laboral, por causa de un permiso.

Si el vehículo lo lleva el trabajador a su domicilio y/o el celular lo tiene, como es lo normal las 24 horas, y en ambos bienes de la empresa el GPS está activado las 24 horas; entonces, sin duda alguna, el empleador conocerá no solo los datos señalados en los párrafos precedentes, durante la jornada de trabajo, y que serían pertinentes para el control laboral, sino mucha otra más información personal; como los lugares a donde va fuera del horario laboral, donde pernocta, locales donde compra, o donde le prestan un servicio determinado, así como la periodicidad de su asistencia a los mismos, etc. constituyendo esto no sólo un tratamiento desproporcionado sino ilegal.

A modo de ejemplo, analicemos determinados supuestos:

-Si el GPS está en el vehículo de la empresa pero debe dejarlo en sus instalaciones, al final de la jornada laboral; habiéndose establecido, la finalidad de control laboral sobre los datos geolocalizados. Si el trabajador cumple sus funciones laborales fuera de las instalaciones de la empresa, podría darse el caso que utilice algunos

momentos como los de refrigerio o de descanso, permitido, o inclusive, durante el horario de trabajo, ir de paso, a lugares extralaborales, sin faltar a sus deberes derivados del contrato de trabajo; como comprar en una farmacia, recoger un encargo personal, o parar frente a una iglesia o en un lugar donde venden apuestas de caballos, o expenden un tipo de alimentos, entre otros.

Si el empleador conoce de estas circunstancias y las tolera, pues no está explícitamente prohibido, y se da dentro de los usos laborales en esta forma de trabajos, entonces no podría a través de los datos geolocalizados sancionar a su empleado que en algunos momentos de la jornada laboral pueda atender estas actividades privadas.

El tema radica en que el empleador accederá a información personal que no es adecuada ni relevante y por lo tanto será desproporcionada, para ejercer su potestad de fiscalizar a su trabajador. Por lo que deberá tomar las previsiones para proceder a cancelar dicha información personal.

En todo caso, al tratarse de un trabajador que cumple sus servicios fuera de las instalaciones de la empresa; sea como chofer, sea como vendedor, repartidor, técnico de asistencia, visitador médico, o similares, habrá que analizar en cada caso esta circunstancia, dentro de los lineamientos claros que la empresa ha dado para el cumplimiento de la jornada laboral en adecuación a la legislación sobre protección de datos personales.

-El GPS está en el vehículo de la empresa pero el trabajador debe tenerlo las 24 horas del día con él.

Además de lo señalado en el supuesto anterior, y si el trabajador está facultado para el uso del vehículo fuera del horario de la jornada laboral, e inclusive llevárselo a casa; el empleador tendrá acceso a más información personal que corresponderá a tiempos propios de la intimidad y privacidad del trabajador, y donde sin duda el empleador no está legitimado para conocer ni para controlar; podrá conocer los

lugares a donde se dirige, aproxima o asiste de noche, donde pernocta; lugares donde pasa o va el fin de semana; el tiempo que permanece en los mismos y la frecuencia con la que se dirige a ellos; tales como lugares de culto religioso; de diversión: cine, teatro, bares, casinos; donde se practica algún deporte; centros de salud; etc.

En este supuesto, dicha información sería excesiva para el fin laboral establecido y vulneraría el derecho a la protección de datos personales y otros derechos como a la intimidad personal o familiar, e inclusive a su libre desarrollo y bienestar; pues habrá alguien que, sobre el trabajador, puede conocer sus movimientos permanentemente y hasta monitorizarlo; lo que supondría un tratamiento desproporcionado e ilegal.

Podríamos preguntarnos, pero si el vehículo es de la empresa, es legítimo que tenga el GPS para para fines de seguridad de dicha unidad; esto es cierto; pero también es cierto que al estar asignado a un trabajador, se recopilará información personal no adecuada, excesiva e irrelevante para el fin de seguridad del vehículo. En este caso, y fuera del horario laboral, la finalidad considerada legítima será la de seguridad de la unidad; pero definitivamente no operará la finalidad de control laboral; no obstante, se estarán recopilando datos geolocalizados que darán cuenta de parte de la vida privada o íntima del trabajador.

Ante esta circunstancia creemos que sería ajustado a la normativa de protección de datos personales, sin perjuicio del análisis que correspondería a cada caso concreto, que se le informe al trabajador que al usar el vehículo fuera del horario laboral, se estarán recopilando datos de los lugares a donde él va con el vehículo asignado, debiendo ser consciente de ello y autorizando a dicha recopilación, pero sólo en tanto tenga relevancia para la finalidad de seguridad del vehículo y dándosele las garantías de que esa información será tratada conforme a la Ley y al Reglamento; lo que incluye que será suprimida, superada la finalidad de seguridad y no tratada para ninguna otra finalidad.

Con relación al consentimiento del trabajador, para la activación permanente del GPS, más allá de la jornada laboral; en principio, esto sería desde nuestra legislación

aceptado. No obstante, sobre este punto, reiteramos que en atención a la relación asimétrica y por ende posición subordinada del trabajador, el consentimiento podría cuestionarse, a menos que se haya dejado constancia de que su negativa no le acarrearía resultados o consecuencias adversas.

Otra posibilidad, y nuevamente señalamos la importancia de ubicarnos en el caso concreto, es que ante la misma situación, el empleador y el trabajador, prioricen el respeto al privacidad de este último; ante lo cual, el empresario deberá implementar un mecanismo que limite su acceso a esta información extra laboral. Por ejemplo, que el GPS solo se encuentre activado durante la jornada laboral. Una forma es capacitar al trabajador para que desconecte el GPS al fin de la jornada laboral, u otra es que se disponga y programe que el sistema se desactive al concluir el horario de trabajo. También podría optarse por implementar, que la información de localización se active para ser visualizada si el vehículo sale de determinadas zonas consideradas seguras. De todo ello, tiene que estar informado el trabajador.

Reiteramos que de aceptarse, con todas las salvaguardas que el GPS permanezca activado durante las 24 horas en el vehículo, deberá garantizarse que la información extra laboral y privada del trabajador será cancelada y por supuesto, limitarse a usar los datos geolocalizados para la finalidad de seguridad del vehículo de la empresa y en ninguna circunstancia a la finalidad de control laboral. Procediéndose a eliminar los datos impertinentes para la finalidad de seguridad del vehículo fuera del horario de la jornada laboral.

Veamos el caso resuelto por los tribunales españoles sobre un despido basado en los reportes del GPS instalado en el vehículo que la empresa proporcionó a su trabajador .El tribunal superior de justicia confirma la ilicitud del despido, determinado por la primera instancia, porque el empleador no respetó la normativa de protección de datos personales, al haber afectado el deber de información sobre las condiciones y alcances del tratamiento del GPS, así como el principio de finalidad e inclusive el principio o test de proporcionalidad.

El caso fue visto por el Tribunal Superior de Justicia, Sala de lo Social, STSJ M 3074/2014 y emitió la Resolución N°: 260/2014. El actor, era un empleado que venía prestando servicios por cuenta de la empresa REDES INTERMEDIACION FINANCIERA en la categoría profesional de Gestor de Cuentas. Las funciones encomendadas al actor consistían en pasar por determinadas gasolineras a fin de promocionar la venta de productos financieros (tarjetas de crédito). Cronológicamente los hechos relevantes son los siguientes:

-El 25/04/12 la empresa, para el desempeño de las funciones, puso a disposición del actor un vehículo modelo Volkswagen Golf matrícula 0930HLB. Este vehículo llevaba instalado un Sistema de Gestión de Flotas de la compañía DETECTOR, S.A. Este sistema permitía la localización y seguimiento continuo del vehículo mediante un dispositivo GPS.

-El 25/06/12, la empresa comunicó al actor el "documento de uso de empresa', con la firma del trabajador como cesionante del vehículo, declarando estar de acuerdo y asumiendo los siguientes puntos sobre la cesión del automóvil de empresa: 1. El vehículo es un elemento que la empresa cede para el uso profesional del cesionario, en ningún caso, parte del salario. 2. La responsabilidad del mal uso del vehículo es exclusivamente del cesionario. 3. Las infracciones de tráfico, accidentes u otros percances que no cubra el seguro del vehículo serán responsabilidad personal y económica del cesionario. 4. La cesión del vehículo durará, como máximo, el tiempo de relación laboral del cesionario con Redes de Fuerzas de Ventas, pudiendo la empresa, reclamar la entrega inmediata del mismo, sin haber terminado la relación laboral. La devolución del vehículo se podrá reclamar sin previo aviso. 5. Es responsabilidad del cesionario mantener el vehículo en perfecto mantenimiento, siguiendo las instrucciones del fabricante, y efectuando las revisiones periódicas en centros autorizados. 6. El uso del vehículo es exclusivo del cesionario, no pudiendo hacer uso de él ningún otro conductor que no sea éste. 7. El uso del vehículo de la empresa obliga al cesionario a mantenerlo en un estado de limpieza y decoro que no perjudique a la imagen de Redes de Fuerzas de Ventas; instrucciones exhaustivamente detalladas que, sin embargo, como lo hace notar la Sala, no hacen

referencia alguna a la instalación de un sistema de localización por GPS, al que únicamente alude la comunicación de 24 de julio de 2.012, esto es, un mes después.

-El 24/7/12, un mes después de comunicar las condiciones de uso, la empresa recién le informa al trabajador, sobre el GPS: “Con motivo del nuevo cambio de vehículo de Empresa y para mayor seguridad tanto del vehículo como del usuario, hemos instalado un GPS avalado por el Cuerpo Nacional de Policía. Como ya es de su conocimiento el vehículo que tiene en su poder es exclusivamente para uso laboral, por lo que su utilización para fines personales está prohibido, tal y como se expone en el documento de cesión de vehículo” según documento del 25/06/12, mediante la cual, la empresa comunicó al actor el documento de uso. Como se observa es recién el 24 de julio, que el trabajador fue informado del GPS en el vehículo.

-07/09/12 la empresa comunicó al actor su despido disciplinario. Las causas del despido se basan en unas conductas, todas ellas sustentadas en lo que la empresa afirma ser el resultado de la localización y seguimiento del automóvil que le cedió para uso profesional, “las cuales se sitúan cronológicamente en el abanico que va de 25 de junio a 23 de julio de 2.012, ambos inclusive, siendo así que no obstante haberle facilitado el nuevo automóvil el 25 de abril, poniendo en su conocimiento el 25 de junio de ese año con notable pormenor las condiciones de su uso, no le comunicó, empero, la instalación de tan repetido dispositivo de localización hasta el 24 de julio de 2.012”.

La empresa demandada señaló que su finalidad no era otra que propiciar una mayor seguridad del coche y del usuario. “Es más, tal como dice el documento aportado por la demandada […] se trata de sistema de seguridad dirigido a la "localización de vehículos robados" que "localiza, hace seguimiento y recupera tu vehículo ". En otras palabras, nada más lejos de la finalidad para la que, a la postre, se destinó.

En la presente Resolución no se cuestiona el poder de vigilancia y control del empresario sobre el cumplimiento de las obligaciones del trabajador no obstante es indispensable que “su ejercicio, de igual modo que, incluso, el de los derechos fundamentales no es absoluto, sino que tiene límites que no pueden traspasarse so

pena de resultar abusivo e ilícito", remarca la Sala. Reiterándose además, que el empleador como responsable del tratamiento, debe asegurar la debida información previa.

Se señala que en el presente caso el "GPS para obtener datos sobre la forma de desempeñarse profesionalmente el demandante como Gestor de Cuentas infringió la Ley Orgánica de Protección de Datos de Carácter Personal y, a su vez, su derecho fundamental a la intimidad personal".

Sobre la violación de la intimidad del trabajador, en este caso, la Sala desarrolla en el fundamento decimosexto, lo siguiente:

> En efecto, si el vehículo que la demandada cedió al trabajador para uso exclusivamente profesional sólo podía ser utilizado por él y, además, debía permanecer siempre bajo su custodia, mantenimiento y cuidado, cuantos datos se conecten a su manejo y, por ende, a su localización y desplazamientos fuera del centro de trabajo, se proyectan refleja, pero ineluctablemente, sobre la forma de proceder del usuario, que no es otro que el conductor, permitiendo de este modo conocer en todo momento durante su uso parcelas de la vida del trabajador que por muy imbricadas que estén en el desarrollo de la relación laboral con la empresa inciden potencialmente en la esfera de su derecho a la intimidad personal y, de ser objeto de tratamiento como aquí sucede, del que igualmente le asiste a la protección de datos de tal carácter. Como veremos, así lo tiene entendido la doctrina constitucional y la del Tribunal Europeo de Derechos Humanos.

Abundando en la capacidad invasiva del GPS, la sentencia tiene en cuenta que la posibilidad de conocer en todo momento, mediante un sistema de geolocalización que permite un continuo y permanente seguimiento del vehículo durante su uso, no sólo el posicionamiento de éste por razones de seguridad, sino también el lugar exacto en donde se halla el trabajador y, a su vez, el posterior tratamiento de los datos obtenidos y para una finalidad completamente distinta de la anunciada, que era la de seguridad, y por ende, sin conocimiento del trabajador- conductor, hacen que "las conclusiones extraídas merced a dicho dispositivo tecnológico y su aportación como medio de

prueba en sede judicial para demostrar un pretendido incumplimiento contractual constituyan un procedimiento que lesiona los derechos fundamentales".

