10.18800/themis.202101.025

LAS NUEVAS TECNOLOGÍAS Y LA PROTECCIÓN DE DATOS EN EL ENTORNO LABORAL: RETOS Y PERSPECTIVAS LEGALES

NEW TECHNOLOGIES AND DATA PROTECTION IN THE WORKPLACE: CHALLENGES AND LEGAL PERSPECTIVES

Iván Blume Moore*
Rodrigo, Elías & Medrano

Information and communications technologies, known as ICT, have undoubtedly contributed to the development of societies through the multiplication of data processing and storage in everyday relationships. At the same time and notwithstanding, it is not possible to ignore the risks that these have caused, in relation to the lack of security of personal data. This situation has generated the development of regulatory frameworks aimed at counteracting such risks. Among these regulations, there are the ones relating to the workplace.

In this article, the author reviews the novelties brought about by the entry into force of the Personal Data Protection Law (Law 29733) in Peruvian law. Subsequently, he points out and describes the basic concepts involved in the topic of personal data protection. In a third section, he develops the obligations of employers regarding the protection of personal data and the challenges that this faces in the face of global changes. Finally, he illustrates all this through cases of jurisprudence.

Keywords: Personal data protection; Information and Communication Technologies; Personal Data Protection Law; employer; worker; employment relationship.

Las tecnologías de información y comunicación, conocidas como TIC, han aportado, sin duda alguna, al desarrollo de las sociedades a través de la multiplicación del procesamiento y almacenamiento de datos en las relaciones cotidianas. Sin perjuicio de ello, y en contrapartida, no es posible desconocer los riesgos que, al mismo tiempo, aquellas han causado, relativos a la falta de seguridad de los datos personales. Esta situación ha generado el desarrollo de marcos normativos destinados a contrarrestar tales riesgos. Entre esta normativa, se encuentra aquella relativa al ámbito laboral.

En el presente artículo, el autor revisa las novedades que trajo consigo la entrada en vigencia de la Ley de Protección de Datos Personales (Ley 29733) en el ordenamiento peruano. Posteriormente, señala y describe los conceptos básicos que intervienen en el tópico de la protección de datos personales. En una tercera sección, desarrolla las obligaciones de los empleadores frente a la protección de datos personales y los desafíos que ello enfrenta ante los cambios globales. Por último, ilustra todo ello a través de casos de la jurisprudencia.

Palabras clave: Protección de datos personales; tecnologías de información y comunicación; Ley de Protección de Datos Personales; empleador; trabajador; relación laboral.

* Abogado. Máster en Relaciones Industriales y Laborales por la Universidad de Cornell. Asociado en el Estudio Rodrigo, Elías & Medrano (Lima, Perú). Contacto: iblume@estudiorodrigo.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 1 de febrero de 2021, y aceptado por el mismo el 16 de junio de 2021.

I. INTRODUCCIÓN

La multiplicación del procesamiento y almacenamiento de datos a partir de las relaciones e interacciones cotidianas es una de las muchas formas en que las tecnologías de información y comunicación (en adelante, TIC) han transformado nuestras vidas. Al tiempo que nos han facilitado la vida cotidiana y ampliado el acceso a la información, también han generado riesgos relacionados principalmente con el uso incontrolado y la falta de seguridad de los datos personales. Esto a su vez ha llevado al surgimiento de marcos normativos para hacerle frente a esos riesgos, de los que se desprenden relativamente nuevas obligaciones y responsabilidades legales para quienes intervienen en el tratamiento de datos personales.

En el ámbito laboral, por ejemplo, la mediación de dichas tecnologías incluye procesos tan diversos como la gestión de personal, las comunicaciones internas y externas y las formas de monitoreo y control del trabajo, entre otras. Por efecto de todo ello, los empleadores captan, procesan y almacenan una gran cantidad de datos e información sobre sus trabajadores. En todos esos procesos deben asegurarse de cumplir con lo dispuesto en las normativas sobre protección de datos.

En el Perú se cuenta desde el 3 de julio de 2011 con la Ley 29733, Ley de Protección de Datos Personales (en adelante, LPDP), que define los conceptos básicos que se deben tener en cuenta en esta materia. Sin embargo, el desarrollo legislativo y jurisprudencial no logra ir siempre al paso de los avances de las TIC, ni de los dilemas que surgen de sus aplicaciones en todos los ámbitos de las relaciones sociales, incluyendo al trabajo. Ello plantea una serie de retos jurídicos y tecnológicos sobre cómo garantizar de manera efectiva el derecho a la protección de datos de los trabajadores, así como sobre sus alcances y límites frente a otros derechos y obligaciones que emergen de las relaciones laborales.

En este artículo nos proponemos revisar algunos de esos retos a partir de desarrollos normativos y jurisprudenciales recientes sobre el alcance de la protección de datos personales en casos específicos de aplicaciones tecnológicas que se enmarcan o son relevantes dentro del contexto laboral. Examinaremos estos casos a la luz de los principios consagrados en el marco legal vigente y de los criterios básicos sobre las obligaciones frente al derecho a la protección de los datos personales que se desprenden de la legislación nacional. Asimismo, nos ocuparemos en especial de las orientaciones generales formuladas por la Organización Internacional del Trabajo (en adelante, OIT) y de la guía recientemente publicada por la Agencia Española de Protección de Datos (en adelante, AEPD) sobre la protección de datos en las relaciones laborales. El propósito no es hacer un estudio comparado de la legislación internacional, sino ofrecer un panorama general de los conceptos fundamentales que se deben tener en cuenta al abordar estos temas dentro del ámbito laboral, así como llamar la atención sobre algunos temas novedosos o poco desarrollados que merecen mayor atención en nuestro país.

Con este fin, dividimos este artículo en cuatro secciones. En la primera, nos referiremos a las novedades que introdujo la LPDP en el ordenamiento jurídico peruano y los antecedentes en los desarrollos jurídicos nacionales e internacionales que llevaron a su adopción. En la segunda sección, a partir de las definiciones contenidas en la LPDP y en su correspondiente reglamento, presentamos los conceptos básicos que fundamentan la regulación de la protección de los datos personales. La tercera se ocupa específicamente de las obligaciones de los empleadores frente a la protección de los datos personales de sus trabajadores y revisa los principales desafíos ante los cambios globales, no solo tecnológicos, sino sociales. Finalmente, en la última sección revisaremos tres casos que ilustran la aplicación de los principios generales presentados en las secciones anteriores a situaciones y aplicaciones tecnológicas específicas.

II. LA LEY DE PROTECCIÓN DE DATOS PERSONALES Y SUS ANTECEDENTES

Con la expedición de la LPDP, el Congreso peruano reconoció explícitamente la protección de datos personales como un derecho fundamental y se propuso regular su adecuado tratamiento tanto por las entidades públicas, como por las instituciones privadas (Ley 29733, 2011). Las disposiciones de esta ley y su correspondiente reglamento constituyen normas de orden público y de cumplimiento obligatorio[1].

