EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO LABORAL*

Iván Blume Moore**

Resumen

El avance de las nuevas tecnologías ha traído consigo el uso masivo de información personal y, consecuentemente, generado la necesidad de un marco legal destinado a garantizar su protección. En el presente artículo, se realiza un repaso del derecho fundamental a la protección de datos personales mediante el análisis de su evolución a la luz de derechos conexos como la intimidad y la inviolabilidad de las comunicaciones, a fin de establecer lineamientos para su aplicación en el ámbito laboral.

Palabras clave

Derecho fundamental; protección de datos personales; videovigilancia; derecho a la intimidad; derecho laboral.

Abstract

The development of new technologies has broad along the massive use of personal information and, consequently, the need for a legal framework destined to guarantee its protection. In this article, we make an overview of the fundamental right to the protection of personal data through an analysis of its evolution in the light of related rights such privacy and the secrecy of communications in order to establish guidelines for its application in the workplace.

Keywords

Fundamental right; protection of personal data; video surveillance; right to privacy; labor law.

* Dedicado a la memoria del profesor Javier Neves Mujica.

** Asociado Senior del Estudio Rodrigo, Elías & Medrano Abogados. Master of Industrial and Labor Relations (MPS), Cornell University. Abogado por la Universidad Católica del Perú. Contacto: IBlume@Estudiorodrigo.com

SUMARIO: I. Introducción *1. La inviolabilidad de las comunicaciones: de los correos postales al e-mail. 2. El derecho a la intimidad: reconocimiento, delimitación y protección de la esfera privada 3. La protección de datos personales como derecho autónomo.* II. Un poco de historia: inviolabilidad de la correspondencia, derecho a la intimidad y protección de datos. III. La protección de datos en la legislación peruana. IV. El derecho a la protección de datos personales en el entorno laboral. *1. Videovigilancia 2. Tratamiento de los datos personales de los trabajadores en el contexto del COVID-19.* V. Comentarios finales.

I. Introducción

Desde que la correspondencia empezó a considerarse inviolable, han surgido normas enfocadas en la protección de las comunicaciones y la información personal. Sin embargo, a raíz de los cambios introducidos por las tecnologías de información y comunicación, desde finales del siglo pasado se ha cristalizado un nuevo derecho de carácter autónomo que va más allá de la protección a las comunicaciones y a la intimidad de las personas: el derecho fundamental a la protección de los datos personales.

El desarrollo normativo de este derecho no siempre ha logrado ir al paso de los avances tecnológicos y de la multiplicidad de sus aplicaciones. En particular en el Perú, si bien desde 2011 se cuenta con la Ley No. 29733, Ley de Protección de Datos Personales (LPDP), al tratarse de normas que intersectan todas las industrias y sectores, hace necesario un esfuerzo interpretativo importante para resolver casos concretos en determinadas áreas del derecho; el derecho del trabajo no es la excepción.

En el ámbito laboral, por ejemplo, se han desarrollado diversas aplicaciones de las tecnologías de información y comunicación para apoyar la gestión de personal y las funciones de control y monitoreo. 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 estos temas, subsisten muchos vacíos en la legislación y en la jurisprudencia peruana.

Este artículo busca desarrollar los aspectos más importantes del derecho fundamental a la protección de datos personales. Además, lleva a cabo un repaso

sobre la evolución del concepto del derecho a la protección de datos personales, para ello revisa antecedentes locales, referentes internacionales y la posición la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Autoridad Nacional de Protección de Datos Personales - ANPDP) sobre el tratamiento de datos personales de los trabajadores en el contexto de la pandemia de COVID-19, con el fin de ofrecer algunas guías de acción para su aplicación en casos específicos dentro del ámbito laboral.

II. Un poco de historia: inviolabilidad de la correspondencia, derecho a la intimidad y protección de datos

Para entender el surgimiento de la protección de datos como un derecho autónomo es útil trazar su relación y sus diferencias con otros derechos más antiguos con los que a veces se los confunde. Revisaremos en concreto su evolución a partir, por un lado, del concepto de inviolabilidad de la correspondencia y, por otro, del derecho a la intimidad. La historia de estos derechos está ligada a cambios sociales ocurridos no solo en los ámbitos de las doctrinas jurídicas; sino en el campo tecnológico, en especial de las tecnologías de información y comunicación.

1. La inviolabilidad de las comunicaciones: de los correos postales al e-mail

La primera revolución tecnológica que facilitó las comunicaciones a distancia y amplió el poder y el radio de acción de las actividades humanas no fue Internet. Tampoco el teléfono o el telégrafo. Fue la organización de sistemas postales oficiales por parte de administraciones imperiales. Ya fueran los chasquis de los Incas o los correos reales de los monarcas europeos, el uso de "postas" o relevos a lo largo de rutas establecidas y protegidas por el poder permitió la regularización del control comercial, militar y burocrático sobre extensos territorios[1].