De otro lado, en el fundamento vigesimoséptimo, la Sala establece que el seguimiento por el GPS del trabajador no supera los juicios de necesidad, idoneidad y proporcionalidad:

> […] en cuanto a los cánones constitucionales de enjuiciamiento del dispositivo de localización utilizado, que en modo alguno supera los juicios de necesidad, idoneidad y proporcionalidad, por cuanto que si lo que quería demostrar la empresa era que algunos días el trabajador no agotó la duración de su jornada laboral, o utilizó en una ocasión para uso propio el vehículo que le había facilitado, o no tenía que haber pasado gastos de comida otros días en que después de comer regresó sin más a su domicilio, se trata de hechos que pudieron ser probados sin ninguna dificultad por otros medios mucho menos aflictivos e intrusivos en la esfera de su intimidad personal y vida privada.

Como hemos señalado, ante una medida restrictiva de derechos fundamentales y a través de una tecnología invasiva como la del GPS, una de las primeras evaluaciones que debe realizar el responsable del tratamiento, es el test de proporcionalidad; para que superado el mismo, pueda implementar dicha medida, dentro del marco de la normativa sobre protección de datos personales y en atención al respeto de los demás derechos fundamentales de la persona, en este caso el trabajador, cuya actividad laboral se va a supervisar; pero que, en atención a la tecnología utilizada, se recopilarán, y por lo tanto tratarán más datos de los necesarios, debiendo tomarse las salvaguardias que correspondan a cada caso concreto.

En el supuesto de que el vehículo se quede con el trabajador y éste tiene expresamente prohibido, su uso para fines extra laborales y fuera del horario de la jornada laboral, con conocimiento de las consecuencias de incumplir ello; en el caso de violar esta prohibición, el empleador podrá utilizar los datos geolocalizados fuera de la jornada laboral para aplicar las medidas disciplinarias correspondientes.

-Si el GPS se encuentra en el celular del trabajador, el tema de la invasión al ámbito de la intimidad es más elocuente al ser un dispositivo que permanece siempre en posesión de la persona. En este caso, si nos parece que el GPS instalado en el móvil, para fines de control no tendría sustento para permanecer activo más allá de la jornada laboral, tampoco por fines de seguridad del dispositivo mismo, en atención a su valor.

-La proporcionalidad, exige también, que se opte siempre por los mecanismos menos invasivos para los derechos del trabajador. Pongamos un caso.

¿Qué pasa si el empleador le entrega a sus trabajadores un reloj donde instala el GPS para controlar el cumplimiento el horario de trabajo?, lo que sin duda es parte de los deberes del trabajador; es decir quiere controlar el cumplimiento del ingreso y salida del empleado a las instalaciones de la empresa e inclusive puede pretender supervisar el cumplimiento del no ingreso a zonas restringidas de la empresa.

El empleador, como responsable del tratamiento, ha debido, en primer lugar, aplicar el principio constitucional o test de proporcionalidad, con sus tres subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto, pues estamos frente a una medida que restringe derechos fundamentales. El uso del GPS para el control horario y el acceso a zonas restringidas dentro de las instalaciones de la empresa y además en un reloj que lo lleva consigo constantemente el trabajador, no superaría el subprincipio de necesidad, pues existen otros mecanismos o tecnologías menos invasivas para cumplir dicho fin, como el reloj marcador de entrada o salidas o, en su caso, el de la videovigilancia.

Los datos geolocalizados que reportarán los relojes serán más de los necesarios, por lo tanto excesivos para el control horario de ingreso y salida y de acceso o no a las zonas restringidas, afectándose con ello el principio de proporcionalidad.

Si el trabajador cumple funciones fuera de las instalaciones de la empresa, como regla, podría utilizarse el GPS instalado en el celular o en el vehículo, según sea el caso, como un mecanismo de controlar el cumplimiento del horario de trabajo.

Desde el punto de vista de la protección de datos debemos llegar a evaluar y ponderar cada supuesto de limitación de un derecho frente a una tecnología como la del GPS con fines de control. Así, por ejemplo, si la empresa le ha proporcionado a su chofer el vehículo y el celular, ¿dónde deberá instalar el sistema de geolocalización para el control horario?; en el presente supuesto, debería hacerlo en el vehículo, en atención a la naturaleza del puesto que ocupa, la de chofer; por lo que su instrumento de trabajo es el vehículo proporcionado por la empresa.

Lo señalado, no obsta el tener en consideración que si el trabajador debe recoger el vehículo de las instalaciones de la empresa, el tiempo que le tomó, estando ya en dichas instalaciones, para llegar y luego dejar el vehículo debería ser contabilizado dentro de su tiempo de trabajo cumplido. Será necesario analizar cada supuesto.

Pero, supongamos que el empleador lo instala en el celular del chofer. El celular le brindará mayor información personal del trabajador que la que le proporcionaría si estuviera instalado en el vehículo; siendo suficiente en este caso que el GPS se encuentre en el vehículo, para controlar el cumplimiento de la jornada de trabajo. De optarse por el control horario por el GPS del celular, según sea el caso, debería desactivarse el mismo, luego de la marcación respectiva.

Como lo señala González Ortega “la geolocalización, no puede ser un objetivo en sí mismo, sino exclusivamente una consecuencia indirecta de una medida necesaria e imprescindible para garantizar el funcionamiento eficiente de la empresa y para proteger la producción, la salud o la seguridad” (2019:59).

El responsable del tratamiento, el empleador, a la luz de la normativa sobre protección de datos personales siempre debe evitar recopilar información que exceda lo necesario y resulte desproporcionada para la finalidad autorizada. En la línea de lo señalado, en el artículo 132 del Reglamento de la Ley, se tipifica como falta leve el “Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las

que requieren ser obtenidos" lo que será considerado falta grave, si dicho tratamiento indebido recae sobre datos sensibles.[197]

La Autoridad Nacional de Protección de Datos Personales en la opinión consultiva OC 6, contenida en el Oficio Nº 611-2014-JUS/DGPDP, señala que "el procesamiento de datos personales (sea recopilar o transferir) implica respetar los principios de la LPDP ya enunciados, a fin de que dichos tratamientos se limiten a aquellos que son necesarios, pertinentes y no excesivos a las finalidades autorizadas".

El empleador como responsable del tratamiento es el que deberá implementar todas las medidas necesarias para cumplir con la normativa sobre protección de datos; y además, estar en capacidad de demostrarlo.

### 3.4. Principio de Calidad

Como desarrollamos en el capítulo 1.1.6.2, el principio de calidad supone abordar su cumplimiento desde cuatro aspectos. Que los datos sean:

a) Veraces, exactos y en la medida de lo posible actualizados;

b) Necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados;

c) Deben conservarse de forma tal que se garantice su seguridad; y

d) Deben conservarse solo por el tiempo necesario para cumplir con la finalidad del tratamiento.

Abordaremos estos aspectos de la calidad desde el tratamiento de los datos geolocalizados de los trabajadores para fines de control laboral.

[197] Ley: artículo 2, inciso "5. Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual". Reglamento: Artículo 2, inciso "6. Datos sensibles: Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad".

a) Con respecto a la veracidad y exactitud del dato, al tratarse de datos geolocalizados, en atención a la naturaleza del sistema de geo posicionamiento satelital, la información captada refleja o reporta un hecho objetivo independiente de la voluntad del trabajador, como titular de la información. El tema de la actualización del dato deberá manejarse en relación con la finalidad de control laboral y el tiempo que tiene el empleador para hacer efectiva su facultad de control con relación a lo que ha recogido el GPS.

Si en virtud a dicho sistema, el empleador logra identificar una falta, deberá tomar en consideración, no sólo la legislación sobre protección de datos personales; sino también, la legislación laboral para poder ejercer su facultad disciplinaria, que entre otros aspectos establece el principio de inmediatez para despido por falta grave por ejemplo, según el artículo 31º del TUO de la Ley de Productividad y Competitividad Laboral.

b) Que los datos sean necesarios, pertinentes y adecuados respecto de la finalidades para la que fueron recopilados e informadas a los titulares de los datos; supone que desde antes de la recopilación de los datos geolocalizados de los trabajadores, el empleador haya definido con claridad la finalidad de control laboral y las actividades de tratamiento que ella implicará; de allí la importancia del principio de finalidad que exige que la misma debe ser descrita de manera determinada, explícita y lícita, pues esto es lo que marcará el uso y destino de los datos geolocalizados y permitirá, a su vez, descartar cualquier actividad de tratamiento y dato no necesario ni adecuado para la finalidad de control establecida.

Lo señalado es particularmente necesario no sólo de tener en claro, sino para establecer los mecanismos para su debido cumplimiento, pues tratándose del uso del sistema GPS, en atención a su naturaleza y capacidad, suele monitorizar de manera permanente el lugar y el momento en que se encuentra el trabajador mientras

esté con el sistema activado. Lo cual es durante la jornada laboral o inclusive fuera de ella, pudiendo llegar hasta ser las veinticuatro horas de los siete días de la semana, como podría darse al perseguir fines de seguridad, más no así de control laboral .

Ante este hecho, el responsable del tratamiento debe establecer salvaguardas para recopilar solo los datos necesarios y pertinentes para ejercer su facultad de control, la que no puede ir más allá de la jornada laboral ni abarcar espacios extra laborales. Dichas salvaguardas pueden traducirse en políticas de tratamientos de los datos personales en general y en especial de los datos geolocalizados; en protocolos sobre el tratamiento de este tipo de datos y capacitación del personal que lleva este sistema instalado en el dispositivo que usa, por ejemplo para saber desactivarlo durante sus horas de descanso, de refrigerio, de permiso o, de ser el caso fuera de la jornada laboral si sigue con el dispositivo con GPS.

No obstante a pesar de las salvaguardas que puedan adoptarse, es factible que durante la jornada de trabajo se capten datos innecesarios para el control laboral perseguido, como datos vinculados a su intimidad o privacidad, como ya hemos mencionado, datos que individualmente o relacionándolo con otra información que el GPS haya proporcionado en oportunidades anteriores, pueden brindar información intima del trabajador que es totalmente impertinente para la finalidad de control, entre otros muchos supuestos.

En la circunstancia descrita, el empleador deberá haber implementado un protocolo de cancelación de dicha información que deberá cumplir el personal que interviene en el tratamiento de esta información, porque de no hacerlo, no tendría datos de calidad en su banco de datos, violando el principio referido.

Además, el solo mantenimiento o conservación de dicha información impertinente y no adecuada para la finalidad establecida, supondría un tratamiento excesivo y para un fin distinto al autorizado.

No bastaría que el empleador establezca un protocolo o una política de gestión que incluya la supresión de datos impertinentes o, en su caso excesivos, sino que debería establecer, como parte de ese protocolo auditorías y revisiones periódicas de su cumplimiento.

Recordemos que la calidad y todos los principios de la protección de datos deben observarse durante todo el ciclo de vida y durante todas las actividades del tratamiento del dato personal, en general, y por supuesto del dato geolocalizado del trabajador.

En el mismo sentido, la Autoridad Nacional de Protección de Datos Personales lo ha manifestado en la opinión consultiva N.º 267-2019- JUS/DGTAIPD-DPDP[198] " En virtud del `principio de calidad´ regulado en el artículo 8 de la LPDP, los datos personales deben ser adecuados, pertinentes, actualizados y necesarios, para la finalidad para la cual fueron recopilados, por lo que deben examinarse no sólo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo en que se produce este tratamiento".

c) Que los datos geolocalizados deban conservarse de forma tal que se garantice su seguridad, es vital para la calidad del dato. En efecto, si la calidad del dato geolocalizado supone que ellos sean veraces, exactos y actuales, para poder controlar de manera adecuada y justa el cumplimiento laboral de los trabajadores, una brecha de seguridad puede tener como consecuencia la alteración del dato, corromperlo, suprimirlo o hacerlo accesible para una persona que no está autorizada para ello, con lo que se comprometería la calidad del dato así como su tratamiento para controlar al trabajador; es decir, ya no serviría para cumplir la finalidad establecida.

d) El principio de calidad exige que los datos deben conservarse solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Por lo tanto, los datos geolocalizados deben ser suprimidos cuando ya hayan servido para el fin del control laboral por parte del empleador.

[198] Expediente N. º 40-PTT2018, p-11.

Hay datos personales de los trabajadores, que gestiona el empleador y que son necesarios, por ejemplo para fines de la gestión laboral, como pueden ser los datos de identificación, de estado civil, de estudios, el número de hijos, cuenta de ahorros, etc.; datos que en atención a leyes especiales en materia tributaria, de seguro social, del sistema nacional de pensiones, etc., se puede obligar a la conservación de los mismos más allá de la finalización de la relación laboral.

No obstante, tratándose del tratamiento de los datos geolocalizados con fines de control laboral, el tiempo de conservación de los datos es mucho más limitado, pues solo podrán conservarse para verificar el cumplimiento o incumplimiento de las obligaciones del trabajador derivadas del contrato de trabajo. Se trata de una finalidad concreta y específica que se aplica solo durante la existencia de la relación laboral y ni siquiera durante toda ella, sino que tiene una temporalidad muy limitada en atención a la específica finalidad de control.

Siguiendo la línea de lo señalado, no sería admisible que los datos geolocalizados con fines de control laboral estuvieran almacenados de manera indefinida, o por tiempos que excedan a la finalidad para la que se han recopilado; pongamos el ejemplo de un año o seis meses, o tres meses. Nos parecería excesivo.