Antes de la aprobación de la LPDP, el principal referente para la resolución de los conflictos en torno al tratamiento de datos personales era el inciso 6

[1] La LPDP establece lo siguiente:
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, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen (Ley 29733, 2011).

del artículo 2 de la Constitución Política que consagra el derecho de las personas "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" (Constitución Política del Perú [Const.], 1993). El inciso 7 del mismo artículo, además de consignar el derecho "al honor y a la buena reputación, a la intimidad personal y familiar", establece el derecho "a la voz y a la imagen propias" (Const., 1993). Adicionalmente, el inciso 4 del artículo 200 establece el proceso de *habeas data* para garantizar la protección de este derecho (Const., 1993).

Es decir, desde principios de los noventa el constituyente había identificado los potenciales riesgos que se derivaban de la capacidad de registro y almacenamiento de los datos personales por parte de medios audiovisuales e informáticos, pero enmarcaba la protección frente a dichos riesgos como una cuestión pertinente al derecho a la intimidad. Con la aprobación de la LPDP, no solo se desarrollan con mayor claridad las disposiciones constitucionales, sino que se introduce en el ordenamiento jurídico peruano la noción del derecho a la protección de datos como un derecho autónomo con un alcance que va más allá de la protección de la intimidad. Recoge así un concepto que ya había sido plasmado en la legislación de otros países y al que, incluso, ya habían hecho referencia algunas decisiones a nivel local.

Por ejemplo, el Tribunal Constitucional (en adelante, TC), en la sentencia sobre el proceso de *habeas data* tramitado bajo el Expediente 1797-2002-HD/TC, había señalado lo siguiente:

> […] 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 […]. 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 (2003, fundamento 3).

Como veremos, esta facultad de todo individuo de controlar sus datos personales es el principio básico de las normativas sobre protección de datos personales. La insuficiencia del derecho a la intimidad para garantizar dicha protección en el contexto tecnológico actual la explica Castro Cruzatt:

> […] en el contexto del creciente desarrollo informático y tecnológico se advirtió también que el registro indiscriminado de datos personales, su interrelación y posterior transmisión descontrolada, confiere un alto poder de control sobre los titulares de dichos datos, llegando a representar una nueva forma de dominio social a la que le ha denominado Poder Informático (2008, p. 261).

Es decir, hoy es tan extendido el uso la tecnología informática que los requerimientos de protección no pueden solamente limitarse a la necesidad de resguardar la intimidad, pues existen una serie de riesgos relacionados al uso masivo de la información de las personas que van desde el perfilamiento hasta los fraudes bancarios que hacen especialmente necesario la protección de los datos personales.

A este contexto busca precisamente responder el desarrollo normativo y jurisprudencial sobre la protección de datos personales. En Perú, el marco legal está conformado principalmente por la LPDP y su reglamento, aprobado por Decreto Supremo 003-2013-JUS (2013) (en adelante, Reglamento). Se han emitido además directivas sobre seguridad de la información y sistemas de videovigilancia[2].

III. CONCEPTOS BÁSICOS

La aplicación de la anterior normativa a casos específicos requiere tener clara una serie de conceptos básicos definidos por la LPDP y por su Reglamento. Presentamos a continuación un resumen de los conceptos más relevantes a modo de preguntas y respuestas.

A. ¿Qué es un dato personal?

Lo primero que se debe tener claro es la amplitud de esta denominación. Dentro de ella se incluye, según el inciso 4 del artículo 2 del Reglamento, "información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que pueden ser razonablemente utilizados" (Decreto Supremo 003-2013-JUS, 2013). Así, la LPDP solo protege los datos de personas naturales. Los datos de personas jurídicas no son parte de su ámbito de aplicación.

Los desarrollos tecnológicos han ido ampliando el listado de datos que pueden caber dentro de esta

[2] Véase, Resolución Directoral 019-2013-JUS/DGPDP, del 11 de octubre de 2013, y Resolución Directoral 02-2020-JUS/DGTAIPD, del 14 de febrero de 2020.

definición. Actualmente, por ejemplo, un dato personal de gran relevancia es la información de geolocalización. La Autoridad Nacional de Protección de Datos Personales (en adelante, ANPDP), en la Resolución Directoral 008-2017-JUS/DGPDP (2017), ha concluido que la geolocalización es un dato personal. Al respecto, ha señalado que

> […] debido al rápido desarrollo tecnológico que viene dándose en nuestra sociedad, los teléfonos móviles inteligentes o dispositivos electrónicos de naturaleza similar permiten la geolocalización y con ello la identificación de una persona, ya que con ellos se conoce el desplazamiento de un determínalo individuo. Esto último se da pues estos teléfonos móviles inteligentes o dispositivos electrónicos de naturaleza similar se mantienen cerca de la persona desde su bolsillo hasta la mesa de noche que se encuentra en su habitación. En consecuencia, 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, siendo de aplicación las disposiciones contenidas en la LPDP y su Reglamento (p. 14).

Los datos sensibles son objeto de especial protección (Ley 29733, 2011, art. 3). Dentro de estos se incluyen: información biométrica que permita la identificación de una persona; datos sobre identidad racial o étnica; información sobre la situación económica (ingresos, patrimonio, deudas, etc.); opiniones o adscripciones políticas o religiosas; afiliación sindical; datos sobre la salud física o mental; hechos que correspondan a la vida afectiva, familiar o a la esfera más íntima de las personas; entre otros.

En estos casos, el consentimiento debe ser otorgado por escrito y debe ser clara la justificación para recolectar, almacenar y tratar datos sensibles. Asimismo, de acuerdo con el Reglamento, la finalidad debe ser legítima, concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales (Decreto Supremo 003-2013-JUS, 2013).

B. ¿Qué es un banco de datos o base de datos personales?

Banco de datos es un "conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera sea la forma o modalidad de su creación, formación, almacenamiento, organización y acceso" (Ley 29733, 2011, art. 2 inciso 2). El titular de la base de datos personales puede ser una "persona natural o jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad" (Ley 29733, 2011, art. 2 inciso 15).

Sin que necesariamente sean conscientes de las obligaciones que se desprenden de ello, los empleadores son titulares de bases de datos con la información personal de sus trabajadores que recolectan y tratan en las diferentes etapas de la relación laboral. Son bases de datos típicas del entorno laboral los legajos de los trabajadores, la información de candidatos para los procesos de selección, la información de salud ocupacional de los trabajadores, los sistemas de videovigilancia, entre otros.

C. ¿Qué constituye un tratamiento de datos?

La LPDP y el Reglamento de la LPDP se aplican a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado, e independientemente del soporte en el que se encuentren (Decreto Supremo 003-2013-JUS, 2013, art. 3).

La LPDP define al tratamiento de datos personales como

> 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 (Ley 29733, 2011, art. 2 inciso 19).