Esos sistemas que originalmente se establecieron para asegurar el flujo de las órdenes y disposiciones de los monarcas, empezaron más tarde a prestar sus

1 Carmen RODRÍGUEZ GONZÁLEZ, "Los viajes a la ligera, un medio tradicionalmente rápido de transporte, desbancado por el ferrocarril". *Investigaciones históricas: Época moderna y contemporánea*, Nº 4, 1983, págs. 159-184.

servicios a particulares. Los servicios de correos se convirtieron en un monopolio oficial, lo que facilitó las comunicaciones, pero también puso los mensajes que se trasmitían a través de ellas al alcance de quienes manejaban el correo. En tiempos de Luis XIV se creó incluso una oficina dentro de los servicios postales encargada de espiar la correspondencia, el famoso *cabinet noirs* o "gabinete negro". El rechazo a esa práctica, que se generalizó en varios gobiernos del Antiguo Régimen, fue el origen histórico de la consagración de la inviolabilidad de la correspondencia en las constituciones liberales del siglo XIX. Ya en la segunda mitad de ese siglo, el principio se empieza a extender a las comunicaciones telegráficas y, más tarde, a las telefónicas[2].

En constituciones como las de España o Perú, que datan de la segunda mitad del siglo XX, la inviolabilidad y protección al secreto de las comunicaciones se presentan comprendida dentro de los derechos fundamentales de las personas y ligado a conceptos como "intimidad", "honor" o "privacidad". Así, por ejemplo, en la Constitución española, dentro del artículo 18, que se ocupa del "derecho al honor, a la intimidad personal y familiar y a la propia imagen", uno de los incisos garantiza "el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial"[3]. La Constitución peruana, por su parte, consagra dentro de los "derechos fundamentales de la persona" el derecho "al secreto y a la inviolabilidad de sus comunicaciones y documentos privados" (artículo 2, inciso 10).

A diferencia de lo que ocurre con la constitución española, en la peruana no se hace referencia a los medios de comunicación a los que se les podría aplicar el principio de secreto o inviolabilidad. Esto genera preguntas sobre los alcances de este derecho, ¿se aplica, por ejemplo, a una conversación entre dos personas en un espacio público? Jaime Vegas Torres, catedrático de derecho procesal de la Universidad Rey Juan Carlos, argumenta que, como principio general, el alcance del secreto de las comunicaciones se debe determinar teniendo en cuenta el origen histórico de estas disposiciones. Es decir, que no se debe entender extensivo a cualquier tipo de comunicaciones, sino a las que puedan considerarse análogas a los servicios postales; en otras palabras, aquellas "en las que entre el emisor y

2 Jaime VEGAS TORRES, *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa.* Madrid: Universidad Rey Juan Carlos- KPMG, 2011. p. 34

3 VEGAS TORRES, *Op. Cit*, p. 34

el destinatario del mensaje se interponen uno o varios servicios que implican el uso de medios técnicos y la intervención de personas ajenas a los comunicantes y sobre los que éstos no tienen completo control"[4]. Su razón de ser, según esta doctrina, es evitar los abusos de quienes controlan o pueden intervenir en los medios de transmisión de los mensajes. Se aplica además a comunicaciones cerradas entre el emisor y uno o varios destinatarios y no a comunicaciones públicas.

El correo electrónico puede considerarse en este sentido como una extensión obvia de las comunicaciones postales, telegráficas y telefónicas. Se puede afirmar que a los mensajes transmitidos por este medio se les aplica claramente el secreto de las comunicaciones. Este criterio parece sin embargo insuficiente para regular la protección de la información y de los documentos personales que en la actualidad se captan, procesan o transmiten a través de una infinidad de aplicaciones de los medios informáticos, así como para interpretar su alcance en cada uno de los contextos en donde estos procesos ocurren.

Un asunto particularmente discutido en el ámbito laboral, es si un trabajador puede reclamar una violación a su derecho al secreto de sus comunicaciones cuando su correo institucional o corporativo es accedido por el empleador. Al respecto, el Tribunal Constitucional ha señalado de manera consistente en varias sentencias que la inviolabilidad de las comunicaciones personales de los trabajadores aplica incluso cuando estas han sido transmitidas a través de los equipos y las cuentas de correo suministrados por el empleado[5]. Esta tendencia jurisprudencial ha sido ratificada por la Corte Suprema. En una controvertida decisión en que estudió una demanda a un Reglamento Interno de Trabajo consideró que "[c]onstituye un exceso que el empleador señale que es propietario de las cuentas de correo electrónico (e-mails) y que se encuentra facultado a revisar su contenido; admitir ello, sería colisionar con el derecho a la intimidad e inviolabilidad de las comunicaciones de los trabajadores"[6].

4 Op. cit. p. 38.

5 Exp. No. 1058-2004-AA/TC (caso SERPOST) resuelto el 18 de agosto de 2004. El Tribunal declaró inconstitucional el despido de un funcionario por usar el computador de la compañía para enviar material pornográfico a terceros en horas laborales, al considerar que el empleador solo podía examinar el contenido del computador que le había entregado a su empleado, a través de un proceso judicial en lugar de una investigación privada.