En este punto podría considerarse como referencia el tiempo de conservación de los datos provenientes de la videovigilancia, establecido en la Directiva N°01-JUS/DGTAIPD, en la que se establece el plazo de 30 a 60 días como máximo. La Directiva señala que transcurrido este plazo y no habiendo requerimiento de alguna autoridad competente para entregar o visualizar el contenido de la grabación, los datos deberán ser eliminados.

La Directiva se pone en el supuesto de no aplicación del plazo máximo de conservación, lo que podría darse si existe alguna finalidad o interés legítimo que justifique su conservación, o la concurrencia de alguna contingencia de orden técnico que justifique razonablemente el aplazamiento de la eliminación de la información.

En sentido similar el Grupo sobre protección de Datos del Artículo 29, mediante su Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido, considera que " Habida cuenta de las posibles justificaciones para el tratamiento de los datos de localización, éste se llevará a cabo fundamentalmente en tiempo real . En cualquier caso, el Grupo recomienda que el período de retención de los datos de localización sea razonable, es decir, que no supere los dos meses".

Asimismo, el GT29 recomienda para el caso, en el que el empleador desee llevar a cabo el tratamiento de los datos de localización por un período superior a los dos meses, (como podría ser para elaborar un registro histórico de los viajes con el fin de optimizar los recursos), que podría realizarse si previamente se hacen anónimos los datos.

Si el trabajador cumplió sus deberes laborales; verificado esto dentro del plazo razonable establecido, el dato geolocalizado ya no debería seguir almacenado en el banco de datos respectivo de la empresa.

En caso de haberse identificado, por medio de los datos geolocalizados, que el trabajador incumplió un deber laboral, tendrá sustento que el dato se conserve en tanto dure el procedimiento disciplinario que podrá implicar la imposición de una sanción; y en su caso, la posible respuesta de su impugnación ante la autoridad competente o hasta que transcurra el plazo de la interposición de la misma. Ni la normativa sobre protección de datos personales ni ninguna otra, señala en el Perú, un plazo al respecto. Por lo que el empleador deberá evaluar a la luz del principio de proporcionalidad y de toda la normativa sobre protección de datos personales un tiempo razonable de conservación de los datos geolocalizados con fines de control. Si los datos geolocalizados se conservarán más allá del tiempo necesario para la finalidad establecida se vulneraría también el principio de calidad.

Al no existir regulación sobre el plazo de conservación, ese tiempo puede variar en cada centro laboral, con lo cual el riesgo a un tratamiento no adecuado, de los datos geolocalizados de los trabajadores, crece; a lo que se suma la posibilidad del no cumplimiento de las medidas de seguridad, que entre otras finalidades buscan garantizar la confidencialidad de la información.

Es necesario que el empleador incluya dentro de su política interna, en sus protocolos de gestión de los datos personales en la empresa, ese tiempo de conservación de los datos personales, teniendo en cuenta la naturaleza del sistema GPS, para demostrar su voluntad de estar en orden con la normatividad sobre protección de datos personales; pues como lo señala la Ley , la calidad también está vinculada con la finalidad, por lo que los datos personales solo pueden conservarse por el tiempo necesario para cumplir con la finalidad del tratamiento; es decir, para el control laboral sobre el trabajador.

### 3.5. Principio de Seguridad

El principio de seguridad es fundamental para garantizar la protección de los datos personales junto con los otros principios y el cumplimiento de las demás obligaciones legales. La seguridad de la información personal debe observarse durante todas las etapas del tratamiento de los datos personales hasta su cancelación.

El informe del CJI de la OEA (2016:p.12) sostiene que:

> Los datos personales deben protegerse, independientemente de la forma en que se mantengan, por medio de salvaguardias razonablemente concebidas para prevenir que las personas sufran daños considerables como consecuencia del acceso no autorizado a los datos o de su pérdida o destrucción. La índole de las salvaguardias podría variar según la sensibilidad de los datos en cuestión. Evidentemente, para los datos más sensibles se requiere un nivel más alto de protección.

Asimismo, las medidas de seguridad deben estar acordes con la evolución y

dinamismo de las amenazas tecnológicas para no quedar obsoletas, pues como dice el informe de la CJI de la OEA (2016:13) “En vista de la celeridad de los cambios en el entorno actual de la información, una práctica que hace solo unos meses era permisible podría considerase en la actualidad como una práctica intrusiva, riesgosa o peligrosa para la privacidad individual.

Análogamente, una restricción que haya parecido razonable hace algunos meses podría ser obsoleta o injusta a la luz de los adelantos tecnológicos”; por lo que si el empleador usa una tecnología como el GPS, debe optar por las medidas técnicas y los métodos más avanzados de seguridad.

El responsable de implementar las medidas de seguridad adecuadas a los datos geolocalizados de los trabajadores es el empleador en su calidad de titular del banco de datos personales y, por ende, de responsable del tratamiento.

Cuando la Ley en el artículo 2, inciso 17, define al titular del banco de datos coloca como una de las actividades que lo identifican como tal, el ser “[…] el que determine las medidas de seguridad del banco de datos personales así como de los datos mismos”.

Pero la obligación de la implementación de las medidas de seguridad no solo recaerá en el responsable del tratamiento, pues el artículo 9, de la Ley que define el principio de seguridad, incluye al encargado del tratamiento junto al titular del banco de datos como los que deben implementar las medidas, técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales.

En el caso de la empresa, tratándose de los datos geolocalizados, con fines de control laboral, pueden darse varios supuestos con relación a la persona que se ocupe de manera directa de la recopilación, conservación o de otras actividades de tratamiento de dichos datos geolocalizados.

Puede ser el mismo empleador directamente; en cuyo caso él asumirá toda la responsabilidad del tratamiento de la información como titular del banco de datos sin

encargado del tratamiento; pero tratándose del sistema GPS, lo que normalmente ocurre es que sea una persona externa, la que brinda los servicios de geolocalización; en cuyo caso actuará como encargado del tratamiento y se deberá concretar este encargo por medio de una relación jurídica, que vincule a ambas partes y que delimite el ámbito de actuación del encargado ( empresa que brinda el servicio de geolocalización), siendo de esto responsable el empleador, como titular del banco de datos respectivo.

En Perú, ya desde hace varios años, podemos encontrar empresas, como XmartClock que brinda un servicio que ofrece: "Todas las ubicaciones que hayan sido registradas por un empleado podrán ser consultadas en la sección de Reportes de nuestro sistema, de esta manera, podrás verificar si tu equipo de trabajo está en la ubicación correcta o hace el recorrido correspondiente, tan solo solicitando el reporte al sistema de manera individual o grupal"[199].

Convergia Perú, indica "que los datos son mostrados en una plataforma web y sobre mapas digitalizados para facilitar la gestión, aunque también cuenta con alertas dirigidas al correo electrónico y una versión móvil para el monitoreo"[200].

Hacom, ofrece una plataforma Office Track- Localizador GPS y Gestión Móvil Empresarial [201] que permite:

> […] supervisar a la perfección su negocio, saber de forma permanente la ubicación de su personal y de sus clientes, para […] crear un mapa digital a la medida de su requerimiento que le ayudará a identificar a sus clientes y al personal que cubre dichas zonas designadas. Este servicio le permite automatizar los registros de visitas de su

[199] Consultado al 05 de diciembre de 2020 en: https://www.eleconomista.es/opinion-legal/noticias/10316565/01/20/Geolocalizacion-riesgos-limites-y-oportunidades.html

[200] Consultado al 05 de diciembre de 2020 en: http://www.iriartelaw.com/gps-controla-trabajadores-que-laboran-calle. Publicación el año 2013.

[201] (2019:59) al 05 de diciembre de 2020 en: http://www.hacom.com.pe/servicios-de-gestion-de-fuerza-laboral-de-campo-y-aplicaciones-moviles/

> personal de campo al permitir que desde la aplicación haga un “Check in” a cada lugar que visitan y enviar esta información, también le permite registrar la asistencia de su personal, sin la necesidad que tenga que ir a su oficina central, ahorrando tiempo de gestión. […] podrá crear formularios de manera ilimitada que el personal de campo podrá registrar desde sus smartphones, estos formularios ayudaran para que el área de despacho sepa en tiempo real lo que deben enviar a cada uno de sus clientes.

Dentro de los beneficios que ofrece la empresa Hacom, se señalan: “controlar el tiempo laboral de sus empleados que trabajan fuera de la oficina. Olvídese de los tiempos muertos y de los reportes inexactos […] optimizar la eficiencia y eficacia de su fuerza de ventas […]”

Tanto el titular del banco de datos, que en este caso será siempre el empleador, como el encargado de su tratamiento (empresa que presta el servicio de geolocalización), ambos están obligados a adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales; así lo manda el artículo 9 de la Ley. Las medidas de seguridad a adoptar deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

Cabe tener presente, que en el caso de un encargo de tratamiento, como podría ser el rol que le corresponde a las empresas que brindan los servicios de geolocalización, el artículo 30 de la Ley, manda que los encargados de tratamiento no podrán utilizar dichos datos con un fin distinto al que figura en el contrato o convenio celebrado ni ser transferidos a otras personas, ni aun para su conservación. Por lo que las empresas que brindan los servicios de geolocalización están prohibidas de manera específica de utilizar dichos datos más allá de lo que diga el contrato de encargo celebrado con el empleador.

La ley sigue desarrollando el principio de seguridad, y en el artículo 16 señala que es el titular del banco de datos personales (geolocalizados) quien debe adoptar las medidas técnicas, organizativas y legales que garanticen su seguridad.

¿Qué es lo que persiguen las medidas de seguridad? ¿Para qué se deben implementar las medidas de seguridad? ¿Qué buscan evitar o proteger?

Las tres clases de medidas de seguridad que existen: legales ( como la adecuación de los formatos de información sobre las condiciones y los alcances del tratamiento de los datos geolocalizados); organizativas (como desarrollar una estructura organizacional con roles y responsabilidades en relación a los datos geolocalizados a proteger) y técnicas (como identificar todos los accesos realizados a los datos geolocalizados para su tratamiento); son las que deben implementarse para los datos geolocalizados de los trabajadores, tanto por el empleador como por el encargado de tratamiento, en su caso; y tienen como finalidades las siguientes:

-Evitar la alteración de los datos geolocalizados. (Art.16 de la Ley)

-Evitar la pérdida de los datos geolocalizados. (Art. 16 de la Ley)

-Evitar el tratamiento o acceso no autorizado. (Art. 16 de la Ley)

-Evitar cualquier tratamiento contrario a la Ley o al Reglamento: como la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. (Artículo 10 del Reglamento)

- Garantizar la confidencialidad de la información. (Art. 32 del Reglamento)

En este punto es necesario tener en cuenta, como lo establece el artículo 17º de la Ley, que el deber de confidencialidad, le corresponde al titular del banco de datos personales (empleador), al encargado (empresa que presta el servicio de geolocalización) y a quienes intervengan en cualquier parte de su tratamiento (como pueden ser los encargados del área de tecnologías de la información que en la práctica ven de manera directa el funcionamiento técnico del banco de datos geolocalizados); deber que supone que los datos personales de los trabajadores solo sean conocidos por el titular del dato y por aquéllas personas de la organización cuyo perfil les permite acceder a dicha información; asimismo, el deber de confidencialidad perdura inclusive después de finalizada la relación con el titular del

banco de datos geolocalizados. Esto puede ser atendido con una política de gestión del personal involucrado.

Este deber de confidencialidad se va a ver complementado con el deber de secreto profesional, de ser el caso; siendo que ambos constituyen una garantía para el derecho fundamental a la protección de datos personales; así como para la reputación de la organización.

Las medidas de seguridad a adoptarse las decide el empleador como titular del banco de datos geolocalizados, teniendo en cuenta la tecnología del GPS, las actividades de tratamiento a las que someterá a los datos geolocalizados y la clase o categoría de datos personales que recopilará con dicha tecnología.

Los datos geolocalizados con fines de control laboral son datos que no entrarían dentro de la categoría de datos sensibles, pues lo que indican es el lugar y el momento exacto en el que se encuentra, durante la jornada laboral, el trabajador en cumplimiento de sus obligaciones derivadas del contrato de trabajo.

Es importante que el trabajador como titular del dato geolocalizado, conozca qué clase de información recoge el GPS; cómo se gestiona; cómo se analiza; si será transferida o no; qué decisiones se tomarán a partir de ella; etc. Información de la que el trabajador debe conocer desde antes de la recopilación de la misma y sobre la que el empleador, ha debido de realizar la evaluación adecuada para adoptar las medidas de seguridad correspondientes; también previo a la primera actividad de tratamiento que vaya a realizar.

Una brecha de seguridad, puede vulnerar los derechos del trabajador y también los fines legítimos de control laboral.

Supongamos, que los trabajadores tienen el GPS en el móvil que les proporciona la empresa, y que sigue activado durante las 24 horas; y toda la información se va

almacenando en el banco de datos geolocalizados.

Por una brecha de seguridad, entra un hacker al banco de datos geolocalizados y accede a información sobre el uso frecuente de una determinada parada de autobuses de un grupo de trabajadores hacia una determinada dirección de la capital, al final de la jornada laboral; posteriormente, estos trabajadores reciben oferta de servicios de movilidad en grupo con ese destino; o, que determinados trabajadores van periódicamente a la sede de una asociación protectora de animales, y luego reciben una invitación para que firmen una proyecto de ley en beneficio de los animales, sin haber tenido contacto con los proponentes; situaciones equivalentes puede replicarse y multiplicarse.

Sin duda, toda esta información de los trabajadores pertenece a su esfera íntima personal o privada y está siendo conocida indebidamente por terceros, o por personal de la misma empresa; sin autorización para acceder a ella; y puede ser tratada con fines ilegítimos por causa de una brecha de seguridad.