D. ¿Cuáles son las principales obligaciones establecidas por la normativa de protección de datos?

Las principales obligaciones para cumplir con la normativa de protección de datos son las siguientes:

a) **Obtener consentimiento:** la protección de datos supone, en primer lugar, que todo 'tratamiento' se realice con el consentimiento previo, informado y expreso del titular, salvo excepciones establecidas por la ley. Así, el consentimiento relativo a datos sensibles debe ser obtenido por escrito. Se considera consentimiento escrito a aquel que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por el ordenamiento jurídico que queda o pueda ser impreso en

una superficie de papel o similar. Tratándose del entorno digital, el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito.

b) **Cumplir con el deber de información:** el titular del banco de datos debe dar a conocer al titular de los datos personales toda la información relevante sobre los usos y el 'tratamiento' que se le dará a estos. Se debe informar de manera completa y veraz antes de la recopilación de los datos[3].

c) **Asegurar la confidencialidad y la seguridad:** la responsabilidad por el manejo de los datos personales recae no solo sobre el titular del banco de datos, sino sobre todos los que intervengan en su tratamiento. Todos ellos están obligados a garantizar la confidencialidad y la seguridad de los datos personales. La responsabilidad se extiende más allá de la finalización de las relaciones con el titular del banco de datos personales. Esto supone la obligación de adoptar las medidas que sean necesarias, tanto técnicas como legales y organizacionales, para impedir la filtración, alteración o el uso inadecuado de esos datos.

d) **Conservar la información por tiempo limitado:** la protección implica también que los datos personales no se conserven más tiempo del necesario que se requiera para cumplir con la finalidad del tratamiento. El tiempo permitido de conservación depende del tipo de relación y de las correspondientes obligaciones legales y contractuales. Podemos decir que se pueden conservar mientras persistan las responsabilidades legales derivadas de dicha relación.

e) **Garantizar los derechos ARCO:** esta sigla se refiere a los derechos al acceso, rectificación, cancelación y oposición, que sintetizan los atributos del control que se le debe garantizar a las personas sobre sus datos personales. Cada uno de estos derechos está sujeto a sus propias formalidades.

f) **Inscripción de bases de datos:** los titulares de las bases de datos deben inscribirlos en el Registro Nacional de Protección de Datos Personales.

g) **Requisitos para el flujo de datos transfronterizo:** en caso de que los datos se transfieran fuera del territorio nacional, el titular de la base de datos debe informarlo a la autoridad nacional de protección de datos. Solo se puede realizar dicha transferencia a países que cuenten con una normativa apropiada de protección de datos. En caso contrario, se debe obtener el consentimiento informado del titular para realizar la transferencia y tomar medidas que garanticen que el tratamiento de los datos cumpla con los requisitos de la ley.

E. ¿Qué casos están exceptuados del consentimiento informado para el tratamiento de datos personales?

Enumeramos a continuación los casos previstos en la LPDP, en los cuales no se requiere el consentimiento del titular de datos personales[4]:

[3] El artículo 18 de la LPDP establece que

> 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 (Ley 29733, 2011).

Asimismo, el Reglamento establece que se le deberá comunicar al titular de los datos personales clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos lo siguiente:

a) La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.
b) La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.
c) La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
d) La existencia del banco de datos personales en que se almacenarán, cuando corresponda.
e) El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
f) Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
g) En su caso, la transferencia nacional e internacional de datos que se efectúen (Decreto Supremo 003-2013-JUS, 2013, artículo 12 inciso 4).

[4] Resumen tomado de Blume Moore (2021, pp. 275-276).

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 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 (Ley 29733, 2011, art. 14).

F. ¿Qué principios rigen el tratamiento de los datos personales según el marco legal?

Los principios que rigen el tratamiento de los datos personales, en concordancia con la normativa actual, son los siguientes:

> **Artículo 4. Principio de legalidad**: el tratamiento de los datos personales se hace conforme a lo establecido en la LPDP. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
>
> **Artículo 5. Principio de consentimiento:** para el tratamiento de los datos personales debe mediar el consentimiento de su titular.
>
> **Artículo 6. Principios 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 fue-

ron 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 la LPDP o por los estándares internacionales en la materia (Ley 29733, 2011, arts. 4-11) [el énfasis es nuestro].

IV. OBLIGACIONES DE LOS EMPLEADORES FRENTE A LOS DATOS PERSONALES DE SUS TRABAJADORES

Los principios que enunciamos en el punto anterior aplican en términos generales al ámbito laboral. Sin embargo, en el caso de las relaciones laborales, el empleador no requiere un consentimiento expreso cuando la finalidad del tratamiento se pueda enmarcar en las obligaciones previstas en el contrato de trabajo. Aunque no requiere consentimiento, sí está obligado a informarle al trabajador sobre el tratamiento que se les dará a los datos.

Sin embargo, en nuestro país la mayoría de empleadores no son conscientes de que en la relación con sus trabajadores actúan como titulares legales de bases de datos personales y que como tales son responsables de las obligaciones previstas en la LPDP. Cumplir con esas obligaciones implica tomar medidas para garantizar la seguridad y confidencialidad de los datos, así como para evitar su alteración, pérdida, tratamiento o acceso no autorizado. No tomarlas pone en riesgo la protección de derechos fundamentales de los trabajadores y expone a los empleadores a las correspondientes sanciones.

Por otro lado, son escasos los desarrollos normativos y la jurisprudencia sobre la aplicación del derecho a la protección de datos en el ámbito, y los requerimientos específicos de las relaciones laborales. Teniendo en cuenta lo anterior, es útil revisar algunos referentes internacionales. Por ejemplo, la publicación titulada Protection of Worker's Personal Data (International Labour Office Geneva, 1997) contiene una especie de código adoptado a principios de octubre de 1996 en una Reunión de Expertos de la OIT en materia de privacidad de los trabajadores, siguiendo las decisiones del Órgano de Gobierno de la OIT en su sesión de noviembre de 1995. En este documento se señala lo siguiente:

a) El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita, y limitarse exclusivamente a asuntos directamente pertinentes a la relación de empleo del trabajador.

b) En principio, los datos personales deberían utilizarse únicamente para el fin con el cual hayan sido acopiados.

c) Los empleadores deberían evaluar periódicamente sus métodos de tratamiento de datos, con el objeto de: (i) reducir lo más posible el tipo y el volumen de datos personales acopiados, y (ii) mejorar el modo de proteger la vida privada de los trabajadores.

d) Las personas encargadas del tratamiento de datos personales deberían recibir periódicamente una formación que les permita comprender el proceso de acopio de datos y el papel que les corresponde en la aplicación de los principios.

e) El tratamiento de datos personales no debería conducir a una discriminación ilícita en materia de empleo u ocupación.

f) Todas las personas, tales como los empleadores, los representantes de los trabajadores, las agencias de colocación y los trabajadores, que tengan acceso a los datos personales de los trabajadores deberían tener una obligación de confidencialidad, de acuerdo con la realización de sus tareas y el ejercicio de los principios de tratamiento de datos.

g) Los empleadores deberían garantizar, mediante las salvaguardias de seguridad que permitan las circunstancias, la protección de los datos personales contra su pérdida y todo acceso, utilización, modificación o comunicación no autorizados.

h) Los empleadores deberían verificar periódicamente que los datos personales conservados son exactos, actualizados y completos (International Labour Office Geneva, 1997).