6 Sentencia del 10 de marzo de 2017 de la Corte Suprema sobre la Causa No 14614-2016. Se trata de un recurso de casación interpuesto por Nestle Perú frente a una demanda

Según estas decisiones, aun en medio de las relaciones laborales persiste una esfera propia de los individuos que requiere protección frente a intromisiones de terceros. Ese reconocimiento no se desprende únicamente del principio de inviolabilidad de las comunicaciones. De hecho, la protección se extiende no solo al contenido de los correos electrónicos, sino a la información personal que los trabajadores guardan en los computadores de la empresa e incluso a los datos sobre la navegación en Internet desde esos equipos. Invocan con este fin otro de los derechos que históricamente han estado estrechamente vinculados a la protección de datos: el derecho a la intimidad, al que nos referiremos en el siguiente apartado.

2. El derecho a la intimidad: reconocimiento, delimitación y protección de la esfera privada

Antes de la aprobación de la LPDP, el principal referente para el tratamiento legal de la privacidad era el inciso 6 del artículo 2 de la Constitución que consagró 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". Se estableció, además, en nuestra Constitución el proceso de Habeas Data para garantizar su protección (inciso 4, artículo 200). También es importante el inciso 7 del mismo artículo, que 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".

Los anteriores incisos reconocían ya la realidad de los medios audiovisuales e informáticos y sus potenciales riesgos para los derechos fundamentales, pero abordaba la protección frente a dichos riesgos desde la perspectiva del derecho a la intimidad. Dicho derecho a su vez empieza a aparecer a finales del siglo XIX y surge del reconocimiento de la necesidad de toda persona de poder vivir con libertad su "vida privada", sin ser objeto de injerencias arbitrarias por parte del gobierno o de cualquier otra persona o autoridad[7].

iniciado por el Sindicato Único Nacional de Trabajadores de Nestle Perú S.A. sobre impugnación del reglamento interno de trabajo (RIT).

7 La primera formulación de este derecho, conocido en la tradición anglosajona como "the right to privacy" se suele atribuir a un artículo publicado en 1890 en el *Harvard Law Review* por dos abogados de Bostón: Samuel D. Warren y Louis D. Brandéis. Alberto ARCE JANARIZ, "El derecho a la intimidad, de Samuel d. Warren y Louis D. Brandéis". *Revista*

Los límites entre esa esfera privada y el ámbito de lo público han sido desde entonces objeto de controversias y constantes redefiniciones. Los alcances de la intimidad tienen un importante componente de subjetividad, pues en buena medida depende de la valoración que las personas le dan a su autonomía en distintos ámbitos, así como de la percepción de los riesgos que se derivan de perder dicha autonomía. La evolución de su aplicación ha ido, sin embargo, generando consensos sobre algunos aspectos que intervienen en la demarcación de la intimidad y que recogen declaraciones de derechos como la contenida en el artículo 2 de la Constitución peruana, entre ellos la vida familiar, la inviolabilidad del domicilio y de la correspondencia, el libre desarrollo, el honor, el derecho al buen nombre, entre otros. Además de la Constitución, el artículo 14 del Código Civil establece que la intimidad de la vida personal o familiar no pueden ser puesta de manifiesta sin el asentimiento de la persona.

Respecto a la aplicación de este derecho en el entorno laboral, el Tribunal Constitucional ha considerado que los detalles contenidos en la boleta de pago de los trabajadores "atañen, prima facie, a la esfera privada" y, por lo tanto, están protegidos por el derecho a la intimidad, lo que implica excluir a terceros extraños del acceso a dicha información. Para el Tribunal, los datos sobre remuneraciones y en general sobre la situación financiera de una persona "atañen a asuntos vinculados íntimamente con el entorno personal y/o familiar cercano y con el desarrollo personal de sus miembros, las que al quedar descubiertos podrían ocasionar daños irreparables en el honor y la buena reputación" (Sentencia STC No. 05982-2009-PHD/T-fundamento 12).

Sin desconocer la importancia de estos referentes, la evolución de las tecnologías de información desde la dación de nuestra Constitución en 1993 ha hecho que el criterio de afectación a la intimidad se torne insuficiente como único bastión para proteger los datos personales de los individuos. De allí que sea necesario hablar de la protección de datos personales como un ámbito propio del derecho que va más allá de la aplicación de dicho criterio.

3. La protección de datos personales como derecho autónomo

En la actualidad la capacidad de almacenar, transmitir y procesar masivamente todo tipo de información hace potencialmente sensible el manejo de

Española de Derecho Constitucional. Año 16. Núm. 47. Mayo-Agosto 1996. 367-371.

cualquier dato personal, incluso los que no pertenecen estrictamente al ámbito de la vida íntima o personal.

Las preocupaciones actuales van desde los riesgos de seguridad por acceso a imágenes biométricas o a claves bancarias, hasta la posibilidad de perfilamientos a partir de decisiones o interacciones que quedan registradas en plataformas informáticas. Como lo 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"[8]. Por lo anterior, ningún dato personal se puede considerar neutro y se considera fundamental que en todos los casos se reconozca la facultad de sus titulares de controlar su acopio y posterior uso.