Pero el empleador también puede verse afectado por las brechas de seguridad; porque si quien accede indebidamente al banco de datos geolocalizados borró el reporte de un determinado trabajador, justamente en un lapso de tiempo donde el empleador tiene particular interés en verificar el cumplimiento de sus deberes laborales; ya no podrá realizar dicha verificación, impidiéndole contar con la prueba del posible incumplimiento; justamente habiendo sido ésta una de las finalidades más importantes para las que se instaló el GPS.

Las medidas generales de seguridad se han desarrollado por el Reglamento entre los artículos 39 al 46, las cuales son de obligatorio cumplimiento, según corresponda a la categoría de los datos tratados, a las actividades de tratamiento y la tecnología utilizada.

Asimismo, la ANPDP, emitió una Directiva de Seguridad de la Información, aprobada

por Resolución Directoral N.º 019-2013-JUS/DGPDP, la cual constituye un instrumento que posibilita un accionar ajustado a derecho de quienes realizan tratamiento de datos personales y es que, como la propia Directiva señala, ésta no es obligatoria sino orientativa sobre las condiciones, requisitos y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de las normas de la Ley y del Reglamento.

El empleador deberá adoptar las medidas de seguridad establecidas en la Ley y en el Reglamento y tomar en cuenta las orientaciones de la Directiva; pero en realidad lo que debería hacer, si quiere actuar con responsabilidad y con mayor seguridad de proceder conforme a la normatividad sobre protección de datos personales, es adoptar lo que señala la Directiva como si fuera obligatoria; más aún, teniendo en cuenta que usa la tecnología del GPS para controlar el cumplimiento de las labores de sus trabajadores.

Es importante no dejar pasar por alto el último párrafo del artículo 16 de la Ley, porque establece una prohibición: “Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo”; de manera tal, que sería una labor importante el de verificar el cumplimiento de esta disposición; pero eso sólo podría hacerlo la Autoridad Nacional de Protección de Datos Personales, en ejercicio de sus funciones fiscalizadoras.

Hasta el 05 de noviembre del 2020, no se ha encontrado, en la página web de la ANPDP ninguna resolución de inicio o que concluya un procedimiento administrativo sancionador sobre un banco de datos geolocalizados de trabajadores o sobre datos geolocalizdos de los mismos. Sin embargo, ello no podría considerarse tampoco un indicativo de que los tratamientos de los datos geolocalizados de los trabajadores que se estén realizando, están rodeados de las medidas de seguridad correspondientes.

Implementadas las medidas de seguridad a las políticas o programas de seguridad establecidos, constituye solo el punto de inicio, pues se deben revisar de manera periódica para determinar las modificaciones que sean necesarias.

### 3.6. Principio de Legalidad

Como sabemos la legalidad supone que toda actividad de tratamiento de datos personales que se realice debe ajustarse a lo señalado en la Ley y el Reglamento. Esto comprende desde la actividad de la recopilación hasta la cancelación del dato. Por lo que la inobservancia de la normativa implicará una violación al principio de legalidad.

La legalidad comienza desde que el empleador recoge los datos de los trabajadores. En el caso de los datos de localización, en primer lugar, el empleador deberá evaluar si este mecanismo de control laboral supera el principio constitucional de proporcionalidad con sus tres subprincipios, necesidad, idoneidad y proporcionalidad en sentido estricto. Asimismo, si su utilización será conforme con todos los principios rectores de la protección de datos, como hemos analizado.

En segundo lugar, y de manera previa a la recopilación de los datos geolocalizados de los trabajadores, el empleador deberá haber inscrito en el Registro Nacional de Protección de Datos Personales un banco donde conste que va a tratar datos geolocalizados de sus trabajadores con fines de control.

Esta obligación fluye de la Ley en su artículo 29º; así como del artículo 78º del Reglamento, por el que se manda que las personas naturales o jurídicas, sean del sector público como del privado, que creen, modifiquen o cancelen bancos de datos personales, están obligadas a inscribirlos ante el Registro Nacional de Protección de Datos Personales.

Asimismo, los empleadores tienen la obligación de almacenar los datos personales de sus trabajadores, objeto de tratamiento, de manera que se posibilite el ejercicio

de sus derechos, como titulares de los mismos[202].

Como sabemos los derechos ARCO, que la Ley le reconoce al titular del dato, son parte del contenido esencial del derecho fundamental a la autodeterminación informativa que le corresponde, en este caso a los trabajadores. Por lo que la forma de almacenamiento de los datos, su soporte o la tecnología utilizada no deben limitar el ejercicio de dichos derechos, porque ello supondría supeditar a la persona, a sus derechos o a su dignidad, a la tecnología, lo que no puede ser aceptado en un Estado Constitucional de Derecho.

La inscripción del banco de datos donde se deje constancia que se realizará el tratamiento de datos de geolocalización y explícitamente con fines de control, es obligatoria; constituyendo una obligación que debe cumplir el empleador como responsable del tratamiento.

La inscripción del banco de datos geolocalizados persigue la finalidad de dar publicidad a la existencia de dichos bancos, de tal forma que sea posible ejercer los derechos de acceso, a la información, rectificación, cancelación, oposición y otros regulados en la Ley y el Reglamento.

Posteriormente a la inscripción del banco de datos, que contenga datos geolocalizados de los trabajadores, el empleador podrá proceder a recopilar dichos datos, habiendo cumplido también previamente, con el deber de información, que incluye entre otros aspectos[203], el dar a conocer sobre la existencia del banco de datos en el que se tratará la información personal (los datos de geolocalización) del trabajador.

Buscando un argumento objetivo que permita darnos una aproximación al conocimiento de si en el Perú, los empleadores que tratan datos geolocalizados de

[202] Artículo 28º, inciso 5, de la Ley.

[203] Conforme a lo que dispone el artículo 18 de la Ley y el 12 del Reglamento, según lo analizado en el acápite correspondiente.

sus trabajadores están cumpliendo con el principio de legalidad; con su deber de información y de transparencia que es a su vez un derecho del titular del dato; con permitir y facilitar el ejercicio de los derechos de dichos titulares (los trabajadores geolocalizados), es decir si están cumpliendo con sus obligaciones derivadas de la Ley y del Reglamento; hemos realizado una búsqueda en el Registro Nacional de Protección de Datos Personales, el RNPDP, administrado por la Autoridad Nacional de Protección de Datos Personales, en los términos que a continuación detallamos:

La búsqueda se ha realizado en todo el RNPDP del MINJUS – ANPD en el siguiente link: https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado

De esa manera se ha buscado en todas las resoluciones (desde las primeras hasta las inscritas hasta al 24 de enero de 2021), detalladas a continuación:

**TIPO DE BANCO DE DATOS**

**PERSONA JURÍDICA**

| | |
|---|---|
| **Trabajadores** | Desde la Resolución N. ° 005-2013-JUS/DGPDP (12/07/13) hasta la Resolución N. ° 2053-2020-JUS/DGTAIPD – DPDP (30/11/20) |
| **Recursos Humanos** | Desde la Resolución N. ° 2741-2019-JUS/ DGTAIPD – DPDP (20/09/19) hasta la Resolución N. ° 2036-2020-JUS/DGTAIPD - DPDP (30/11/20) |

## PERSONA NATURAL

| | |
|---|---|
| **Trabajadores** | Desde la Resolución N. ° 315-2014-JUS/DGPDP - DRN (11/12/14) hasta la Resolución N. ° 164-2020-JUS/DGTAIPD – DPDP (07/01/20) |
| **Recursos Humanos** | Desde la Resolución N. ° 1239-2015-JUS/DGPDP - DRN (05/08/15) hasta la Resolución N. ° 2685-2016-JUS/DGPDP - DRN (07/10/16) |

-Se han buscado e identificado a todos los bancos de datos de personas naturales y de personas jurídicas que hayan inscrito un banco de datos de trabajadores o de recursos humanos[204]. Se ha ingresado a las resoluciones de inscripción de cada uno de esos dos tipos de bancos de datos inscritos en el RNPDP hasta el 24 de enero de 2021.

- En ninguno de los bancos de datos con denominación de "Trabajadores" o "Recursos humanos" existentes en el RNPD al día de 24 de enero de 2021 se ha anotado que se traten datos localizados o geolocalizados de sus trabajadores.

- Por lo señalado, se deduce que si no hay inscrito un banco de datos que trate datos localizados o geolocalizados de los trabajadores, tampoco se encuentra registrado que los fines de control o de vigilancia laboral se cumplan mediante el tratamiento de dichos datos localizados o geolocalizados; los cual tampoco aparece en el RNPDP.

- Adicionalmente, podemos afirmar que los últimos bancos de datos inscritos, de trabajadores y de recursos humanos, dentro de los dos tipos de personas mencionadas (persona natural y persona jurídica), corresponden a la fecha 30 de noviembre de 2020. Entonces desde esa fecha no se han inscrito más bancos de

[204] Nombre del banco de datos según criterio del RNPDP.

datos de trabajadores o de recursos humanos hasta el 24 de enero de 2021, día en que ha terminado nuestra búsqueda en el RNPDP.

Hemos constatado entonces que en el Registro Nacional de Protección de Datos Personales, no existe ningún banco de datos de trabajadores o de recursos humanos, que de cuenta del tratamiento de datos geolocalizados de los trabajadores, tal como ha quedado expresado.

Pero ¿en el Perú no se tratan datos geolocalizados de los trabajadores? y en específico con fines de control laboral?

Es indiscutible que en el Perú se realiza el tratamiento de datos geolocalizados de los trabajadores desde hace un buen número de años; sostenemos esto no sólo por las diversas empresas que hace varios años ofrecen dichos servicios en nuestro medio[205]; o porque conocemos personas que nos señalan que tienen gps en los vehículos o en los celulares u otros dispositivos que la empresa empleadora les ha proporcionado; sino que del tratamiento de este tipo de datos de los trabajadores se ha dejado constancia en sentencias judiciales.

Con relación a los pronunciamientos del Poder Judicial los hechos constatados vienen desde más antiguo. Tal como lo hemos desarrollado en el capítulo 2, acápite 2.3.1.2.; ya desde el Pleno Jurisdiccional Regional Laboral realizado en Chiclayo el 06 de junio del 2009, se identifica al GPS como un mecanismo de fiscalización directa y constante del empleador, lo propio ocurre, en sentido equivalente en las cinco sentencias de casación Laboral analizadas en el mismo apartado.

Lo que hemos podido constatar es que tenemos en el Perú, pronunciamientos del Poder Judicial que dan cuenta del uso de datos geolocalizados de los trabajadores desde el año 2009[206]; la Ley de Protección de Datos Personales se da en el 2011, el

[205] Ver capítulo 3, acápite 3.5.
[206] Lo cual no significa que desde ese año se haya comenzado a tratar datos geolocalizados de los trabajadores; lo que podemos asumir es que esto se da desde antes.

Reglamento en el 2013; y hasta el 24 de enero del 2021, no existe ningún banco de datos de trabajadores o de recursos humanos inscrito en el RNPDP que haya declarado que trata datos geolocalizados de sus trabajadores. Esto denota un incumplimiento -pasado, presente y que continúa- a la Ley y al Reglamento sobre la materia.

Esta situación de incumplimiento y de violación de derechos de los trabajadores geolocalizados; y en específico, de los geolocalizados con fines de control, no debe continuar, requiriendo ser atendida; más aún, ante el incesante avance tecnológico que aumenta las capacidades de control del empleador y pone en más riesgo los derechos de los trabajadores que realizan sus servicios en un contexto de subordinación. Una de las formas de hacer frente a esta situación es mediante la atención del tema por medio de una regulación específica sobre el tratamiento de los datos geolocalizados con fines de control laboral.

Como lo ha señalado, la Recomendación CM/Rec (2015) 5 del Comité de Ministros del Consejo de Europa, sobre el tratamiento de datos personales en el contexto del empleo[207], cuando se refiere a la transparencia del procesamiento de los datos, señala que la información que le debe proporcionar el empleador al trabajador, es necesaria para garantizar un procesamiento justo y legal. Por lo que si el empleado no está informado que sus datos personales, que proporciona el GPS, serán utilizados con fines de control laboral y las demás condiciones de su tratamiento, se habrá incurrido en un tratamiento injusto e ilegal.

Precisa además, la referida recomendación europea para los empleadores, que la información pertinente deberá proporcionarse en un formato accesible y mantenerse actualizada; siendo que deberá ser proporcionada antes de que el empleado lleve a cabo la actividad; asimismo, debe estar disponible a través de los sistemas de información que normalmente utiliza el empleador.

[207] Punto 10. Consultado el 22 de noviembre del 2020 en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

A la luz de los principios analizados, el sistema GPS le provee al empleador de más información de la que necesita para ejercer su legítima facultad de control; accediendo, por ejemplo a información extra laboral, como podrían ser, los lugares donde el trabajador suele ir a almorzar durante su hora de refrigerio, o sus movimientos y lugares a donde asiste todo el tiempo, si lo tiene activado las veinticuatro horas, o durante los tiempos de permiso, vacaciones, etc. El empleador, como responsable del tratamiento, deberá realizar los procedimientos pertinentes para que no se dé un tratamiento excesivo de los datos de sus trabajadores, pues estaría afectándose, entre otros principios, los de proporcionalidad y de calidad.