Los rápidos desarrollos tecnológicos y la evolución de las relaciones sociales que permea también el ámbito laboral plantea una serie de retos no solo jurídicos, sino prácticos para el cumplimiento por parte del empleador de las normativas y principios generales en casos específicos. En este sentido, un referente que puede llegar a ser muy ilustrativo es la guía sobre la protección de datos personales en las relaciones laborales publicada recientemente por la AEPD. Dicha publicación no solo resume el nuevo marco normativo español y europeo sobre protección de datos, sino que proporciona orientaciones de carácter práctico, no vinculante, para facilitar el cumplimiento de la legislación.

Con ese fin, el documento fue elaborado con la participación tanto del Ministerio del Trabajo como de organizaciones empresariales y sindicales. Recoge además "la experiencia atesorada por la AEPD a lo largo de los años" (Agencia Española de Protección de Datos [AEPD], 2021, p. 6). Esto le permite ofrecer un panorama comprehensivo de las múltiples facetas de la gestión de personal y la relación laboral en las que surge la necesidad de la protección de datos personales.

Nos referiremos a algunas recomendaciones específicas que trae la guía en el siguiente apartado, cuando revisemos ejemplos de problemáticas concretas que surgen a partir de algunas aplicaciones informáticas. Vale la pena, sin embargo, mencionar de manera general los temas que introduce o desarrolla la guía y que pueden ser relevantes para nuestro medio (AEPD, 2021):

a) La necesidad de contar con estándares para el tratamiento de datos personales en los procesos de selección de personal. Se aclara que, dentro del marco legal español, el proceso de selección no exige el consentimiento de la persona candidata, pero que se debe cumplir con el deber de informar y las demás obligaciones propias del tratamiento de los datos personales. La empresa es responsable de la custodia de la documentación entregada por la persona candidata (como el *currículum vitae*) y será responsable por su pérdida, sustracción o el uso indebido de la información allí contenida.

b) El uso de la información de las redes sociales de los trabajadores. La guía aclara que, aunque el perfil en las redes sociales de un candidato a un empleo sea de acceso público, el empleador necesita una base jurídica válida para "efectuar un tratamiento de los datos obtenidos por esa vía" (AEPD, 2021, p. 22). Las personas no están obligadas a permitir que el empleador indague en sus perfiles de redes sociales, ni durante el proceso de selección ni durante la ejecución del contrato.

c) La protección de la privacidad de las víctimas de acoso laboral o de violencia de género, así como de quienes presentan cualquier tipo de denuncia interna. Estos son casos especialmente sensibles de protección de datos personales que obligan al empleador a implementar medidas y mecanismos que protejan la identidad de las personas involucradas.

d) El uso de los mecanismos lo menos invasivos posibles y la restricción de la publicación de la información obtenida a través de herramientas de control, como el registro de jornada obligatorio, los controles de ingreso, la georreferenciación o la videovigilancia (sobre esto último punto, profundizaremos más adelante).

e) Los riesgos y obligaciones frente a los datos personales derivados de la responsabilidad del empleador de velar por la salud de los trabajadores. En España, al igual que en Perú, esta responsabilidad faculta al empleador a realizar vigilancia periódica del estado de salud de sus trabajadores. Aspecto que ha adquirido una especial relevancia en el contexto de la pandemia y al que nos referiremos más adelante.

f) En términos de aplicaciones tecnológicas, lo más novedoso que incluye la guía es lo relativo al uso de algoritmos o sistemas de inteligencia artificial para tomar decisiones en cuanto al acceso (procesos de selección), condiciones y mantenimiento del empleo. La normatividad española obliga al empleador a informar sobre los parámetros en los que se basa el algoritmo y a tomar medidas que eviten que estos produzcan algún tipo de discriminación (AEPD, 2021).

V. DECISIONES RECIENTES SOBRE PROTECCIÓN DE DATOS EN SITUACIONES Y DESARROLLOS TECNOLÓGICOS ESPECÍFICOS

Aunque en nuestro país no es mucho lo que se ha avanzado en el establecimiento de reglas específicas para la protección de datos personales en situaciones o usos de tecnologías particulares, existen algunos desarrollos normativos y jurisprudenciales recientes que han empezado a abordar la problemática concreta que surge a partir de algunas aplicaciones informáticas, como los correos electrónicos, las redes sociales institucionales o la videovigilancia.

Por otro lado, la emergencia del COVID-19 puso al descubierto las tensiones que pueden surgir entre la necesidad de proteger la salud, evitando la propagación del virus, y el derecho a la protección de los datos personales. Esto obligó al gobierno a pronunciarse a través de una opinión consultiva sobre el tratamiento de datos de salud durante la pandemia en el ámbito laboral. Si bien en esta no se aborda directamente el uso de tecnologías, por su urgencia y actualidad consideramos pertinente examinar las principales consideraciones que el reto de controlar la epidemia plantea en cuanto a protección de datos personales y las obligaciones de los empleadores de velar por la salud de sus trabajadores.

Al respecto, revisaremos a continuación algunas decisiones jurisprudenciales o actos regulatorios recientes.

A. La inviolabilidad de las comunicaciones en tiempos del *e-mail* y las redes sociales

Si bien desde hace ya más de veinte años se generalizó el uso del correo electrónico como herramienta de trabajo de las empresas, persisten aún dudas sobre cómo se deben aplicar en el contexto actual los principios que protegían las comunicaciones antes de la era digital. Además del ya mencionado derecho a la intimidad, el principal referente para el tratamiento de las comunicaciones antes de que se considerara la protección de los datos personales como un derecho autónomo era el principio de la inviolabilidad de las comunicaciones. Desarrollado originalmente para evitar que alguien distinto al destinatario abriera la correspondencia, el principio se extendió más tarde a las comunicaciones telegráficas y telefónicas (Vegas Torres, 2011, p. 34). Atendiendo a dicho principio, las comunicaciones solo pueden ser interceptadas por terceros por orden de un juez y siguiendo un procedimiento regular.

Estos principios se extienden por analogía al correo electrónico. Sin embargo, su uso generalizado como herramienta laboral plantea algunas dudas sobre el alcance de este principio en dicho ámbito. En particular, ¿qué pasa con las comunicaciones que se realizan por medio de las cuentas institucionales o de los equipos de computación que la empresa entrega a los trabajadores? ¿son comunicaciones privadas protegidas por los principios de inviolabilidad de la correspondencia o del derecho a la intimidad? ¿O, al ser una herramienta de trabajo por medio de las cuales las empresas suelen llevar buena parte de sus procesos e interacciones, tiene derecho el empleador a acceder a esas comunicaciones como parte de sus funciones de control y supervisión del trabajo?

Tanto en nuestro país como en el ámbito internacional, esta disyuntiva ha conducido a un debate jurídico que aún no se ha resuelto del todo. La posición de varias sentencias del TC ha sido consistente en considerar que los trabajadores están protegidos por el principio de inviolabilidad de las comunicaciones, aun si se comunican a través de los equipos y las cuentas de correo suministrados por el empleador. El TC incluso ha declarado ilegal el despido o la sanción disciplinaria de un empleado por conductas que iban en contra del reglamento interno de trabajo (como enviar correos con material pornográfico en horarios laborales desde cuentas oficiales) porque la prueba de ese comportamiento se obtuvo accediendo al correo institucional sin acudir a un proceso judicial[5]. En años recientes, esta tendencia jurisprudencial ha sido ratificada por una controvertida decisión de la Corte Suprema (en adelante, CS). En respuesta a una demanda iniciada por el sindicato de una empresa, consideró como un 'exceso' que en el reglamento interno laboral el empleador señalara que era propietario de las cuentas de correo institucionales y que eso le permitía revisar su contenido para fines de control, pues ello desconocía el derecho a la intimidad e inviolabilidad de las comunicaciones de los trabajadores[6].