Se trata de un derecho distinto a los derechos a la inviolabilidad de las comunicaciones e intimidad. En el primer caso, porque su violación no requiere la intervención indebida en comunicaciones cerradas entre el emisor y los destinatarios. En el segundo caso, porque tal como lo señala el Tribunal Constitucional en la sentencia sobre el proceso de habeas data tramitado bajo el expediente 1797-2002-HD/TC, el derecho a la protección de datos busca proteger lo que denomina "derecho a la autodeterminación informativa":

> "[…] 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".

En esta decisión, la cual antecede a la LPDP, ya se contemplaba el derecho a impedir el suministro de datos personales y a que el titular exija jurisdiccionalmente el acceso a ellos e incluso su cancelación, independiente de si estos se consideran sensibles o parte de su intimidad.

8 Karin CASTRO CRUZATT, "El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú". *IUS ET VERITAS*; Núm. 37 (2008) [260-276] 261.

Naturalmente, esto se aplica al contexto laboral:

> "El derecho de la protección de datos personales no se reduce a los datos relacionados con la privacidad o intimidad de las personas. No debe confundirse el primero con el derecho a la intimidad. La protección de datos personales comprende cualquier naturaleza de información (privada, sensible, semiprivada y pública), lo cual implica que toda clase de dato personal del trabajador debe ser tratado debidamente por parte del empleador"[9].

Además de lo señalado, la necesidad de establecer el derecho a la protección de datos como un derecho autónomo responde también a la relevancia que las diversas formas de tratamiento masivo de información han adquirido como apoyo a muchos procesos sociales. Precisamente por el reconocimiento de los potenciales beneficios que se pueden derivar de los nuevos desarrollos informáticos es que es importante encontrar maneras de equilibrarlos con la protección de derechos fundamentales que estas tecnologías pueden potencialmente poner en riesgo.

Un ejemplo de mucha actualidad es lo que ha ocurrido con el desarrollo de aplicaciones que facilitarían el rastreo epidemiológico para controlar la propagación del Covid-19. Los expertos consideran que rastrear el mayor número posible de los contactos de las personas contagiadas es la manera más efectiva de evitar que el virus se salga de control. Se trata, sin embargo, de un proceso dispendioso y costoso. Se ha buscado por eso desarrollar aplicaciones descargables en el celular que puedan llevar automáticamente el registro de las personas con las que las personas diagnosticadas tuvieron contacto en los últimos días. Sin embargo, además de las dificultades tecnológicas, estos esfuerzos han generado preocupaciones porque permitirían a las autoridades vigilar y llevar el control de los movimientos e interacciones de sus ciudadanos. La solución para los dilemas que plantean situaciones como lo anterior puede pasar por los propios desarrollos tecnológicos, que deberían diseñarse o implementarse de manera que contribuyan a la seguridad de los datos personales procesados.

9 Nelson REMOLINA ANGARITA, "Tratamiento de datos personales en el contexto laboral". *Revista Actualidad Laboral*, No. 175, ene-feb/2013 [19-24] 25.

III. La protección de datos en la legislación peruana

Las disposiciones sobre protección de datos contenidas el inciso 6 del artículo 2 de la Constitución, solo se desarrollaron de manera integral hasta 2011 con la promulgación de la LPDP, la cual permitió además actualizar la normativa a la concepción de la protección de datos personal como un derecho autónomo distinto al derecho a la intimidad.

En la actualidad, el marco legal en materia de protección de datos personales en el Perú, cuenta con los siguientes instrumentos legales y normativas técnicas:

- Ley No. 29733 – Ley de Protección de Datos Personales.
- Decreto Supremo N° 003-2013-JUS – Reglamento de Ley N° 29733 (22.03.13).
- Resolución Directoral Nº 019-2013-JUS – Aprueba la Directiva de Seguridad de la Información (11.10.13).
- Resolución Directoral Nº 02-2020-JUS/DGTAIPD– Aprueba la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia (16.01.20).
- Norma Técnica Peruana NTP-ISO/IEC 270001:2008. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (12.12.08).
- Resolución Ministerial Nº 129-2013-JUS – Aprueba el uso obligatorio de la NTP-ISO/IEC 270001:2008 (25.05.12).

La LPDP y su Reglamento, regulan el tratamiento de datos personales de personas naturales contenidos o destinados a ser contenidos en bancos de datos personales de carácter público o privado en el Perú. Se trata de normas de orden público que deben ser respetadas a cabalidad tanto por las autoridades administrativas como por el sector privado[10].

La LPDP y el Reglamento ofrecen algunas definiciones importantes. La primera de ellas, justamente, es qué se entiende por "dato personal": "[e]s aquella

10 ***"Artículo 1.- Objeto.***
"El presente reglamento tiene por objeto desarrollar la Ley Nº 29733, Ley de Protección de Datos Personales, en adelante la Ley, a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado. Sus disposiciones constituyen normas de orden público y de cumplimiento obligatorio."

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" (artículo 2, numeral 4 del Reglamento).

Hay además dos consideraciones importantes para la aplicación de la LPDP. La primera es lo que la LPDP denomina en sentido amplio una "bases de datos". Con esto se refiere al "conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera sea la forma o modalidad de su creación, formación, almacenamiento, organización y acceso" (artículo 2, numeral 2, de la LPDP).