Si el dato geolocalizado excesivo, al que tiene acceso el empleador, le da cuenta que su trabajador es un apasionado de la comida italiana, porque varios días a la semana va a almorzar a restaurantes donde se expende dicha clase de comida, y usa esa información para comunicarla a una empresa de marketing que procede a enviarle publicidad sobre restaurantes de comida italiana a su trabajador; el empleador habrá infringido el principio de consentimiento, pues para ese tipo de tratamiento, extra laboral, debió pedir la autorización de su trabajador; pero también el de proporcionalidad, pues el dato era excesivo para la finalidad de control.

Asimismo, habrá vulnerado el principio de finalidad, pues el tratamiento al que está habilitado el empleador es con el fin de control laboral y no para transferir esos datos a un tercero con fines de publicidad comercial.

Además, este tercero habrá recopilado el dato del trabajador sin su consentimiento; aún más, sin su conocimiento; con lo cual se tratará de una recopilación ilícita del dato y por ende ilegal.

Lo señalado es sin dejar de considerar que el uso indebido de este dato de localización de los lugares donde suele almorzar el trabajador durante sus horas de refrigerio, constituye un dato de su intimidad personal, por lo que se habrá vulnerado también este derecho fundamental, constituyéndose asimismo otro fundamento del

tratamiento ilegal.

El empleador, no por el hecho de tener acceso a diversa información a través de los datos geolocalizados de sus trabajadores, significa que pueda utilizarla con los fines que él determine; pues, solo podrá hacerlo, dentro del estricto marco de su facultad de control y de lo que el derecho a la protección de datos de su trabajador le permite; lo que supone entre otras cosas, que el mismo trabajador como titular del dato conozca los fines del tratamiento, para poder estar frente a un tratamiento leal y legal.

El tratamiento de los datos geolocalizados de los trabajadores le da un gran poder al empleador, que pone en riesgo los derechos del trabajador, si no ajusta la gestión de dichos datos, a la Ley. El empleador en su calidad de tal no solo accede a los datos geolocalizados de sus trabajadores; sino que, desde el inicio de la relación laboral, accede y gestiona muchos otros datos personales destinados no solo a la ejecución de la relación laboral, sino también al cumplimiento de sus deberes administrativos que como empleador le corresponden; por ejemplo, como con el sistema de pensiones, público o privado; con el seguro de salud; con el Sistema de Administración Tributaria; con la organización sindical, cuando corresponda; con el Ministerio de Trabajo y Promoción del Empleo; etc.

Si a esto le sumamos un empleador que busca y accede a información del trabajador que se encuentra desplegada en internet, como en buscadores, redes sociales, redes profesionales, etc.; el empleador podrá relacionar datos y controlar el comportamiento de su trabajadores, lo más seguro de manera indebida; pero a la vez, sin control, pudiendo llegar a elaborar un perfil de la persona de sus trabajadores con el fin de tomar decisiones sobre ellos o, inclusive, predecir sus comportamientos de consumo, entre otros. Lo acabado de señalar, constituye un comportamiento ilegal.

El empleador debe dar muestras objetivas de que conoce la Ley y el Reglamento y

que al interior de su organización ha implementado las medidas pertinentes que demuestran su cumplimiento y respeto.

Creemos importante abordar desde la legalidad, que en buena cuenta tiene conexión con todos los principios rectores de la protección de datos, la pregunta si ¿el empleador puede o no obligar al trabajador a facilitar medios personales para ser geolocalizado?.

Este tema se abordó en Madrid por la Audiencia Nacional, la Sala de lo Social, en la sentencia N° .13/2019. En dicha sentencia se resolvió contra la empresa Telepizza Sau declarando la nulidad del "proyecto Tracker" que suponía la obligación para el trabajador repartidor de aportar a la actividad empresarial un teléfono móvil con conexión a internet de su propiedad, que permitiera la instalación de la aplicación (App) creada por Telepizza y que debería utilizarse durante la totalidad de la jornada laboral del trabajador a efectos de que tanto la empresa como sus clientes pudieran realizar un seguimiento en tiempo real y mediante geolocalización, de la ubicación de los pedidos a ser atendidos.

La sentencia consideró insuficiente la información sobre los datos de geolocalización porque se omitieron datos esenciales, pues la empresa solo informó: "que pretendía implantar un sistema de geolocalización de pedidos lo que conllevaría que los empleados aportasen una terminal de telefonía móvil en la que descargarse una App confeccionada al efecto a instancias de la empresa, que se efectuaría una compensación y que la negativa reiterada o imposibilidad sobrevenida de aportación de esta herramienta por parte del trabajador, o de la aplicación informática antes mencionada, será causa suficiente para la extinción del contrato de trabajo […]"

La información fue considerada insuficiente porque la geolocalización es una medida que afecta a datos personales, del trabajador, protegidos constitucionalmente; por lo que se estimó que era necesario que; "hubiese explicado el concreto funcionamiento de la aplicación, esto es, cómo se instala en el teléfono móvil, a qué datos del terminal la misma debe acceder, qué concretos datos propios ha de aportar el trabajador para

acceder a la aplicación, qué datos, en su caso, ha de archivar la misma y cómo van a ser tratados los mismos […]". Habiendo faltado informarle también sobre el posible ejercicio de los derechos como titular de la información.

El proyecto tracker implicaba que los trabajadores para descargar la aplicación en su teléfono móvil debían de proporcionar un número de teléfono o una dirección de correo electrónico en la que pudieran recibir el código de descarga.

Era indudable para la Sala que la implantación de dicha medida suponía una injerencia en los derechos fundamentales de los trabajadores, por lo que era necesario de realizar y superar el denominado juicio de proporcionalidad.

Las razones por las que fundamentalmente se violaba el derecho a la protección de datos personales, tal como había sido implantado por la empresa, radicaban en lo siguiente; en primer lugar:

> […] porque la medida implantada, si bien obedece a fines constitucionalmente legítimos en el desarrollo del derecho a la libre empresa como son el control el empleado en el desempeño de su puesto de trabajo y la oferta de un mejor servicio al cliente- de forma que éste pueda conocer en todo momento la ubicación de su pedido, dotando a la empresa de capacidad para proporcionar servicios que se afirma ya ofrecen otras empresas del sector-, no supera a juicio de la Sala, el necesario juicio de proporcionalidad.
>
> La misma finalidad se podría haber obtenido con medidas que suponen una menor injerencia en los derechos fundamentales de los empleados como pudieran ser la implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o las pulseras con tales dispositivos que no implican para el empleado la necesidad de aportar medios propios y lo que es más importante, ni datos de carácter personal como son el número de teléfono o la dirección de correo electrónico en la que han de recibir el código de descarga de la aplicación informática que activa el sistema.

En segundo lugar, porque, como ya se ha señalado, para la implantación del sistema de geolocalización por parte del empleador se prescindió de comunicar a los trabajadores de la información establecida por la Ley de Protección de Datos Personales.

Pero la Sala abundó en el análisis de la ilegalidad del proyecto Tracker; pues consideró como abuso del derecho del empresario el exigir, al trabajador, la aportación de un teléfono móvil con conexión de datos para desarrollar el trabajo; responsabilizándole además de dichos medios, de manera tal que cualquier impedimento en la activación del sistema de geolocalización implicaría una sanción para el trabajador, como la suspensión con la consecuente pérdida del salario; asimismo, al dar una aportación como compensación que era insuficiente; y que además, suponía obligar a los trabajadores a la contratación de unos datos por internet que solo se compensaban en función de su utilización en el trabajo, prescindiendo de si tal contratación era o no deseada por el empleado para el desarrollo de su vida personal. Por lo que se declaró la nulidad del Proyecto Tracker, fallando contra la empresa Telepizza Sau.

Se descartó, a la luz de esta sentencia, y como regla, la obligación del trabajador de aportar sus propios medios para la realización de la actividad laboral.

Creemos que los criterios de la Sala son razonables y proporcionados; y que ponen de manifiesto, la ilegalidad en el citado tratamiento de datos personales; lo que, en atención a su derecho relacional, supone también la afectación de otros derechos.

Otro aspecto importante, que como obligación le compete al empleador, como titular del banco de datos o responsable del tratamiento, es observar las medidas de seguridad, técnicas, legales y organizativas pertinentes; las mismas que se deben implementar teniendo en cuenta las actividades de tratamiento a realizar y la categoría de los datos a tratar. En el caso de los datos geolocalizados, su tratamiento deberá observar las disposiciones correspondientes a la seguridad digital que desarrolla el reglamento en los artículos 39 al 46, así como las normas orientativas

de la Directiva de Seguridad aprobada por resolución Directoral N.º 019-2013-JUS/DGPDP.

Un empresario debe abordar las múltiples obligaciones derivadas de la Ley y del Reglamento de una manera preventiva, de manera integral y documentada. Nuestra legislación no señala como una obligación este triple aspecto para su cumplimiento; no obstante, no hay una forma unívoca de asumir el cumplimiento de la Ley; pero cualquiera que esta sea debe ser responsable y respetuosa de los derechos de los titulares de los datos.

Como ha quedado señalado y en la medida que el principio de legalidad, abarca en buena cuenta todo incumplimiento a la normativa sobre la materia, el empleador que controle la actividad laboral de sus trabajadores en ejercicio de su facultad de fiscalización, debe ser consciente que el sistema del GPS debe desactivarse durante la realización de las actividades extra laborales, que realice el trabajador en tiempos de permisos, vacaciones, descansos médicos o equivalentes; así como fuera de la jornada laboral propiamente dicha; pero esto supone también que el trabajador sea consciente de su derecho y haya sido capacitado para la desactivación del GPS; o, en su caso, que el empleador haya programado la desactivación de su funcionamiento.

Esto no está establecido en ninguna normativa; pero en atención a la naturaleza del GPS, debería realizarse para actuar acorde con la legislación sobre protección de datos personales.

El debido tratamiento de los datos personales de los trabajadores pasa por una modificación de la mentalidad empresarial que comprende a toda la organización, desde las instancias más altas hasta las más bajas, que involucren transversalmente a todas las áreas. Lo señalado es porque siempre se ha realizado el tratamiento de los datos personales de los trabajadores; pero hace más de nueve años en el Perú, el contexto normativo ha cambiado radicalmente, con el desarrollo

legislativo del reconocimiento constitucional del derecho a la protección de datos personales.

A esto debe sumarse, el incremento del uso de la tecnología para realizar actividades de tratamiento como la de los datos geolocalizados de los trabajadores; que tiene la característica de la potenciación de las capacidades de esos sistemas (GPS) de una manera muy dinámica, a la que la legislación no puede seguirle el ritmo.

Asimismo, el empleador en atención a su responsabilidad como titular del banco de datos y para asegurarse de un mejor cumplimiento de la legislación sobre la materia, podrá recurrir a la implementación de una medida proactiva antes de iniciar una actividad de tratamiento, antes de elegir usar una tecnología como la del GPS para controlar a sus trabajadores; dentro de estas medidas podría usar lo que en la doctrina y legislación comparada se denomina, " privacidad desde el diseño" como lo hace la Guía sobre la materia de la Agencia Española de Protección de Datos[208] o "Privacidad por diseño y privacidad por defecto" como la llama, los Estándares de protección de datos de la Red Iberoamericana de Protección de Datos (2017: 29)[209]:

> 38.1. el responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que

[208] "La idea de 'protección de datos desde el diseño' existe desde hace más de 20 años y se ha trabajado intensamente en ella bajo la terminología de 'privacidad desde el diseño' (Privacy by Design, PbD). Este concepto fue desarrollado por la Comisionada de Protección de Datos de Ontario, Ann Cavoukian, en la década de los 90; presentado en la 31ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad del año 2009 bajo el título "Privacy by Design: The Definitive Workshop" [1][2] y aceptado internacionalmente en la 32ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, celebrada en Jerusalén en el año 2010, con la aprobación de la "Resolución sobre la Privacidad por Diseño" [3] . En esta resolución se reconocía la importancia de incorporar los principios de privacidad dentro de los procesos de diseño, operación y gestión de los sistemas de la organización para alcanzar un marco de protección integral en lo que a protección de datos se refiere. Además, se animaba a la adopción de los Principios Fundacionales de la Privacidad desde el Diseño definidos por Ann Cavoukian y se invitaba a las Autoridades de Protección de Datos a trabajar activamente e impulsar la incorporación de la privacidad desde el diseño en las políticas y la legislación en materia de protección de datos de sus respectivos Estados." Consultado al 04 de diciembre del 2020 en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

[209] Consultado al 19 de noviembre de 2020 en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable.

38.2. El responsable garantizará que su programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas.

El Reglamento (UE) 2016/679, General de Protección de Datos, incorpora, en su artículo 25[210], a la normativa de protección de datos, la práctica de considerar los requisitos de la privacidad desde el diseño desde las primeras etapas del diseño de productos y servicios. Como señala la Guía de Privacidad desde el Diseño de la Agencia Española de Protección de Datos, confiriéndole con ello, "la categoría de requisito legal al principio de integrar las garantías para la protección de los derechos y libertades de los ciudadanos con relación a sus datos personales desde las primeras etapas del desarrollo de sistemas y productos. Entendiendo pues como la necesidad de considerar la privacidad y los principios de protección de datos desde la concepción de cualquier tipo de tratamiento".