Sin embargo, algunas decisiones recientes parecen estar señalando un cambio, o al menos una matización, de esta línea jurisprudencial garantista. En efecto, en la sentencia recaída en el Expediente 00943-2016-PA/TC, discutido en el Pleno de Sentencia 412/2020 de 14 de julio de 2020, el TC consideró por primera vez la posibilidad del empleador de poder revisar los correos electrónicos que le ha proporcionado al trabajador para el desarrollo efectivo de sus actividades, sin vulnerar con ello derechos constitucionales. Aunque no hubo la mayoría necesaria para formar sentencia al respecto, los conceptos expresados por los magistrados parecen apuntar a una flexibilización en la interpretación del principio de inviolabilidad de la correspondencia aplicado a los correos y redes institucionales de las empresas[7].

[5] Para mayor información, véase la sentencia recaída en el Expediente 1058-2004-AA/TC (2020).

[6] Para mayor información, véase la Casación 14614-2016 (2017).

[7] En un proceso de amparo ante el TC, una sentencia se forma a partir del voto conforme de cuatro magistrados. En este caso, la sentencia fue declarada improcedente debido a que dos magistrados (Ledesma y Miranda) consideraron que el caso debió resolverse en la vía ordinaria laboral, y otros dos (Sardón y Ferrero) siempre han estimado que la protección

El caso corresponde a un proceso de reposición seguido en la vía de amparo. En este se invocaba la vulneración de los derechos constitucionales al trabajo, al secreto y la inviolabilidad de las comunicaciones, a la intimidad personal, entre otros. El trabajador denunció que, para imputarle las faltas, la empresa accedió a una conversación en Facebook entre su persona y una asistente de la empresa, interviniendo una conversación de carácter privado.

El TC reiteró la línea jurisprudencial en el sentido de que, aun cuando las cuentas y los equipos sean provistos por la compañía, el trabajador mantiene una esfera de privacidad y de autodeterminación personal en el uso que hace de ellos, por lo que la empresa no tiene la prerrogativa de atribuirse la titularidad de las comunicaciones y los documentos pertenecientes a las redes de sus trabajadores. Sin embargo, consideró algunas circunstancias en las que el empleador podría acceder a las comunicaciones de sus trabajadores en el marco de procesos de monitoreo laboral o de procesos disciplinarios, sin el requisito de una orden judicial. Para ello, tuvo en cuenta en la discusión algunos referentes internacionales.

Menciona, por ejemplo, que el Tribunal Europeo de Derechos Humanos ha establecido los siguientes criterios para determinar si el empleador puede monitorear la comunicación de sus trabajadores: (i) el trabajador debe ser informado previamente y con claridad de las medidas de control que la empresa puede utilizar (y el alcance de estas); (ii) el empleador debe optar por la acción menos intrusiva en la vida personal y familiar del trabajador; (iii) se debe acreditar la existencia de motivos objetivos y concretos que justifiquen la necesidad de fiscalizar las comunicaciones del trabajador; y (iv) la medida de fiscalización se debe llevar de forma previa al inicio del procedimiento disciplinario (*Bărbulescu c. Romania*, 2017).

Por su parte, el Tribunal Constitucional español ha establecido que: (i) el control o fiscalización se debe realizar con garantías (como, por ejemplo, a través de un petitorio informático y notario); (ii) el contenido fiscalizado no puede ser sobre aspectos personales y familiares del trabajador, sino únicamente de la actividad empresarial realizada; y (iii) debe existir proporcionalidad entre la posible infracción del trabajador y la afectación a su privacidad por parte de la actividad fiscalizadora de la empresas (STC 170/2013, 2013).

Teniendo en cuenta lo anterior, el TC peruano consideró que sí es posible intervenir o fiscalizar el correo institucional del trabajador si previamente se le ha comunicado de dicha posibilidad y de sus alcances, y si dicha intervención contempla criterios de proporcionalidad con relación al grado de afectación a la privacidad y al fin último de la intervención (en este caso, determinar una infracción del trabajador).

No obstante, para el TC, el empleador no puede ejercer esta prerrogativa si se trata del acceso a una red social del trabajador, puesto que es un medio de comunicación externo a los instrumentos que brinda el empleador. Aunque no profundiza mucho en este aspecto, la discusión dentro del órgano también pone en evidencia los retos que plantean las redes sociales y otras formas de interacción social por medio de tecnologías digitales para la aplicación de los principios de inviolabilidad de las comunicaciones y protección de la intimidad en el ámbito laboral.

Por ejemplo, será necesario revisar qué ocurre cuando no se trata de redes sociales personales del trabajador, sino de actividades de *community manager* en las redes sociales institucionales. Esta preocupación fue señalada por uno de los magistrados en el mencionado expediente[8], quien se apartó de la opinión mayoritaria sobre las redes sociales considerando que el empleador podría fiscalizar el uso de las redes institucionales de quien le esté prestando los servicios de *community manager*, con la finalidad de asegurar un grado de idoneidad en el servicio brindado al cliente y en la imagen de la empresa.

Una decisión anterior correspondiente a la CS apunta en un sentido similar en cuanto a una mayor flexibilización de la protección a la inviolabilidad de las comunicaciones cuando se trata de correos institucionales, así como resalta la necesidad de monitoreo y control por parte de los empleadores, el cual no se refiere a un control disciplinario, sino a una investigación interna por la posible comisión de un delito. En el Recurso de Nulidad 817-2016, la CS anuló una sentencia previa que excluía de un proceso penal por colusión las pruebas obtenidas mediante el acceso del empleador sin

constitucional contra un despido ilegítimo sería el pago de una indemnización y no la reposición. Es por ello que estos jueces no se pronuncian sobre el fondo de la controversia. Sin embargo, los tres magistrados restantes (Espinosa-Saldaña, Blume y Ramos) han suscrito una posición en minoría por la que consideran que la demanda debería declararse fundada.

8 Véase los fundamentos del Magistrado Ramos Núñez en la citada sentencia recaída en el Expediente 00943-2016-PA/TC (2020).

mediar orden judicial a la información contenida en los correos electrónicos y los equipos de un trabajador (2017).

La CS considera que la protección a la inviolabilidad de las comunicaciones del trabajador debe tener en cuenta la existencia de una expectativa razonable de privacidad en relación a las circunstancias; es decir, que la persona entienda que su información privada puede ser objeto de fiscalización o registro en el marco de las funciones de control y monitoreo que ejerce el empleador. Ante ello, la CS consideró que la empresa sí tenía un fundamento razonable para fiscalizar; puesto que (i) la empresa misma habilitó la herramienta informática (correo) para la prestación laboral y (ii) en las circunstancias, el correo electrónico se utilizó para las comunicaciones respectivas de carácter delictivo (posible colusión). Este último aspecto es relevante en el caso, puesto que no nos encontramos ante una medida disciplinaria por parte de la empresa, sino ante la posible comisión de un delito. Así, la CS determinó que el caso en cuestión es de interés público, en la medida en que comprende la posible colusión en una licitación pública para patrullas policiales.