La segunda consideración es el "tratamiento" que se les da a estos datos, que se entiende 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" (artículo 2 inciso 19 del LPDP). El principio medular del derecho a la protección de datos es que ninguno de estos "tratamientos" puede realizarse sin el consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, salvo excepciones establecidas explícitamente por la ley. Cabe acotar, no obstante, que hay determinados casos establecido en el artículo 14 de la LPDP, en los cuales no se requiere el consentimiento del titular de datos personales, tales como:

a) Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.

b) Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.

c) Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a la ley de la materia.

d) Cuando los datos personales sean necesarios para la 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.

e) 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.

f) Cuando se hubiera aplicado un procedimiento de anonimización o disociación.

g) Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales.

El consentimiento relativo a datos sensibles —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 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, etc.— debe ser obtenido por escrito. Se deben cumplir además los principios de finalidad[11], proporcionalidad[12], calidad[13], seguridad[14], entre otros.

11 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.

12 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.

13 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.

14 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

Además de la regla del consentimiento, es importante que tener presente que las principales obligaciones para cumplir con la normativa de protección de datos, son las siguientes:

- **Inscripción de bases de datos:** Las organizaciones deben inscribir los bancos de datos personales de su titularidad en el Registro Nacional de Protección de Datos Personales.
- **La transferencia de datos personales fuera del territorio nacional:** El flujo transfronterizo, debe ser comunicado a la APDP dentro del formulario de inscripción de la base de datos o través de una modificación al mismo. El titular del banco de datos personales debe realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados. En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a la Ley u obtener el consentimiento del titular para realizar la transferencia bajo dichas circunstancias, entro otros.
- **Confidencialidad y seguridad:** 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. Del mismo modo, el titular de los bancos de datos personales debe implementar medidas de seguridad. Así, para el tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad, confidencialidad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
- **Conservación de la información:** Los datos personales que vayan a ser tratados deben conservarse solo por el tiempo necesario que se requiera para cumplir con la finalidad del tratamiento. Las organizaciones podrán conservar los datos durante el tiempo en que pueda exigirse

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.

algún tipo de responsabilidad derivada de la una relación u obligación jurídica o de la ejecución de un contrato por el interesado. Una vez cumplido este período los datos sólo podrán ser conservados previa anonimización. Por ello, el periodo de conservación viene íntimamente vinculado al periodo de prescripción aplicable.

- **Derechos Arcos:** Derechos de acceso, rectificación, cancelación y oposición, entre otros, a través de los cuales la LPDP y su Reglamento, garantizan a las personas el control sobre sus datos personales. Cada uno de estos derechos está sujeto a sus propias formalidades y plazo de cumplimiento. La denegatoria o la respuesta insatisfactoria habilitan al solicitante a iniciar el procedimiento trilateral de tutela ante la Dirección General de Protección de Datos Personales o acudir al Poder Judicial para interponer una acción de Hábeas Data.
- **Deber de información:** Básicamente, esta obligación consiste en que el titular del banco de datos personales ponga a disposición del titular de los datos personales toda la información relevante sobre el "tratamiento" de sus datos personales. Como derecho, implica que el titular de los datos personales deba recibir tal información en forma previa a su recopilación, y que aquélla sea idónea y veraz.

Veamos ahora cómo se aplican estos principios generales al ámbito laboral y qué tanto se ha avanzado en establecer reglas específicas para el ejercicio en situaciones o usos de tecnologías particulares.

IV. El derecho a la protección de datos personales en el entorno laboral

La gestión de cualquier organización implica el tratamiento de datos personales de sus trabajadores para diferentes finalidades tales como la selección de personal, el cumplimiento de las obligaciones laborales (por ejemplo, la planilla electrónica) y el de control y seguimiento de las actividades laborales.

Esto puede ocurrir a distintas escales y sin que el empleador necesariamente sea consciente de que está actuando como titular y responsable legal de una base de datos personales, lo cual puede resultar en una gestión de riesgos inadecuada y en las sanciones que esto conlleva. Asimismo, este desconocimiento le imposibilita garantizar este derecho fundamental a sus trabajadores.

No hay sin embargo desarrollos normativos específicos (salvo por el caso de la videovigilancia, como veremos más adelante) ni tampoco jurisprudencia que procure información sobre la adecuada armonización de estos principios con, por ejemplo, las necesidades de monitoreo y control del empleador, asunto en el que se auguran mayores tensiones en el futuro con la intensificación y mayor desarrollo de la tecnología.