[210] Artículo25. Protección de datos desde el diseño y por defecto. 1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. 3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Lo ideal, entonces[211] y como una forma de actuar responsablemente por parte del empleador, interesado en cumplir los objetivos empresariales; pero, a la vez, con respeto de los derechos del trabajador, sería que cada vez que va a implementar una mecanismo de control laboral y, si éste es por medio de una tecnología invasiva como lo es el GPS, verifique si con ella a través de todo su funcionamiento, va a cumplir con la normativa de protección de datos. El objetivo último, como señala la Guía de la Agencia Española de Protección de Datos, (2010:7), es "que la protección de datos esté presente desde las primeras fases de desarrollo y no sea una capa añadida a un producto o sistema".[212] Esto sin duda, generará un clima de mayor confianza y será una muestra de la buena fe en las relaciones laborales; además colocará a los empleadores, como responsables del tratamiento, de los datos geolocalizados de los trabajadores, en mejor posición para, dado el caso, sustentar ante la autoridad de control, el cumplimiento de su rol como titulares de los bancos de datos personales.

## 3.7. Opciones de regulación frente a la inexistencia de normativa específica

### 3.7.1. Normativa general

En el presente trabajo no se ha considerado necesario realizar un estudio de la normativa existente en los países latinoamericanos que cuentan con legislación general sobre protección de datos personales porque, de manera similar a lo que ocurre en Perú, no cuentan con regulación sobre los datos geolocalizados de los trabajadores.

Sí se ha optado por tener en cuenta la legislación sobre la materia específica con la que cuenta España desde el año 2018, en la su Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, en lo que respecta a la protección de datos del trabajador; porque puede servirnos de orientación para

[211] Esto no constituye una obligación legal en Perú.
[212] Consultado al 04 de diciembre del 2020 en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

posibles mejoras en esta clase de tratamiento de datos personales geolocalizados de los trabajadores; de la misma forma como, la legislación española, nos sirvió, en su momento, de base fundamental para la Ley de Protección de Datos Personales y su Reglamento, que tenemos en Perú.

La Ley española, incorpora, como novedad, en su título X, diecisiete derechos relacionados a la protección de datos en el ámbito digital. Lo hace en atención al artículo 88 del Reglamento General de Protección de Datos de la Unión Europea (2016/679), mediante el que se dispone que los Estados miembros, podrán a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral.

El punto de partida y la base para el reconocimiento de los derechos digitales, en la Ley española[213], y que es perfectamente aplicable a cualquier Estado Constitucional de Derecho, como el Perú, es poner en claro que en este mundo globalizado, caracterizado por un proceso de transformación tecnológica, los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internaciones de los que un país sea parte, son plenamente aplicables también en internet.

Por lo que el tratamiento de los datos personales en internet, y a través de una tecnología específica, no deben suponer una flexibilización o rebajar el estándar de protección del derecho a la protección de datos personales.

Lo que se debe hacer, entonces es adaptar estos derechos fundamentales al entorno digital, en el que se desenvuelve el ámbito laboral y la vida de la sociedad en general, sin disminuir el respeto y la garantía propia de los derechos involucrados.

Dentro de los derechos digitales que reconoce la Ley española sobre protección de datos personales hay cinco que están vinculados al ámbito laboral, y son el : derecho

[213] Artículo 79.

a la intimidad y uso de dispositivos digitales en el ámbito laboral ( art. 87º); derecho a la desconexión digital en el ámbito laboral ( art. 88º); derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo ( art. 89º); derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral ( art. 90º) y los derechos digitales en la negociación colectiva (art. 91º) .

Teniendo en cuenta el objetivo del presente trabajo, consideramos que hay dos, de los derechos mencionados, que se enlazan temáticamente por lo que deben operar ambos a la vez; y son el derecho a la desconexión digital en el ámbito laboral y el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Veamos cómo los reconoce, la Ley española:

Artículo 88. Derecho a la desconexión digital en el ámbito laboral.

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

El derecho a la desconexión digital tiene que ver con la calidad de vida del trabajador en un ambiente donde el uso de la tecnología en el ámbito laboral se está generalizando y normalizando, sin tener en cuenta los riesgos que supone su uso, con relación a los que suponían los medios tradicionales, no digitales, utilizados para el control laboral.

Este derecho, por su carácter general, no tendría que estar limitado al uso del GPS, pues puede aplicarse al uso de otro tipo de tecnología, como mensajes por WhatsApp, o el correo electrónico; sin embargo, para el presente trabajo, lo consideraremos en relación al GPS con fines de control laboral.

Con el derecho a la desconexión digital, Moreno Vida señala, que: "se trata de garantizar el derecho del trabajador a "no tener ningún contacto con herramientas digitales relacionadas con su trabajo durante su tiempo de descanso y sus vacaciones" pues el trabajador "tiene constitucionalmente garantizado el poder de auto determinarse fuera de la jornada de trabajo" (2019).

La Comisión Mundial sobre el Futuro del Trabajo de la OIT-Oficina Internacional del Trabajo, (OIT 2019:13) en su informe "Trabajar para un futuro más prometedor" ha señalado la necesidad de ampliar la soberanía sobre el tiempo de trabajo:

> Los trabajadores necesitan una mayor autonomía sobre su tiempo de trabajo, sin dejar de satisfacer las necesidades de la empresa. Aprovechar la tecnología para ampliar las oportunidades y conciliar la vida profesional con la vida personal puede ayudarles a alcanzar este objetivo y encarar las presiones derivadas de la difuminación de la línea divisoria entre el tiempo de trabajo y el tiempo privado. Será preciso perseverar en los esfuerzos encaminados a aplicar límites máximos al tiempo de trabajo además de medidas para mejorar la productividad, así como un mínimo de horas de trabajo garantizadas que genere opciones reales de flexibilidad y control sobre los horarios de trabajo.

Llegando a exhortar a que se tomen medidas que "faciliten una autonomía del tiempo de trabajo que satisfaga las necesidades de los trabajadores y de las empresas", identificando como una de esas medidas, para lograr el objetivo equilibrado propuesto en la presente era digital, el derecho a la desconexión digital: "En la era digital, los

gobiernos y las organizaciones de empleadores y de trabajadores tendrán que encontrar nuevos medios para aplicar de forma eficaz a nivel nacional determinados límites máximos de las horas de trabajo, por ejemplo, estableciendo el derecho a la desconexión digital" (OIT 2019: 42) .

¿Cuáles serían los aspectos que debería incluir una regulación del derecho a la desconexión digital?

-Señalar los bienes jurídicos principalmente protegidos por la desconexión. digital. Dentro de ellos, están varios derechos, que al ser los principalmente afectados por un control tecnológico constante, serían los que normalmente se verían vulnerados. Nos referimos a los derechos que ya tienen la garantía jurídica de protección en nuestro ordenamiento jurídico: a la intimidad personal y familiar (art. 2, inciso 7. constitucional); a la paz, a la tranquilidad, al disfrute del tiempo libre y al descanso (art. 2, inciso 22. constitucional); al respeto a la jornada laboral y al descanso remunerados (art. 25. constitucional).

Asimismo, que el ejercicio de este derecho se dará fuera del tiempo legal o convencionalmente establecido.

-Modalidades de ejercicio. Que se señale que sujetará a lo establecido en la Ley y el Reglamento, así como, y según corresponda, a lo que haya sido establecido por el convenio colectivo, o a lo acordado entre la empresa y los representantes de los trabajadores; que se atienda a la naturaleza y objeto de la relación laboral potenciando el derecho a la conciliación de la actividad laboral y la vida personal y familiar.

-Elaboración de una política interna. Mediante la que se definirán las modalidades del ejercicio del derecho a la desconexión digital; también acciones de formación y de sensibilización del personal para el uso adecuado del sistema del GPS, tanto para que funcione debidamente como mecanismo de control, con el fin de evitar el riesgo de fatiga informática; pero también para que el trabajador conozca las consecuencias de su indebida manipulación que impida el normal funcionamiento para el fin establecido.

La elaboración de esta política no puede ser arbitraria por parte del empleador, pues deberá guiarse por las obligaciones y principios de la protección de datos personales y por la normativa laboral aplicable; no obstante sería positivo que se permitiera y señalara, como en la legislación española, la participación de los representantes de los trabajadores (estén o no sindicalizados) en la elaboración de esta política interna, considerando la naturaleza de medio invasivo que supone el GPS.

Con respecto a la regulación específica del uso del sistema de geolocalización como mecanismo de control laboral, la ley española establece lo siguiente:

> Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
>
> 1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.
>
> 2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Podemos apreciar que la Ley española, coloca en el epígrafe del artículo 90º, el derecho a la intimidad como límite directo al uso del GPS como sistema de control laboral. Si bien es cierto, como se ha desarrollado, que el derecho a la protección de datos personales nace vinculado al derecho a la intimidad, por lo que es muy frecuente su afectación, por un uso indebido de los datos personales, y en el caso de la tecnología bajo análisis esto supone un riesgo potencialmente mayor; también sabemos que, por la naturaleza relacional del derecho a la protección de datos personales, esta afectación puede producirse también con relación a otros derechos, dependiendo de las circunstancias de cada caso concreto. Esa fue la

opción del legislador español que, en este, caso va en concordancia con el capítulo denominado “Garantía de los derechos digitales”, del cual forma parte el artículo bajo comentario.

La Ley española sobre protección de datos personales y garantía de los derechos digitales, incorpora estos dos derechos, que siendo derechos de materia laboral, implican el tratamiento de datos personales de los trabajadores; pudiendo generarse la afectación de distintos derechos como el derecho a la protección de datos personales, a la intimidad, al disfrute del tiempo libre, entre otros. Con lo señalado, se pone de manifiesto, la relación entre las dos clases de materia legislativa: la de protección de datos personales y la laboral, siendo necesaria su interacción para atender de manera adecuada a la solución de problemas que busquen un equilibrio entre los derechos del trabajador y los intereses empresariales.

Dentro de los aspectos que consideramos necesarios que debería contener una regulación especifica sobre el uso del GPS para control laboral estarían los siguientes:

-Establecer que los empleadores podrán tratar los datos obtenidos por medio del sistema de geolocalización con fines de control laboral, con las limitaciones establecidas en la Ley y el Reglamento.
Si bien es cierto que, lo acabado de señalar, podría abarcar todo por mencionar a la Ley y al Reglamento, su generalidad, frente a la naturaleza del GPS, no sería suficiente.

-El tratamiento de los datos geolocalizados se podrá realizar, cuando sea pertinente adecuado y no excesivo para el fin de control laboral y no deberá extenderse a otra finalidad.
En atención a la naturaleza invasiva del GPS es imprescindible tomar previsiones para el cumplimiento de los principios de proporcionalidad y de finalidad; resaltarlos, ratifica su importancia, como condiciones para este tipo de tratamiento de datos personales.

- Los trabajadores deben ser informados de manera expresa, inequívoca y previa a la recopilación de los datos geolocalizados, de la existencia y características del dispositivo; debiendo quedar expresada la posibilidad de usar los datos geolocalizados recopilados con fines disciplinarios y la posible aplicación de las sanciones que correspondan.

-Los trabajadores deben ser informados sobre la facultad de ejercer los derechos que les asisten como titulares de los datos geolocalizados; así como, los mecanismos implantados por la empresa para ello.

- La empresa debe establecer una política de conservación de los datos geolocalizados por un plazo que no exceda a la finalidad de control, debiendo señalarse las condiciones de su supresión cumplida esta. El plazo excepcionalmente puede extenderse lo necesario para la realización de un proceso disciplinario; o para responder ante una obligación legal para el empleador, como podría ser ante la impugnación de un despido, aplicada como resultado de la facultad de control laboral.

- El empleador debe establecer las medidas adecuadas que garanticen la seguridad y confidencialidad de los datos geolocalizados.

- Cuando se permita el uso privado de la herramienta de trabajo que incorpora el GPS, se debe garantizar la desactivación del sistema fuera de las horas comprendidas en la jornada laboral.

Si el GPS se encuentra con fines de seguridad en el vehículo, y éste puede ser utilizado fuera de la jornada laboral para usos personales; la política de uso debe garantizar el cumplimiento del principio de proporcionalidad y que los datos geolocalizados no se utilizarán para otra finalidad.

En consecuencia, como una forma de atender la ausencia de regulación y de criterios tanto jurisprudenciales, como provenientes de la ANPDP, en relación a los datos geolocalizados de los trabajadores; teniendo en cuenta lo desarrollado sobre el

derecho a la desconexión digital en el ámbito laboral y las condiciones para la utilización de sistemas de geolocalización en el mismo ámbito, podrían servir de base para su incorporación en nuestra legislación desde alguno de los siguientes tres niveles de la misma:

-En la Ley. El derecho a la desconexión digital podría ser técnicamente incluido en la Ley en atención a ser una norma del segundo nivel del ordenamiento jurídico. De otro lado, si se optara por incluir las condiciones para el tratamiento de los sistemas de geolocalización satelital en las relaciones laborales y específicamente con fines de control laboral, podría ser como una regulación para un tratamiento de datos personales específico, tanto en la Ley[214] como en el reglamento de la misma.

-El Reglamento, como parte de su Título III. Tratamiento de datos personales, capítulo IV, "Tratamientos especiales de datos personales", da algunas normas sobre determinados tipos de tratamiento: de los datos personales de menores; así como, en el sector de las comunicaciones y telecomunicaciones. A este nivel, podrían darse disposiciones sobre el tratamiento de los datos geolocalizados de los trabajadores con fines de control laboral y establecer a la desconexión digital como una salvaguardia de este tipo de tratamiento de datos geolocalizados en el contexto laboral.[215]

-En una Directiva que emita la ANPDP, con carácter obligatorio. La ANPDP tiene competencia normativa, de conformidad con lo dispuesto por el artículo 33º, inciso 12) de la Ley, en virtud de la cual puede emitir directivas que permitan la mejor aplicación de la Ley y el Reglamento.