Tal situación genera que sea factible y previsible que la empresa pueda ejercer su facultad de fiscalización al contenido de los correos archivados del trabajador, en tanto (i) supervisa el correcto cumplimiento del monitoreo de sus obligaciones laborales, y (ii) constata que la utilización del instrumento informático respete el ordenamiento jurídico y las propias directivas internas de buen funcionamiento y licitud. Así, la CS concluye que: (i) no existe otra medida menos lesiva para conseguir la información correspondiente a la posible comisión de un delito; (ii) la fiscalización fue ponderada, puesto que se evaluó el interés general en comparación a los perjuicios generados a bienes jurídicos en particular; (iii) la medida fue justificada, puesto que existían sospechas de la posible comisión de un delito; (iv) la medida era necesaria, puesto que la información buscada solo se encontraba en los correos; y (v) la información obtenida versa sobre información relevante al caso y no sobre aspectos personales o familiares del trabajador (Recurso de Nulidad 817-2016, 2017).

Finalmente, en una sentencia aún más reciente recaída en el Expediente 04386-2017-PA/TC (2020), el TC reiteró una vez más que para acceder al correo electrónico de los trabajadores es necesario iniciar una investigación judicial, en la medida que se requiere de un mandato motivado del juez y con las garantías previstas en la ley, para que las comunicaciones y documentos privados sean abiertos, incautados, interceptados o intervenidos.

En atención a ello, consideramos que resulta altamente recomendable obtener la autorización expresa del trabajador para que el empleador pueda acceder con total seguridad al correo electrónico asignado a aquél.

B. La videovigilancia

La voz y la imagen de una persona registrada por medios tecnológicos como las cámaras de videovigilancia hacen parte de los datos personales protegidos por las disposiciones de la LDPD. Este es una de las pocas aplicaciones del derecho a la protección de datos para las que se ha desarrollado una directiva específica en el Perú. La Directiva de Tratamiento de Datos Personales mediante Sistemas de Videovigilancia entró en vigor el 16 de marzo de 2020.

En cuanto a las obligaciones y recomendaciones de la directiva que aplican al ámbito laboral, destacamos las siguientes (Directiva 01-2020-JUS/DGTAIPD, 2020):

a) **Consentimiento:** la empresa no requiere consentimiento de sus trabajadores, salvo situaciones que no se enmarquen en su poder de dirección, que a su vez engloba el control, supervisión de las labores, protección de bienes, seguridad y salud en el trabajo, entre otros.

b) **Proporcionalidad:** debe cumplirse con el principio de proporcionalidad (ej. las cámaras de videovigilancia no deben ubicarse en lugares destinados para el descanso, esparcimiento, vestuarios, servicios higiénicos, comedores, etc.). La grabación con sonido solo se admite cuando es relevante para los riesgos involucrados. La videovigilancia debe ser adecuada, pertinente y no excesiva en relación con el ámbito y finalidad para la instalación de las cámaras.

c) **Conservación:** las imágenes o voces grabadas deben ser almacenadas por 30 días como mínimo y por 60 días como máximo. Sin embargo, las imágenes y voces sin editar que den cuenta de presuntas infracciones laborales y/o accidentes de trabajo, deben conservarse por 120 días, salvo que existan razones que justifiquen su conservación por más tiempo. En caso de indicios de delito o falta debe comunicársele a la autoridad de inmediato. Los archivos deben eliminarse hasta dos días hábiles de cumplido el plazo máximo.

d) **Derecho de acceso:** los trabajadores podrán solicitar el acceso a las grabaciones o una

copia digital de sus inconductas o incumplimientos que se les haya imputado.

e) **Registrar bases de datos:** al igual que con cualquier dato, los sistemas de videovigilancia implican la titularidad de una o más bases de datos que deben ser registradas ante la Autoridad de Protección de Datos Personales.

f) **Implementar medidas de seguridad:** la empresa debe garantizar la seguridad, confidencialidad y evitar la alteración, pérdida, tratamiento o acceso no autorizado a las imágenes captadas por los sistemas de videovigilancia. Se recomienda, por eso, adoptar medidas técnicas, organizativas y legales pertinentes.

g) **Informar:** cada acceso a la zona de videovigilancia debe tener un cartel o anuncio visible. Se recomienda que contraste con el color de pared y que sea suficientemente visible. Como mínimo el cartel debe indicar la identidad y domicilio de la empresa; ante quién y cómo ejercer los derechos en materia de protección de datos (ej. derechos ARCO), y el lugar en el que se puede obtener más información (la empresa debe contar con un informativo adicional sobre el sistema de videovigilancia). Debe tener una dimensión mínima de 297 x 210 mm, salvo que el espacio no lo permita.

h) **No afectar derechos de terceros**: prevenir la captación de imágenes de terceros ajenos a los fines de la captación. La empresa es responsable por la implementación de mecanismos o medidas adecuadas para no afectar los derechos de terceros (anonimizar, difuminar, etc.).

i) **Tratamiento por encargo:** existen reglas para el uso de servicios o gestión de la videovigilancia realizados por terceros.

j) **Confidencialidad:** deben suscribirse acuerdos de confidencialidad con las personas que, en razón de sus funciones, operan o tiene acceso al sistema de videovigilancia.

k) **Derechos ARCO:** se establecen reglas específicas para el ejercicio de los derechos al acceso, rectificación, cancelación y oposición de los titulares de las imágenes y sonidos captados por los sistemas de videovigilancia.

Más allá de estas disposiciones, al igual que con el correo electrónico, el uso de la videovigilancia plantea preguntas sobre el alcance de la esfera privada y la intimidad de los trabajadores en el ámbito laboral y sobre cómo armonizar la protección de datos personales con las necesidades de monitoreo y control del empleador.

El documento ya citado de la OIT sobre protección de datos personales (International Labour Office Geneva, 1997) establece que el empleador puede hacer uso de los sistemas de videovigilancia para fines de monitoreo de sus trabajadores, pero debe cumplir ciertos requisitos, que coinciden con lo señalado en la directiva de la autoridad del Perú. En primer lugar, solo puede ser llevado a cabo si los trabajadores involucrados son informados previamente de las intenciones del empleador. Los trabajadores deben conocer el propósito del monitoreo y tener una idea clara del funcionamiento de los aparatos que se utilicen (ubicación y horarios en que funcionan, por ejemplo). No puede haber 'cámaras escondidas'.

En segundo lugar, los empleadores no están en libertad total de elegir el método y medios del monitoreo que ellos consideren más apropiados para sus intereses; antes bien, deben tener en consideración las consecuencias para la privacidad de los trabajadores y preferir los medios de vigilancia menos invasivos. En el caso del monitoreo secreto o continuo, la aproximación es mucho más restrictiva. Debe ser limitado a los casos en los que el monitoreo es indispensable para lidiar con específicos problemas vinculados a la seguridad y salud, o a la protección de la propiedad.