A nivel internacional, sin embargo, sí existen algunos lineamientos que pueden servir de referente y de esta forma dar algunas luces sobre el asunto que planteamos. Quizás el más importante es el documento titulado "Protection of Worker's Personal Data", una publicación de la OIT[15], que contiene una suerte de código en materia de privacidad de los trabajadores. En ella se resaltan los siguientes principios relacionados con la debida administración de los datos personales en ámbitos laborales:

- 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.
- En principio, los datos personales deberían utilizarse únicamente para el fin con el cual hayan sido acopiados.
- Los empleadores deberían evaluar periódicamente sus métodos de tratamiento de datos, con el objeto de: a) reducir lo más posible el tipo y el volumen de datos personales acopiados; y, b) mejorar el modo de proteger la vida privada de los trabajadores.
- 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.
- El tratamiento de datos personales no debería conducir a una discriminación ilícita en materia de empleo u ocupación.
- 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

15 OIT, 1997, p. 33- https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf

una obligación de confidencialidad, de acuerdo con la realización de sus tareas y el ejercicio de los principios de tratamiento de datos.

- 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.
- Los empleadores deberían verificar periódicamente que los datos personales conservados son exactos, actualizados y completos.

En la legislación peruana, en términos generales, se puede decir que en el ámbito laboral aplican los mismos principios de protección de los datos personales contemplados en la LPDP. Sin embargo, la mayor particularidad radica en que por lo general el empleador no requiere del consentimiento del trabajador para tratar sus datos, siempre que la finalidad del tratamiento se enmarque dentro del contrato de trabajo, cumpliendo con el deber de información, proporcionalidad y seguridad, entre otros. Por el contrario, cuando el tratamiento de los datos personales no tenga su razón de ser en el vínculo laboral, por ejemplo, para fines publicitarios, requerirá del consentimiento del trabajador.

Pese a lo anterior, no existe aún en nuestro país una cultura de transparencia sobre el tratamiento y uso de los datos personales y sobre la manera se usará los datos personales. Dentro de las organizaciones tampoco existe suficiente preocupación sobre la seguridad de los datos ni sobre la manera de garantizar su confidencialidad y el manejo apropiado para evitar su alteración, pérdida, tratamiento o acceso no autorizado. Pensemos, por ejemplo, en un trabajador que por las funciones a su cargo tiene acceso y manejo de datos protegidos o información sensible sobre muchas personas en la organización. Las normas sobre protección de datos obligan al empleador a adoptar medidas de seguridad y confidencialidad para prevenir que sus empleados le den mal uso a la información que manejan y evitar que violen el derecho a la privacidad de las personas que han suministrado sus datos. En ese sentido, si un trabajador no cumple con esas medidas de seguridad y se filtra la información, el empleador podría tener que responder ante los eventuales daños que se generen.

Para complementar el anterior panorama, examinaremos a continuación dos normativas recientes con las que la ANPDP ha intentado responder a retos específicos planteados por aplicaciones tecnológicas o por situaciones

particulares. Se trata de la directiva sobre videovigilancia y de la opinión consultiva sobre tratamiento de datos de salud durante la pandemia en el ámbito laboral.

1. Videovigilancia

El pasado 16 de marzo, entró en vigencia la directiva No 01-2020-JUS/DGTAIPD que busca garantizar que las entidades que requieren hacer uso de la videovigilancia no vulneren derechos ciudadanos ni pongan en riesgo la seguridad de la información personal. Se trata del primer esfuerzo por parte de la ANPDP de regular la aplicación de las normas generales sobre protección de datos en el marco de una tecnología específica.

Como lo recuerda la misma directiva, la imagen y el sonido de la voz de una persona se consideran parte de sus datos personales, pues estos "permiten identificar o hacer identificable a una persona natural a través de medios que pueden ser razonablemente utilizados". La directiva sigue así la regla fundamental de las normativas de protección de datos. Como hemos visto, esta consiste en que no se puede obtener, recolectar, sistematizar y trasladar información personal sin previo consentimiento de los titulares de esa información.

Cada zona que esté vigilada por un sistema de video debe tener un cartel o anuncio suficientemente visible para quien acceda a dicha zona. La directiva especifica las dimensiones, las características del diseño y el contenido mínimo del anuncio. Este debe incluir (i) la identidad y domicilio de la empresa; (ii) ante quién y cómo se puede ejercer los derechos en materia de protección de datos; y, (iii) lugar en el que se puede obtener más información sobre el particular (la empresa debe contar con un informativo adicional sobre el sistema de videovigilancia que debe estar disponible a través de medios informáticos, digitalizados o impresos).

Cumplir con la normatividad va, sin embargo, más allá de colocar un aviso. La directiva incluye indicaciones sobre disposición y ubicación de las cámaras que buscan sobre todo proteger el derecho a la intimidad. Pero en lo que se refiere a la protección de datos el componente más sensible es el almacenamiento, transmisión y manejo posterior de las imágenes captadas. Por esta razón, cada entidad que desee instalar sistemas de videovigilancia debe (i) registrar las

correspondientes bases de datos ante la Autoridad de Protección de Datos Personales; y, (ii) estar en capacidad de asumir una serie de responsabilidades legales y técnicas asociadas, por ejemplo, con la seguridad de la información personal que estos sistemas almacenan. El cumplimiento de todas estas disposiciones requiere de la creación de perfiles y la asignación clara de responsabilidades en el manejo de los datos, que incluye establecer procedimientos de identificación y autentificación de los usuarios con acceso a la información.

Dichas responsabilidades aplican para toda la videovigilancia en general, pero existen algunas especificidades para su aplicación en contextos laborales.