La ANPDP, como se ha señalado, ya ejerció esta competencia el año 2020 con la Directiva N.º 01-2020-JUS/DGTAIPD, aprobada mediante la Resolución Directoral N.º 02-2020-JUS/DGTAIPD, denominada "Tratamiento de datos personales mediante

[214] Título II. Tratamiento de datos personales.
[215] En el Reglamento no consideramos apropiado regular la desconexión digital como un derecho independiente, pues el Reglamento no es una norma que reconoce derechos, sino que regula los reconocidos en la Ley, o en todo caso desarrolla algún aspecto de la misma.

sistemas de videovigilancia", la misma que incluye un apartado sobre la videovigilancia para el control laboral; no refiriéndose, porque escapaba de su objetivo temático, al tratamiento de los datos geolocalizados de los trabajadores.

En una Directiva como la señalada, también podría atenderse la regulación específica sobre el tratamiento de los datos geolocalizados de los trabajadores con fines de control laboral; en este supuesto la desconexión digital, no podría ser reconocida como derecho, sino que podría establecerse como una medida de salvaguardia, dentro las otras necesarias para un debido tratamiento delos datos geolocalizados de los trabajadores. Lo señalado, es en atención a que es propio de la naturaleza jurídica de una directiva, emitir disposiciones para la mejor aplicación de la Ley y del Reglamento.

En cualquiera de los supuestos planteados, las disposiciones que se emitieran sobre el tratamiento de los datos geolocalizados de los trabajadores con fines de control laboral serían de obligatorio cumplimiento tanto para el empleador, en su calidad de responsable del tratamiento; para los encargados del tratamiento, de ser el caso; así como para el trabajador, responsable de la gestión de su información personal; por supuesto previa información y la capacitación correspondiente.

### 3.7.2. Normativa interna de la empresa

Una opción que tiene el empleador para dotar de mayor transparencia y seguridad al tratamiento de los datos personales de sus trabajadores en general y en particular a los datos geolocalizados con fines de control, es introducir en el Reglamento Interno de Trabajo, en delante RIT, las medidas específicas que definan su política de tratamiento de dichos datos personales.

Conforme al Decreto Supremo N.º 039-91-TR, se establece que el RIT determina las condiciones a las que deben sujetarse los empleadores y trabajadores en el cumplimiento de sus prestaciones.

Dentro de las disposiciones que deberá contener el RIT, según el artículo 2 del Decreto Supremo citado, se encuentran, de manera enunciativa: los derechos y obligaciones del trabajador y del empleador, y las normas tendientes al fomento y mantenimiento de la armonía entre trabajadores y empleadores.

Creemos que las normas sobre el tratamiento de los datos personales de los trabajadores por parte del empleador se refieren a derechos de ambas partes de la relación laboral y al estar en el RIT contribuirían al fomento y mantenimiento de la armonía de la relación entre los trabajadores y los empleadores, pues se tendría en una normativa vinculante al interior de la empresa, sino todas, por lo menos las normas básicas de cumplimiento o de cómo se cumplirían las disposiciones de la Ley y del Reglamento.

Si bien es cierto que la obligación de contar con el RIT es para la empresa que cuente con más de 100 trabajadores; por lo menos los trabajadores de estas empresas, tendrían el tipo de tratamiento de datos personales geolocalizados ya regulado y con ello una mayor garantía de ejercicio del derecho conforme a la Ley; claro, esto no excluye a las empresas con menor número de trabajadores, que no están obligadas para contar con un RIT, en las cuales esta posibilidad sería aún más remota. En todo caso, el RIT, si es obligatorio que se entregue a los trabajadores; así como su modificación.

El hecho que se optara por incluir en el RIT normas sobre el tratamiento de los datos personales de los trabajadores, no eximiría al empleador de implementar documentos específicos para cumplir, por ejemplo, con el aviso de información sobre el tratamiento de los datos geolocalizados con fines de control laboral; o con un documento de seguridad de la información, entre otros; los que sin duda deberán detallar más de lo que pueda señalar el RIT, según su temática correspondiente.

### 3.7.3. Regulación consensual

En el Perú donde no hay referencia normativa específica sobre el tratamiento de los

datos geolocalizados de los trabajadores, la negociación colectiva puede ser una de las vías, con respecto a las empresas que mediante ella, arriben a un convenio colectivo, para suplir en alguna medida, esta situación.

Palomeque López señala que la negociación colectiva es "[…] el proceso formalizado de diálogo entre representantes de trabajadores y de empresarios encaminado, en ejercicio de su autonomía colectiva, a la consecución de un convenio colectivo regulador de las relaciones entre ambos, así como de las condiciones a que han de ajustarse los contratos de trabajo, en un ámbito determinado" (1994: 351).

La Constitución Política de 1993, reconoce como uno de los derechos laborales específicos al de la negociación colectiva; lo hace en su artículo 28., en cuyo inciso 2) señala lo siguiente: "El Estado reconoce los derechos de sindicación, negociación colectiva y huelga. Cautela su ejercicio democrático: […] 2. Fomenta la negociación colectiva y promueve formas de solución pacífica de los conflictos laborales. La convención colectiva tiene fuerza vinculante en el ámbito de lo concertado".

La Ley de Relaciones Colectivas de Trabajo, cuyo texto único ordenado fue aprobado por el Decreto Supremo N.º 010-2003-TR, en adelante LRCT; en su artículo 41º, señala que la convención colectiva de trabajo es un acuerdo entre los representantes de los trabajadores, sindicalizados o no, y el empleador, sea uno, o un grupo de ellos u organizaciones de empleadores. El destino del convenio colectivo es en general, regular las relaciones entre trabajadores y empleadores. Por lo que es perfectamente posible regular el ejercicio de la facultad de control laboral, de manera particular si se ejerce a través de dispositivos tecnológicos invasivos como el GPS.

En atención a la ausencia regulatoria sobre el particular en nuestro país, cualquier convenio colectivo que aborde el tema, ya suma en la mejor tutela de los derechos involucrados de los trabajadores.

Los convenios colectivos, en los supuestos de las empresas que previa negociación con los representantes de los trabajadores, adoptaran algunas medidas protectoras frente a los riesgos del uso de los datos geolocalizados de los trabajadores con fines de control, tendrían un acuerdo que gozaría de "fuerza vinculante en el ámbito de lo concertado". Tal como lo ha señalado la Constitución y lo ratifica el artículo 42º de la LRCT. Por lo que no podrían ser desconocidas por el empleador las obligaciones derivadas de un convenio colectivo.

También es evidente que la naturaleza propia de la negociación colectiva y del acuerdo o convenio colectivo es opcional, no se puede imponer; no obstante, se presenta como una vía válida para adoptar normas que constituyen parte de una política sana y responsable para el uso de los datos geolocalizados de los trabajadores, que coadyuven al pleno respeto de los derechos y dignidad de estos, en lo que corresponde al uso de su información personal por un medio tecnológico como el GPS.

Sobre el particular, resulta útil tener en cuenta que, España, su Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, contiene un artículo sobre los derechos digitales en la negociación colectiva, el artículo 91; en él se señala que: "Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral".

La Ley española se refiere a "garantías adicionales" puesto que la situación normativa de la protección de datos de los trabajadores en dicho país difiere a la que existe en el nuestro. En efecto, como se ha señalado, el artículo 91 español, es solo uno de los 19 artículos que conforman el Título X "Garantía de los derechos digitales" de la Ley española".

En esta variedad de artículos mencionados, se establecen disposiciones orientadas

a salvaguardar los derechos a la intimidad personal y familiar, al respeto del tiempo fuera del trabajo, al descanso, permiso, vacaciones, a través del uso responsable de los datos personales de los empleados en el contexto laboral y que además son captados por dispositivos digitales, tales como la videovigilancia, y el GPS.

Tomando en alguna medida la normativa española referida, así como distintas acciones que permitirían al empleador, como responsable del tratamiento de datos personales, actuar con mayor responsabilidad en su calidad de tal; un convenio colectivo, en relación al objetivo del presente trabajo, podría referirse a lo siguiente:

-Informar a los representantes de los trabajadores antes de la implantación del GPS como mecanismo de vigilancia.

-Que los representantes de los trabajadores participen en la elaboración de la política y de los criterios de utilización del GPS que establezca el empleador.

-Antes de implementar el GPS, como mecanismo de control, concederles una audiencia y/o pedirles su opinión a los representantes de los trabajadores.

-Que se señale que los trabajadores tendrán derecho a la protección de su intimidad, llegándose a establecer límites razonables al uso del GPS.

-Reconocer el derecho a la desconexión del GPS fuera de la jornada de trabajo lo que incluye los espacios temporales de permisos, refrigerio, vacaciones, u otros.

-Establecer y aplicar un programa de capacitación y toma de conciencia sobre las obligaciones en materia de protección de datos personales de los trabajadores no sólo de los que son objeto de control sino también de los que tienen alguna participación en el tratamiento de los datos geolocalizados.

-Garantizar permanentemente la actualización de su política de acuerdo con la evolución tecnológica y teniendo en consideración la opinión de los representantes de los trabajadores.

Si bien es cierto, que en virtud al derecho – deber de información, a cargo del empleador, este está obligado a informar de manera clara, expresa, indubitable y de manera previa sobre todas las condiciones del tratamiento al que serán sometidos

los datos personales; sería conveniente establecer que para aplicar la facultad disciplinaria y eventual sanción usando los datos geolocalizados de los trabajadores, esto deberá ser motivo de una comunicación específica previo a la implantación del sistema GPS, o a la recolección de los datos con esa finalidad.

Es cierto que estos acuerdos supondrán un costo para el empleador; pero no tanto por lo que implica el proceso de negociación colectiva, sino fundamentalmente por lo que implica adecuarse a lo que manda la Ley y el Reglamento; así como las consecuencias que traería un uso inadecuado de la información personal de los trabajadores y violatorio de la normatividad sobre la materia; las que serían no sólo económicas sino de prestigio y pérdida de confianza en el marco de las relaciones laborales.

Esto dependerá de la toma de conciencia de la responsabilidad que tiene el empleador sobre los derechos de los trabajadores en juego y en equilibrio con los fines empresariales.

Dentro del objetivo de contar con políticas responsables en materia de protección de datos personales; otro uso que se le puede dar a la negociación colectiva, podría ser como un mecanismo para aplicar el principio de proporcionalidad ayudando a decidir qué acciones resultan proporcionadas a la finalidad de control laboral de los datos geolocalizados; con el objetivo de arribar a un acuerdo sobre la manera de conciliar y buscar un equilibrio entre los intereses del empleador y los de los trabajadores.

Es importante tener en cuenta que la apuesta que se hace por implementar una cultura de la protección de datos personales en toda organización, debe expresarse en acciones concretas, que lleven a traducirse en un real respeto del derecho a la protección de los datos personales; que denote un tratamiento no solo legal de la información; sino también, ético y de buena fe.

## CONCLUSIONES

-En el Perú el derecho recocido en el artículo 2º, inciso 6) de la Constitución Política de 1993, puede ser denominado como derecho a la protección de datos personales o como derecho a la autodeterminación informativa.

-Las facultades que el derecho a la protección de datos personales le otorga a su titular comprenden: la disposición, que se traducirá en el consentimiento; y el control de su información, que se concretará en los denominados derechos ARCO.

**-**El contenido del derecho a la protección de datos personales se delimita a través de los derechos ARCO y de los principios rectores de la protección de datos personales.

-La incorporación de los elementos tecnológicos que vienen a multiplicar y a potenciar la facultad de control empresarial, sin que la legislación haya adoptado una posición al respecto, acentúan la asimetría que por naturaleza existe en la relación laboral, en desventaja del trabajador.

-Es preciso complementar el ejercicio del poder de dirección empresarial y sus facultades, con otras normas que están fuera del ámbito laboral; como la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento, en la medida que corresponda.

-El derecho a la protección de datos personales, como derecho laboral inespecífico del trabajador, en su calidad de derecho fundamental autónomo, se instituye como un límite preciso y acorde en el contexto de la sociedad de la información y del conocimiento, frente al ejercicio de la facultad de control empresarial.

-En el Perú tenemos un contexto de carencia legislativa sobre el uso de la tecnología

del GPS para el tratamiento de datos personales en el contexto laboral en general; y en específico, para controlar a los trabajadores.

-El tratamiento de los datos geolocalizados de los trabajadores, con fines de control laboral, no ha sido materia de ninguna sentencia del Tribunal Constitucional.

-El tratamiento de los datos geolocalizados de los trabajadores, con fines de control laboral, no ha merecido pronunciamiento de la Autoridad Nacional de Protección de Datos Personales.

-En lo que respecta al Poder Judicial, la alusión al GPS como mecanismo de control laboral se ha dado en: tres sentencias de casación, a través del voto dirimente; un pleno regional laboral; y en dos sentencias de procesos sobre despido arbitrario; sin embargo, en ninguno de los casos señalados, se analizó el uso del GPS como mecanismo de control laboral, desde la perspectiva y lo que manda la Ley de Protección de Datos Personales y su Reglamento.

-Ley de Protección de Datos Personales y su Reglamento, con sus disposiciones generales, son lo único que puede guiar hasta el momento, a los empleadores cuando ejercen su facultad de control mediante el uso de los datos geolocalizados de sus trabajadores.

-La facultad de fiscalizar mediante GPS, no podrá entenderse como legítima para controlar a todos puestos de trabajo de una empresa.

-Cuando el empleador elija la geolocalización como medida de control laboral; deberá, en primer lugar, someterla al principio constitucional de proporcionalidad; para luego de superado el mismo, evaluar su implementación definitiva, previa adecuación a la normativa del derecho a la protección de datos personales.