El cumplimiento de estas recomendaciones incorpora la valoración de aspectos subjetivos como la intención que se persigue con la utilización de las cámaras y las expectativas razonables de privacidad de los trabajadores.

Al respecto, existe un referente jurisprudencial reciente en el Perú que se ocupa específicamente del uso de cámaras en entornos laborales. El 25 de setiembre de 2020, el TC desestimó una demanda de un sindicato de trabajadores que buscaba que se retirara un sistema de redes de cámaras de video que la empresa había instalado en las áreas de producción, almacenes y fábrica[9]. El sindicato sostenía que las cámaras de vigilancia vulneraban los derechos a la dignidad, la intimidad y la salud de los trabajadores.

[9] El 25 de setiembre de 2020, el Pleno del Tribunal Constitucional emitió, por unanimidad, la sentencia, que declara infundada la demanda de amparo que dio origen al Expediente 02208-2017-PA/TC (2020). Dicha demanda fue presentada contra Nestlé Perú por el Sindicato de Obreros P y A D'Onofrio SA.

La sentencia señala que se pudo constatar que los trabajadores habían sido informados por la empresa de la instalación de las cámaras y del objetivo que se buscaba con ellas. Dicho objetivo correspondía, además, a funciones legítimas de monitoreo y control por parte del empleador y no se encontró evidencia de que se le estuviera dando un uso que extralimitara dichas funciones o que no fuera proporcional a los fines establecidos. Se observó, por ejemplo, que las cámaras habían sido instaladas "en zonas que no constituyen espacios íntimos o reservados para los trabajadores" (Expediente 02208-2017-PA/TC, 2020, fundamento 13). La sentencia describe en detalle lo que considera objetivos legítimos de la utilización de la videovigilancia en este caso específico:

> […] Se puede distinguir que la instalación de cámaras tiene como objetivo el monitorear los procesos de producción y, de ser el caso, poder analizar cualquier incidente de producción o de seguridad; por ejemplo, verificar que las rutas de evacuación se encuentran despejadas, mantener las zonas seguras libres de camiones, asegurar un buen estado y evitar sabotajes en la fuente de energía alterna de la fábrica, poder visualizar el video ante potenciales reclamos vinculados con la presentación de cuerpos extraños en los productos, etc. También se puede advertir que las videocámaras no están instaladas en un ambiente que pudiera ser calificado como "privado", pues son áreas en las que el personal autorizado transita libremente (Expediente 02208-2017-PA/TC, 2020, fundamento 15).

Los fundamentos del TC en el examen de la demanda están en línea con los principios de la legislación sobre protección de datos personales. Lo realmente importante es la ratificación por parte del máximo intérprete de la Constitución sobre la validez del uso de esta tecnología en ámbito laboral.

Además de este referente jurisprudencial, para la aplicación de la directiva al ámbito laboral vale la pena revisar las orientaciones que incluye al respecto la guía que ya hemos citado del gobierno español (AEPD, 2021). Esta aclara, en primer lugar, que la base jurídica para el control de las personas trabajadoras mediante videovigilancia es el contrato de trabajo y las facultades legales de control concedidas al empleador, por lo que no se requiere el consentimiento, pero sí se debe cumplir a cabalidad con el deber de informar. Va, además, en la misma dirección que el TC y la normativa peruana en lo que se refiere a los alcances y limitaciones del uso de este tipo de tecnología para cumplir con funciones de control dentro de las relaciones laborales. Se enfatiza en la importancia de respetar siempre el principio de proporcionalidad.

Por otro lado, aborda el tema específico del uso de las imágenes de videovigilancia como prueba de "la comisión flagrante de un acto ilícito" (AEPD, 2021, p. 52) por un trabajador. Explica que "se entenderá cumplido el deber de informar cuando se haya colocado un dispositivo informativo en lugar suficientemente visible concretando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos" (AEPD, 2021, p. 52). Advierte que la sentencia del Tribunal Europeo de los Derechos Humanos (*López Ribalda et. al. c. España*, 2019) admite que una prueba de incumplimientos graves de las obligaciones laborales (como robos a la empresa) no necesariamente será nula en caso se haya incumplido con el deber de información, siempre que existe una sospecha razonable sobre el ilícito[10].

C. Salud pública y protección de datos de los trabajadores

La emergencia sanitaria generada por la pandemia puso en primer plano una nueva fuente de tensión entre el derecho a la protección de los datos personales y otros derechos individuales y sociales. Una tensión que toca el ámbito laboral en aspectos como la necesidad de controles epidemiológicos y de la vacunación masiva para la protección colectiva de la salud de los trabajadores. Si bien este aspecto no se refiere directamente a una nueva tecnología, sí afecta dinámicas sociales, laborales y legales que pueden, a su vez, incidir en la manera en que en el futuro cercano se desarrollen y adopten nuevas soluciones tecnológicas.

En el marco de la emergencia nacional generada por la pandemia, el 5 de mayo de 2020 la ANPDP emitió la Opinión Consultiva 32-2020-JUS/DGTAIPD en la que fijó los criterios para armonizar la protección de datos personales de los trabajadores con la obligación de los empleadores en materia de la salud de sus empleados y de la prevención de riesgos laborales.

Recordemos que la información sobre la salud se considera un dato sensible sujeto de especial protección. Es decir, solo puede ser tratada con previo consentimiento de sus titulares por escrito, salvo que exista una excepción que lo justifique. En este contexto, constituye una excepción a la regla del consentimiento la celebración, ejecución y desarrollo de la relación laboral en dónde se

[10] Para mayor información, véase Consejo de Trabajo (2019).

circunscribe el deber del empleador de preservar la salud de sus trabajadores en el entorno laboral. Además, la Opinión Consultiva sostiene que, si bien el principio de consentimiento es un principio rector de la LPDP, en el marco de una relación laboral debe tomarse en cuenta las excepciones contempladas en el artículo 14 de dicha norma (Ley 29733, 2011). Es decir, dada la existencia de una relación contractual de trabajo entre empleador y trabajador, y las obligaciones de garantizar la seguridad y la salud de todos los trabajadores, así como la existencia de una emergencia sanitaria declarada, se configuran las citadas excepciones previstas en la LPDP.

La ANPDP considera que

> es posible que el empleador realice el tratamiento de datos personales sensibles referidos al COVID-19 de los trabajadores sin su consentimiento, siempre que este tratamiento […] tenga como fin garantizar la seguridad y salud en el trabajo con el objeto evitar los contagios de esta enfermedad en los centros laborales (Opinión Consultiva 32-2020-JUS/DGTAIPD, 2020, acápite 9).

Lo anterior se justifica jurídicamente en la obligación del empleador de prevenir los riesgos laborales a los que los trabajadores puedan estar sujetos. Además, los trabajadores deben cooperar con el empleador para dicho fin.

La opinión originalmente estaba dirigida a permitir que se llevaran a cabo controles como la toma de temperatura y el registro de la información sobre los trabajadores contagiados. Señalaba al respecto que

> un dato que arroje una situación anormal de salud puede constituir un peligro para los mismos trabajadores, para el resto del personal o para otras personas relacionadas con el centro laboral; por ende, esta medida constituye un medio relacionado con la vigilancia de la salud de los trabajadores que, conforme a la Ley de Seguridad y Salud en el Trabajo, resulta obligatoria para el empleador (Opinión Consultiva 32-2020-JUS/DGTAIPD, 2020, acápite 22).

Esta Opinión no se ha extendido ni actualizado para abordar el tratamiento a la información sobre la vacunación de los trabajadores. Sin embargo, los criterios anteriormente citados pueden ser relevantes a la hora de examinar esta cuestión. Reconociendo que lo ideal sería obtener el consentimiento de los trabajadores para estos efectos, ¿podría el empleador requerirles la información sobre la vacunación en la medida que sea necesaria para salvaguardar la salud de los trabajadores en el centro de trabajo?

Es importante recordar que la normativa vigente establece que la vacunación es libre y voluntaria. Por lo que, salvo que en un futuro se apruebe una norma específica que establezcan la obligatoriedad de la vacunación, no es posible obligar a los trabajadores a vacunarse. Sin embargo, el empleador podría adoptar medidas proporcionales para preservar la salud de sus trabajadores según sea el caso, tal como solicitar medidas de seguridad más estrictas para aquellos trabajadores no vacunados, y promover y exhortar a sus trabajadores a que se vacunen, continuar con el trabajo remoto, entre otros.

En cualquier caso, es importante tener siempre presente las siguientes recomendaciones en el tratamiento de la información sobre la salud de los trabajadores:

- Cumplir con el deber información. Es decir, cumplir con todos los elementos del artículo 18 de la LPDP (Ley 29733, 2011), aportando información clara y veraz sobre el uso y finalidad del tratamiento de los datos personales;

- Limitar el número de personas con acceso a esta información a quienes por razones de su cargo y función deban necesariamente conocerla, a fin de cumplir con las obligaciones legales relacionadas con la prevención del COVID-19.

- Preservar la confidencialidad y seguridad de la información. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido establecida de manera inequívoca al momento de su recopilación. La finalidad del tratamiento de los datos personales debe expresarse con claridad, sin lugar a confusión y reflejando el objeto del tratamiento de los datos.

VI. COMENTARIOS FINALES

Desde los desarrollos normativos y jurisprudenciales, existe hoy más preguntas que respuestas sobre los alcances y límites del derecho a la protección de los datos personales en el ámbito laboral. Los casos analizados tocan apenas una fracción de las aplicaciones tecnológicas que se están usando en dichos ámbitos laborales y que involucran el tratamiento de los datos personales de los trabajadores. Es importante, sin embargo, que los empleadores tengan claras sus responsabilidades frente a la protección de la información personal de sus trabajadores y que apliquen los principios generales en esta materia que hemos intentado resumir en este artículo.

Se trata, sin lugar a dudas, de un tema de gran relevancia y actualidad, no solo por la multiplicación de aplicaciones tecnológicas, sino por los desafíos que la pandemia del COVID-19 nos ha planteado frente a las necesidades de armonizar derechos individuales como la protección de los datos personales, protección de la salud y la seguridad ocupacional. Frente a ello, es necesario revisar no solo la normatividad y las decisiones jurisprudenciales locales, sino los referentes internacionales que pueden coadyuvar a resolver dudas y controversias en casos concretos.

REFERENCIAS

Agencia Española de Protección de Datos [AEPD] (2021). *La protección de datos personales en las relaciones laborales*. Agencia Española de Protección de Datos.

Blume Moore, I. (2021). El derecho fundamental a la protección de datos en el entorno laboral. *Revista Laborem,* (24), 277-299.

Castro Cruzatt, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *Ius et Veritas*, *18*(37), 260-276.

Consejo de Trabajo (15 de noviembre de 2019). Cámaras ocultas en el trabajo, ¿medida legítima o violación a la privacidad? *Enfoque Derecho*. https://www.enfoquederecho.com/2019/11/15/camaras-ocultas-en-el-trabajo-medida-legitima-o-violacion-a-la-privacidad/

International Labour Office Geneva (1997). *Protection of Worker's Personal Data*. International Labour Organization. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

Vegas Torres, J. (2011). *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*. Universidad Rey Juan Carlos- KPMG.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Bărbulescu c. Romania, 2017 Eur. Ct. H.R. 210.

Constitución Política del Perú [Const.] (1993) (Perú).

Decreto Supremo 003-2013-JUS, Decreto Supremo que aprueba el Reglamento de Ley 29733, Ley de Protección de Datos Personales, Diario Oficial *El Peruano*, 22 de marzo de 2013 (Perú).

Directiva 01-2020-JUS/DGTAIPD, Tratamiento de Datos Personales mediante Sistemas de Videovigilancia, Diario Oficial *El Peruano*, 16 de enero de 2020 (Perú).

Ley 29733, Ley de Protección de Datos Personales, Diario Oficial *El Peruano*, 3 de julio de 2011 (Perú).

López Ribalda et. al. c. España, 2013 Eur. Ct. H.R. 233.

Opinión Consultiva 32-2020-JUS/DGTAIPD, Tratamiento de datos de salud durante la pandemia en el ámbito laboral, 5 de mayo de 2020 (Perú).

Resolución Directoral 019-2013-JUS/DGPDP, Aprueba la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales, Diario Oficial *El Peruano*, 11 de octubre de 2013 (Perú).

Resolución Directoral 008-2017-JUS/DGPDP, Tratamiento de datos mediante geolocalización, Diario Oficial *El Peruano*, 25 de enero de 2017 (Perú).

Resolución Directoral 02-2020-JUS/DGTAIPD, Aprueba la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia, Diario Oficial *El Peruano*, 16 de enero de 2020 (Perú).

Sala Penal Permanente de la Corte Suprema de Justicia de la República, 20 de noviembre de 2017, Recurso de Nulidad 817-2016/LIMA (Perú).

Segunda Sala de Derecho Constitucional y Social Transitoria de la Corte Suprema de Justicia de la República, 19 de marzo de 2017, Casación 14614-2016-Lima (Perú).

S.T.C. 170/2013, 7 de octubre de 2013 (B.J.C. 170/2013) (Esp.).

Tribunal Constitucional [T.C.], 29 de enero de 2003, sentencia recaída en el Expediente 1797-2002-HD/TC (Perú).

Tribunal Constitucional [T.C.], 18 de agosto de 2004, sentencia recaída en el Expediente 1058-2004-AA/TC (Perú).

Tribunal Constitucional [T.C.], 14 de julio de 2020, sentencia recaída en el Expediente 00943-2016-PA/TC (Perú).

Tribunal Constitucional [T.C.], 25 de septiembre de 2020, sentencia recaída en el Expediente 02208-2017-PA/TC (Perú).

Tribunal Constitucional [T.C.], 27 de octubre de 2020, sentencia recaída en el Expediente 04386-2017-PA/TC (Perú).