Lo primero que hay que tener en cuenta es la necesidad de contar con el consentimiento del titular de los datos o de ampararse en alguna excepción contemplada por la ley (relación contractual, interés legítimo, etc.). Esto no aplica para los trabajadores. Siempre y cuando la finalidad de la videovigilancia se enmarque en sus facultades de control y dirección laboral, el empleador no necesita del consentimiento de sus empleados, aunque sí está obligado a informarles. Entre los fines legítimos de control y dirección laboral está supervisar tareas, proteger bienes y recursos del empleador o verificar la adopción de medidas de seguridad y salud en el trabajo.

No está permitido en cambio la instalación de sistemas de grabación o captación de sonido ni de videovigilancia en los lugares destinados al descanso o esparcimiento de los trabajadores. La grabación con sonido sólo se admite cuando es relevante para los riesgos involucrados. Al igual que en cualquier sistema de videovigilancia, los empleadores deben ceñirse siempre al principio de proporcionalidad. Es decir, la instalación de las cámaras y el uso de las imágenes debe ser el adecuado y pertinente para los fines buscados y no puede excederse en su alcance.

Por otro lado, las organizaciones que usen sistemas de videovigilancia deben adoptar medidas de seguridad apropiadas y deben contar además con procedimientos para que los titulares de los datos puedan acceder a ellos, sin afectar los derechos de terceros que puedan aparecer en las imágenes grabadas. En lo que se refiere a la aplicación de los derechos ARCO específicamente en contextos laborales, se establece que los trabajadores podrán solicitar el acceso a las grabaciones o una copia digital de las inconductas o incumplimientos que se les haya imputado.

Una disposición muy importante que incluye la directiva concierne al tiempo de conservación de las imágenes. Estas se deben almacenar por 30 días como mínimo y 60 días como máximo. En caso de indicios de delito o falta, debe comunicarse de inmediato a la autoridad. Los archivos deben eliminarse dentro de los dos días siguientes al cumplimiento del plazo máximo. Estos plazos aplican también para la videovigilancia laboral. Sin embargo, las imágenes y voces sin editar que den cuenta de infracciones laborales o accidentes de trabajo deben conservarse por 120 días, salvo que existan razones que justifiquen su conservación por más tiempo.

2. Tratamiento de los datos personales de los trabajadores en el contexto del COVID-19

La emergencia del Covid-19 obligó a las autoridades peruanas a examinar aspectos específicos de la aplicación de la LPDP en el ámbito laboral y a pronunciarse sobre la tensión entre el derecho a la protección de datos y la obligación de los empleadores de proteger la salud de sus empleados.

Mediante Opinión Consultiva No. 32-2020-JUS/DGTAIPD, el pasado 5 de mayo, la ANPDP señaló que el derecho de protección de datos personales no es absoluto, por lo que su ejercicio debe armonizarse con el de otros derechos. En ese sentido, sostiene la ANPDP 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, entre las cuales destaca, 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, como la relación laboral.

Existiendo una relación contractual de trabajo entre empleador y trabajador, teniendo éste las obligaciones de garantizar la seguridad y la salud de todos los trabajadores y de adoptar las medidas de prevención de riesgos laborales y al estar inmersos en un estado de emergencia nacional y en una emergencia sanitaria declarados como consecuencia de una pandemia, 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." (Acápite 9)

De acuerdo con la opinión consultiva, en el contexto de una relación laboral y en el marco de la emergencia sanitaria, el tratamiento por parte de los empleadores de los datos sensibles relacionados con un "posible diagnóstico de coronavirus de los trabajadores" se justifica jurídicamente en el deber de aquéllos de prevenir los riesgos laborales a los que estos puedan estar sujetos.

Tal deber proviene, en palabras de la ANPDP, de la Ley de Seguridad y Salud en el Trabajo (Ley No. 29783), "según la cual el empleador ejerce un firme liderazgo y […] debe estar comprometido a fin de proveer y mantener un ambiente de trabajo seguro y saludable en concordancia con las mejores prácticas y con el cumplimiento de las normas de seguridad y salud en el trabajo" (Artículo 48. Rol del empleador). Acorde con dicho rol, la misma ley le establece obligaciones al empleador, entre las que están: "a) Garantizar la seguridad y la salud de los trabajadores en el desempeño de todos los aspectos relacionados con su labor, en el centro de trabajo o con ocasión del mismo; b) Desarrollar acciones permanentes con el fin de perfeccionar los niveles de protección existentes, y c) Identificar las modificaciones que puedan darse en las condiciones de trabajo y disponer lo necesario para la adopción de medidas de prevención de los riesgos laborales. […]" (Artículo 49. Obligaciones del empleador).

La ANPDP añade que "la legislación sobre protección de datos alude expresamente al interés y salud pública como factores que habilitan el tratamiento de datos personales relativos a la salud de las personas; lo que da cobertura al tratamiento de estos datos cuando existe una correspondencia con el diagnóstico o sintomatología propia del COVID-19, y a fin de que se adopten las medidas pertinentes para prevenir la propagación del virus dentro y fuera del centro laboral." (Acápite 32).

En este contexto y en el marco de la emergencia sanitaria, los empleadores se encuentran facultados para llevar a cabo el tratamiento de los datos sensibles de sus trabajadores referidos al Covid-19 sin necesidad de contar con su consentimiento previo y escrito, pero "siempre que este tratamiento se lleve a cabo con el debido respeto a la [LPDP] y su reglamento […] y tenga como fin garantizar la seguridad y salud en el trabajo con el objeto evitar los contagios de

esta enfermedad en los centros laborales". Lo anterior se justifica jurídicamente en la obligación del empleador de prevenir los riesgos laborales a los que los trabajadores puedan estar sujetos.

Específicamente, la Opinión Consultiva considera lícito que "el empleador implemente medidas preventivas dirigidas a detectar si alguno de sus trabajadores ha contraído el COVID-19, como, por ejemplo, la toma de su temperatura, pues 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." (Acápite 20).

La información recolectada debe ocurrir exclusivamente con el objetivo de salvaguardar la vida y la salud del trabajador sospechoso o confirmado y de sus "contactos", así como con el objetivo de evitar contagios en el centro de trabajo. No obstante, incluso en tal escenario, la identidad de los trabajadores calificados como casos sospechosos o confirmados debería, en principio, ser conocida sólo por el personal médico del departamento médico de la empresa y por los funcionarios que deban conocerla para poder alcanzar los objetivos antes indicados, garantizando siempre su confidencialidad. Pese a que en condiciones normales la información concerniente al estado de salud de un trabajador no debe ser de dominio del resto de trabajadores, la ANPDP establece que no solo es posible, sino también necesario, que dicha información sea revelada a otros trabajadores si su salud pudiera estar en riesgo y con el fin de reconstruir la cadena de contagios y adoptar las medidas correspondientes (Acápite 38).

Sin perjuicio de todo lo anterior, debe tenerse en cuenta que la ANPDP precisa que, en el contexto descrito, el empleador se constituye en responsable del tratamiento de datos personales y, por ello, el tratamiento que realice debe: (i) obedecer a la finalidad específica de contener la propagación del coronavirus, limitarse a esa finalidad y no extenderse a otras distintas, ni mantener los datos personales por más del tiempo necesario para la finalidad para la que se recaban; y, (ii) respetar la LPDP y su reglamento, en general, el deber de información y los principios de finalidad, proporcionalidad, calidad y seguridad, en particular.

En resumen, la ANPDP señaló que (a) los empleadores podrán tratar los datos personales de los empleados necesarios para garantizar la seguridad y salud en el trabajo con la finalidad de evitar la propagación de COVID-19 sin su consentimiento, cumpliendo con las demás disposiciones y obligaciones aplicables; (b) los trabajadores se encuentran obligados a cooperar y a brindar la información al empleador respecto al posible o real contagio que padezcan de COVID-19; y, (c) el tratamiento de datos personales de los trabajadores que realice el empleador con la finalidad de evitar la propagación de COVID-19 debe atender a lo establecido en la LPDP y su Reglamento, en especial a los principios de finalidad, calidad, proporcionalidad y seguridad que hemos descrito en el acápite anterior.

V. Comentarios finales

En la medida que los empleadores intensifiquen la implementación de nuevas tecnologías y se incremente la conciencia sobre las normas en materia de protección de datos personales, es posible que surjan nuevos conflictos en las relaciones laborales. Por ello, se hará cada vez más necesario reconciliar la tensión que puede presentarse entre los derechos fundamentales a la privacidad de los trabajadores y las oportunidades que ofrece el acelerado desarrollo de las tecnologías digitales para optimizar la gestión de las organizaciones, así como para hacer frente a nuevos retos como la inseguridad y la preservación de la salud.

Sobre esto último, la pandemia de COVID-19 mostró que pueden surgir situaciones inesperadas que lleven a examinar con más cuidado y revaluar las tensiones entre el derecho a la protección de datos sensibles como los de salud y el interés legítimo de preservar y garantizar la salud de los trabajadores en este difícil contexto. En el ámbito laboral, en cualquier caso, siempre es importante ser consciente de las responsabilidades legales que implica el manejo de datos personales y de los riesgos particulares asociados a su tratamiento. Por ello, las organizaciones deben examinar sus prácticas de privacidad y capacitar a su personal en la cultura de la confianza, a fin de cumplir con este derecho fundamental, así como evitar sanciones y demandas judiciales por daños ocasionados ante manejos inapropiados de la información.

Es cierto que existen aún más preguntas que respuestas sobre el uso de tecnologías como la inteligencia artificial, la geolocalización, el reconocimiento

facial y el tratamiento de los datos personales que se captan a través de ellas. En ese sentido, no queda duda que la irrupción de las nuevas tecnologías está revolucionando las diferentes esferas de la vida, incluyendo las relaciones laborales. Precisamente, este artículo es un esfuerzo por aportar mayor claridad respecto del tratamiento legal de la protección de datos personales y generar mayor sensibilidad sobre la problemática que presenta este derecho en este contexto tan particular y complejo.