-En el contexto de la relación laboral, el empleador puede, sin el consentimiento de sus trabajadores, tratar sus datos personales para ejercer las facultades derivadas de su poder de dirección; dentro de las cuales se encuentra la de fiscalizar.

-La no exigencia del consentimiento es de lo único de lo que se lo exime al empleador, con relación a la normativa sobre protección de datos personales, a la hora de realizar el tratamiento de los datos geolocalizados de sus trabajadores, con fines de control.

-Si el empleador requiere realizar el tratamiento de los datos geolocalizados para una finalidad que no es necesaria para la ejecución de la relación laboral; en principio y a la luz de nuestra legislación, podrá hacerlo siempre que cuente con el consentimiento de sus trabajadores.

-Al tratarse los datos personales de los trabajadores por medio del GPS, va a ser posible captar más información de la necesaria para la finalidad de control; y con ello, pueden verse afectados otros derechos; tales como, a la intimidad, al honor, a la paz, al descaso y al libre desarrollo de la personalidad.

-La descripción de la finalidad de fiscalizar para sancionar, debe quedar claramente determinada y ser previamente informada, para que el empleador pueda tratar los datos geolocalizados del trabajador con ese fin.

-Por el principio de proporcionalidad, la información personal geolocalizada, que se trae del trabajador, debe ser la estrictamente necesaria para el control laboral.

-El principio de finalidad acompaña todo el ciclo de vida del dato geolocalizado, desde la recogida hasta su supresión. Cumplida la finalidad del control laboral, mediante el tratamiento del dato localizado, queda agotada la legitimidad del empleador para continuar con dicho tratamiento.

-El tiempo de conservación de los datos geolocalizados con fines de control laboral debe ser muy limitado. Ante la ausencia de regulación, el empleador deberá establecer un tiempo razonable a la luz de los principios rectores de la protección de datos personales.

-El empleador debería implementar un protocolo de cancelación de la información geolocalizada excesiva para el control laboral. Debiendo además establecer, como parte de ese protocolo auditorías y revisiones periódicas de su cumplimiento.

-Las salvaguardas que puede implementar el empleador para la adecuación del tratamiento de los datos geolocalizados de los trabajadores, con fines de control laboral, pueden traducirse en políticas del tratamiento de los datos personales en general y en especial de los datos geolocalizados; en protocolos sobre el tratamiento de este tipo de datos y en actividades de capacitación del personal.

-Las empresas que brindan los servicios de geolocalización, como encargadas de tratamiento, están prohibidas de manera específica de utilizar dichos datos más allá de lo que diga el contrato de encargo celebrado con el empleador.

-El cumplimiento del deber de confidencialidad supone que los datos geolocalizados de los trabajadores solo sean conocidos por el titular del dato y por aquéllas personas de la organización cuyo perfil les permite acceder a dicha información. Esto puede ser atendido con una política de gestión a seguir por el personal involucrado.

-Parte del cumplimiento del principio de legalidad implica que, de manera previa a la recopilación de los datos geolocalizados de los trabajadores, el empleador deberá haber inscrito en el Registro Nacional de Protección de Datos Personales un banco donde conste que va a tratar dichos datos con fines de control.

-El tratamiento de datos personales de los trabajadores a través de la tecnología de la geolocalización, no debe suponer una flexibilización o rebajar el estándar de protección del derecho a la protección de datos personales.

-Como una forma de llenar el vacío legislativo y la ausencia de criterios tanto jurisprudenciales, como provenientes de la ANPDP, en relación a los datos

geolocalizados de los trabajadores con fines de control laboral, podrían incorporarse las condiciones para la utilización de sistemas de geolocalización en el ámbito laboral, desde alguno de los siguientes tres niveles regulativos: en la Ley; en el Reglamento; o en una Directiva que emita la ANPDP, con carácter obligatorio.

-A nivel de la empresa, el empleador podría optar por introducir en el Reglamento Interno de Trabajo, las medidas específicas que definan su política de tratamiento de los datos personales geolocalizados de sus trabajadores con fines de control laboral.

- A nivel de la regulación consensual, se podrían utilizar los convenios colectivos, para adoptar algunas medidas protectoras frente a los riesgos del uso de la tecnología del GPS con fines de control; posibilitando con ello tener un acuerdo que gozaría de "fuerza vinculante en el ámbito de lo concertado".

## BIBLIOGRAFÍA


AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

2019 Guía de privacidad desde el diseño. Consulta al 26 de febrero de 2021. https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

BLANCAS, Carlos

2007 Derechos fundamentales de la persona y relación de trabajo. Lima: Fondo Editorial Pontifica Universidad Católica el Perú.

BARRÍA, Dayana.

2009 El poder de dirección del empresario y los derechos fundamentales del trabajador: el control del uso del correo electrónico y de internet en la empresa. Memoria para optar al grado de licenciado en ciencias jurídicas y sociales. Santiago de Chile: Universidad de Chile. Consulta: 13 de setiembre de 2020. http://repositorio.uchile.cl/bitstream/handle/2250/106908/de-barria_d.pdf?sequence=3&isAllowed=y

COMISIÓN DE CONSTITUCIÓN Y DE REGLAMENTO

1993 Debate Constitucional. Tomo I. CONGRESO CONSTITUYENTE DEMOCRÁTICO. Lima. Consulta: 10 de junio de 2020. http://spij.minjus.gob.pe/TextosPDF/Constitucion-1993/ComConstReglam93/Tomo_I.pdf

COMITÉ JURÍDICO INTERAMERICANO DE LA OEA

2015 Informe sobre privacidad y protección de datos personales. Consulta: 18 de noviembre de 2020. http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

CONSEJO DE EUROPA

2018 El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado. Bruselas: Servicios de Estudios del Parlamento Europeo. Consulta: 10 de octubre 2020. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf

DE VICENTE, Fernando

2005 "Las facultades empresariales de vigilancia y control en las relaciones de trabajo: concepto y fundamento". Una primera aproximación a las diversas formas de control empresarial. Valencia: CISSPRAXIS. S.A., pp. 17-47.

FERNÁNDEZ, José y Victoria RODRÍGUEZ-RICO

2016 Nuevas tecnologías y control empresarial de la actividad laboral es España. Vol. 2, N° 1. Granada: Labour&Law issues. Consulta: 10 de diciembre de 2020.
https://labourlaw.unibo.it/article/download/6197/5970/18415

GARCÍA, Ana.

2015 Necesidades empresariales y derechos fundamentales de los trabajadores. Valladolid: Thomson Reuters.

GARCÍA, José

1981 "Artículo veinte. Dirección y control de la actividad laboral" en AA.VV., El estatuto de los trabajadores. Comentarios a la Ley 8/1980, de 10 de marzo. Madrid: Edersa. 1981

GARCÍA, Olga.

2016 La protección de datos de carácter personal en la gestión de los recursos humanos de la empresa. Tesis doctoral. Sevilla: Universidad Pablo de Olavide. Consulta: 08 de junio de 2020. https://rio.upo.es/xmlui/bitstream/handle/10433/3054/garcia-coca-_tesis16.pdf?sequence=1&isAllowed=y

GOERLICH, José

2016 "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas". El derecho a la privacidad en un nuevo entorno tecnológico. Cuadernos y debates N° 248. Madrid: Centro de estudios políticos y constitucionales. pp. 123.150.

GOÑI, José

2009 "Controles empresariales: geolocalización, correo electrónico, internet, videovigilancia y controles biométricos". Justicia laboral: Revista de derecho del trabajo y de la seguridad social. Madrid, número 39, 2009. pp. 11-58.

1988 El respeto a la esferas privada del trabajador. Madrid: Civitas.

GONZÁLEZ, Ortega.

2019 "Las facultades de control a distancia del trabajador: geolocalizadores y Tacógrafos". Revista andaluza de trabajo y bienestar social. Sevilla, número 150, pp. 45-70. Consulta: 10 de diciembre de 2020. https://www.juntadeandalucia.es/empleo/carl/carlportal-portlets/documentos?nombre=2b21c38c-9049-41d0-b85b-c5690438dc18.pdf

GRUPO DE TRABAJO SOBRE PROTECIÓN DE DATOS DEL ARTÍCULO 29

2017 Dictamen sobre el tratamiento de datos en el trabajo 2/2017

2005 Dictamen sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido 5/2005

2001 Dictamen sobre el tratamiento de datos personales en el contexto laboral 8/2001

HERNÁNDEZ, Lourdes y Lourdes ZAMUDIO

2020 "Protección de datos en el ámbito laboral". Diploma experto, especialización y Máster. Reglamento General de Protección de Datos. Madrid, Módulo 16. Consulta: 25 de octubre de 2020. https://formacionpermanente.uned.es/tp_actividad/idactividad/10845.

LANDA, César.

2017 Los derechos fundamentales. Lima: Fondo editorial de la Pontificia Universidad Católica del Perú.

LÓPEZ, Rafael

2005 "Las nuevas condiciones de trabajo y el lugar de prestación de servicios". Derecho social y nuevas tecnologías. Madrid: Consejo General del Poder Judicial, pp 75-128.

LUCAS MURILLO DE LA CUEVA, Pablo y José PIÑAR.

2009 El derecho a la autodeterminación informativa. Madrid: Fundación Coloquio Jurídico Europeo. Consulta: 30 de noviembre 2020. http://www.fcjuridicoeuropeo.org/wp-content/uploads/file/Libros_Publicados/Cuadernos_Fundacion/EL%20DERECHO%20A%20LA%20AUTODETERMINACION%20INFORMATIVA.pdf

MONTOYA, Alfredo.

1965 El poder de dirección del empresario. Madrid: Instituto de estudios políticos.

MORENO, Nieves.

2019 “Las facultades de control fuera de la jornada de trabajo :Desconexión digital y control del trabajador”. Revista andaluza de trabajo y bienestar social. Sevilla, número 150, pp. 161-185. Consulta: 11 de diciembre de 2020. https://www.juntadeandalucia.es/empleo/carl/carlportal-portlets/documentos?nombre=2b21c38c-9049-41d0-b85b-c5690438dc18.pdf

OBANDO, José

2016 Derecho laboral. Bogotá:Editorial Themis S.A.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO

2019 Trabajar para un futuro más prometedor. Comisión mundial sobre el futuro del trabajo. Consulta al 20 de enero de 2021. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_662442.pdf

PALOMEQUE, Manuel

1994 Derecho sindical español. Madrid: Editorial Tecnos S.A.

1991 Los derechos laborales en la Constitución española. Madrid: Centro de Estudios Constitucionales.

PIÑAR, José

2005 “El derecho fundamental a la protección de datos personales”. Protección de datos de carácter personal en Iberoamérica. Valencia: Tirant Lo Blanch, pp.19-36.

PLENO DEL CONGRESO CONSTITUYENTE DEMOCRÁTICO

1993 Diario de los Debates del Pleno. Tomo I. Lima. Consulta: 24 mayo de 2020. http://spij.minjus.gob.pe/Textos-PDF/Constitucion_1993/DebConst-Pleno93/DebConst-Pleno93TOMO1.pdf

POQUET, Raquel.

2013 El actual poder de dirección y control del empresario. Pamplona: Thomson Reuters.

PRECIADO, Carlos

2017 El derecho a la Protección de Datos en el Contrato de Trabajo. Navarra: Thomson Reuters.

PUENTE, Agustín

2005 “Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal”. Protección de datos de carácter personal en Iberoamérica. Valencia: Tirant Lo Blanch, pp.55-59.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

2017 Estándares de Protección de Datos Personales para los Estados Americanos. Consulta: 19 de febrero de 2021.
https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

RODOTÁ, Stefano

2003 “Democracia y protección de datos”. Cuadernos de Derecho Público. Madrid: Instituto Nacional de Administración Pública. pp.15.26. Consulta: 12 de setiembre 2020.
https://revistasonline.inap.es/index.php/CDP/article/view/690/745

RODRÍGUEZ, Susana.

2006 Vigilancia y control en la relación de trabajo: la incidencia de las nuevas tecnologías. Madrid: Ediciones Cinca, S.A. Comisión de Libertades e Informática y Fundación Francisco Largo Caballero.

TOSCANI, Daniel y Antonio VALENCIANO.

2016 Derechos fundamentales inespecíficos de los trabajadores. España: Editorial Bomarzo.

TRONCOSO, Antonio.

2003 La protección de datos personales. Una reflexión crítica a la jurisprudencia constitucional. Cuadernos de Derecho Público. Madrid: Instituto Nacional de Administración Pública. pp.231-334.Consulta: 1 de setiembre 2020. https://revistasonline.inap.es/index.php/CDP/article/view/698/753.

ZABALLOS, Emilia.

2013 La protección de datos personales en España: evolución normativa y criterios de aplicación. Memoria para optar el grado de doctor. Madrid: Facultad de derecho de la Universidad Complutense. Consulta: 10 de mayo 2020. https://eprints.ucm.es/id/eprint/22849/1/T34733.pdf

ZAMUDIO, María de Lourdes.

2014 “La Ley de protección de datos personales peruana. Reflexiones comparativas”. Régimen Jurídico de los datos personales. T. II. Buenos Aires: ABELEDO PERROT. pp. 1159 – 1162.

2012 “El marco normativo latinoamericano y la Ley de Protección de Datos Personales del Perú”. Revista de la Red Académica Internacional de Protección de Datos Personales. Bogotá, 2012, N° 1, Julio-diciembre Consulta: 10 de abril de 2020. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf