

APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES EN LA RELACIÓN LABORAL

Mirella BERNAL SUÁREZ^()*

RESUMEN
EJECUTIVO

En el siguiente informe se sintetizan los doce oficios emitidos por la Autoridad Nacional de Protección de Datos Personales en los cinco últimos años del 2013 al 2017, relacionados a materia laboral (de 93 en diversas materias). Con la finalidad de conocer su postura ante determinados supuestos, tanto del Sector Público como del privado.

» PALABRAS CLAVE

Protección de datos personales / APDP / Datos sensibles / Redes sociales / Intervención de comunicaciones / Transferencia de datos / Consentimiento y excepciones / Marcador de asistencia / Videovigilancia / Derecho de cancelación / SCTR / Sanciones disciplinarias

Recibido : 01/03/2018

Aprobado : 08/03/2018

Introducción

La Autoridad Nacional de Protección de Datos Personales, en adelante APDP, conforme con el numeral 10 del artículo 33 de la Ley N° 29733, Ley de Protección de Datos personales (en adelante, LPDP), tiene la facultad para absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en dicha materia.

El ejercicio de dicha facultad debe revisarse, sobre todo por las multas impuestas por dicha autoridad, así pues, de las 27 resoluciones emitidas en los procedimientos

sancionadores de 2017, encontramos como multa máxima impuesta, la suma ascendente a 10 UIT.

Con la finalidad de colaborar con el entendimiento de las opiniones a continuación descritas, citaremos los sustentos legales utilizados:

- El numeral 4 del artículo 2 de la LPDP define a los datos personales como “toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados”.
- La LPDP y su Reglamento otorga especial protección a los datos sensibles definiéndolos en el numeral 5 del artículo 2 de la ley como aquellos “Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual”.

(*) Abogada por la Universidad de Piura. Egresada de la Maestría en Derecho de la Empresa y de la Maestría de Seguridad y Salud en el Trabajo, por la misma casa de estudios.

- La transferencia de datos personales está definida en el numeral 18 del artículo 2 de la LPDP como “Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.
- Es tratamiento de datos personales: “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”, según lo regulado en el numeral 19 del artículo 2 de la LPDP.
- En cuanto al ámbito de la LPDP, el artículo 3 de la misma señala: “La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional (...”).
- El numeral 1 del artículo 13 de la LPDP, reconoce que el tratamiento de datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta Ley les confiere.
- Aunado a ello, el numeral 4 del artículo 13 de la LPDP reconoce que: “Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley (...”).
- El tratamiento de los datos personales debe realizarse con el consentimiento de su titular, cuyos requisitos se encuentran regulados en el numeral 5 del artículo 13, que indica: “(...) El consentimiento debe ser previo, informado, expreso e inequívoco”.
- La regla general sobre el consentimiento ante datos sensibles está regulada en el numeral 6 del artículo 13: “En el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público”.
- El consentimiento tiene excepciones, las cuales las encontramos reguladas en el artículo 14 de la LPDP, así pues, el numeral 1 de dicho artículo indica: “Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias”.
- Adicionalmente en el numeral 5, se regula otra excepción: “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”.
- La LPDP establece limitaciones al consentimiento, entre las que se encuentra una específica sobre limitaciones al consentimiento para el tratamiento de datos personales relativos a la salud, el numeral 6 del artículo 14, dispone que no se requiere el consentimiento del titular de los datos personales para los efectos de su tratamiento “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”.

- Otra excepción para el principio del consentimiento la encontramos en el numeral 9 del artículo 14 de la LPDP: “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”.
- El artículo 20 de la LPDP recoge el derecho de cancelación de los titulares de la siguiente manera: “El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento (...”).
- El derecho de oposición está regulado en el artículo 23 de la LPDL, que establece: “Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado de tratamiento de datos personales, según

corresponda, debe proceder a su supresión, conforme a ley”.

- El Reglamento de la LPDP, en su numeral 5 del artículo 2 define a los datos sensibles relacionados con la salud como “aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética”.

I. MATERIAS INSPECCIONADAS

1. DATOS SENSIBLES RELACIONADOS CON LA SALUD

Sobre la cuestión si las aseguradoras pueden proporcionar información al empleador sobre los trabajadores con seguro de invalidez por incapacidad absoluta permanente, mas no la enfermedad o causa de la misma, para la Autoridad de Protección de Datos Personales a falta de una norma con rango de ley que por razones de interés público ampare la transferencia de los datos de salud en la forma antes descrita, dicha transferencia solo puede realizarse conforme a la LPDP y su reglamento, es decir, habiendo obtenido el consentimiento previo, informado, expreso y por escrito del asegurado; en otras palabras el empleador no pueda obtener la información médica, de modo directo y de un prestador de servicios de salud en capacidad de emitir un informe médico, en el marco de la relación laboral.

2. TRATAMIENTO DE DATOS PERSONALES EN REDES SOCIALES

La información contenida en los perfiles de los usuarios de las redes sociales, incluye datos personales, y en principio, su tratamiento depende del consentimiento del titular de datos personales (usuario de la cuenta), al tratarse de una persona natural.

Además, la información cuya configuración es pública, en la red social, continúa

perteneciendo a la esfera de la privacidad del usuario, conforme con lo señalado en los numerales 4 y 5 del artículo 2 de la LPDP y numerales 4 y 6 del artículo 2 del Reglamento de la LPDP, por lo tanto, su tratamiento debe hacerse de acuerdo con la legislación de la materia, aunque el acceso esté autorizado.

3. Excepción al consentimiento referida al tratamiento de datos personales necesarios para la ejecución contractual

Debe precisarse, si los tratamientos de los datos personales, son necesarios e indispensables para el desarrollo de la relación contractual, en el presente caso, la relación entre los trabajadores y el Banco Central de Reserva, el tratamiento se encontrará amparado en el marco de dicha excepción. El análisis del contenido de lo previsto en la relación contractual y en cada una de las prestaciones asumidas por las partes al momento de la celebración del contrato, corresponde a su institución, así como el análisis de la posición de los titulares de los datos personales en dicha relación contractual, a fin de establecer si la situación de hecho encuadra en la excepción.

En caso alguna de las partes haya previsto la realización de prestaciones adicionales a la relación contractual (gratuitas u onerosas), cuyo cumplimiento demande el tratamiento adicional de datos personales (sea porque se necesitan más datos o porque se incorporará tratamiento de datos sensibles), será necesario contar, entonces, con el consentimiento del titular de la información; y para ello deberá observarse las características y condiciones previstas tanto en la LPDP y su Reglamento. Dicho consentimiento debe solicitarse de forma previa, informada, expresa e inequívoca, y en caso de tratamiento de datos sensibles, dicho consentimiento debe ser escrito.

En definitiva, deberá evaluarse si las prestaciones realizadas a través del Fondo para Enfermedades, Seguros y Pensiones de

Empleador del Banco Central de Reserva del Perú son necesarias e indispensables para el desarrollo de la relación contractual entre el Banco y los empleados y si la adherencia a este fondo, en el marco de su contrato de trabajo es obligatoria o facultativa; y bajo estas consideraciones evaluar la pertinencia de cumplir con el principio del consentimiento, o considerar aplicable alguna de las excepciones.

4. Consentimiento como regla general aplicable a las transferencias de datos personales de una aseguradora a un empleador

Se preguntó en dos oportunidades, sobre la transferencia de información (datos personales) entre la aseguradora y la empresa contratante respecto de los servicios prestados a trabajadores de la contratante, obteniendo como respuesta, en primer lugar, que dicha transferencia no se encuentra entre las finalidades del tratamiento de datos personales y, en segundo lugar, no encuentran soporte legal en las excepciones al consentimiento.

En definitiva, cualquier transferencia de información entre la aseguradora y la empresa contratante, no imprescindible para la ejecución de la relación vinculante, deberá sujetarse a los lineamientos antes descritos.

5. Garantías previstas en la LPDP sobre la intervención de las comunicaciones y/o telecomunicaciones de carácter o uso privado

Respecto de su consulta sobre el uso del correo electrónico asignado a los trabajadores de una empresa con fines laborales, según la APDP la intervención del contenido de los mismos para acceder al contenido de los correos no constituye un tema de su competencia de esta autoridad, el mismo está vinculado a la tutela de otros derechos, competencia de otras entidades del Estado.

6. Derecho de cancelación en el ejercicio de la relación laboral

Se consultó si los trabajadores de una institución educativa, durante la vigencia de la relación pueden ejercer su derecho de cancelación o supresión de sus datos personales.

Si bien es cierto, el titular de los datos personales tiene la facultad de ejercer el derecho de cancelación, de acuerdo al Reglamento de la LPDL, este no procede si existen motivos fundamentados como el caso de la consulta, cuando entre el empleador y el titular de los datos personales existe un vínculo laboral y el tratamiento de los datos personales resulte necesario e importante para que el empleador cumpla sus obligaciones en el marco de la relación contractual mencionada.

7. Videovigilancia en centros laborales

Por medio del Oficio N° 611-2016-JUS-DGPDP, se absolvió la consulta si las grabaciones realizadas por razones de seguridad al personal en las entradas, salidas y al interior de las áreas de una entidad, se encuentra dentro de los alcances de la normativa de protección de datos personales.

Al ser la imagen un dato personal, se debía analizar si los datos recopilados son necesarios para cumplir la finalidad de la seguridad. Es decir, se debe determinar si la grabación de las imágenes es la única forma de garantizar la seguridad, aunado a ello se revisará si los lugares con cámaras de seguridad instaladas, invaden o no la privacidad de los trabajadores.

En conclusión, debe informarse a las personas a grabarse, de forma previa a dicho tratamiento, por ejemplo, a través de un aviso visible ubicado antes de ingresar a los lugares con cámaras instaladas, en el cual se detalle la información conforme al numeral 4 del artículo 12 del Reglamento de la LPDP:

4. Informado: Cuando al titular de los datos personales se le comunique

clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de 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 almacenan, 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.

8. Tratamiento de datos personales contenidos en el marcador de asistencia de un centro laboral

La huella digital es un dato personal sensible, por lo tanto, para su tratamiento se requiere consentimiento por escrito del titular, sin embargo, de acuerdo al artículo 14, se deduce como excepción al consentimiento cuando este resulte necesario e imprescindible para el cumplimiento de la relación laboral entre el trabajador y empleador, por ello el tratamiento mencionado está dentro de dicha excepción.

Así pues, la hora de entrada y salida de los trabajadores de una institución no constituyen una invasión a la intimidad personal y familiar, puesto que, recoge información sobre el cumplimiento del horario de trabajo, para verificar el cumplimiento de sus obligaciones.

Es decir, si el titular del dato personal solicita a la institución pública no entregar la información mencionada deberá solicitarlo fundamentando los motivos relacionados a una concreta situación personal, conforme a lo señalado en el artículo 22 de la LPDP: “Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado de tratamiento de datos personales, según corresponda, debe proceder a su supresión, conforme a ley”.

Teniendo en cuenta ello, al no requerirse consentimiento, deberá evaluarse la solicitud de oposición del titular del dato personal en cada caso concreto.

9. Criterios para entregar la información sobre el resultado de exámenes médicos en el ámbito del Seguro Complementario de Trabajo de Riesgo

Para la APDP, la información respecto de los resultados médicos realizados se entregará al titular de los datos personales, es decir, al trabajador, guardando la confidencialidad del caso. Sin embargo, el médico ejecutor de dichos exámenes puede informar en términos generales el estado de salud de los trabajadores, únicamente con la finalidad de implementar medidas de preventión pertinentes respecto a la salud de los trabajadores.

Por lo tanto, la empresa aseguradora encargada de realizar los exámenes médicos no debe entregar la información sobre la salud de un trabajador específico al empleador del

mismo sin el consentimiento por escrito del trabajador. Lo cual, no le impide al empleador solicitar a los trabajadores la entrega de documentación, acreditando el cumplimiento de los requisitos necesarios para la ejecución de la relación contractual.

10. Condiciones para el tratamiento de datos sensibles en el marco del ejercicio de las entidades públicas

La información respecto de la entrega de una resolución en la cual se impone una sanción a un trabajador de una institución pública bajo el amparo del derecho de acceso a la información pública no colisiona con el derecho a la protección de datos personales, por ser información considerada pública de acuerdo a la Ley de Transparencia y Acceso a la Información Pública y no constituye invasión a la intimidad personal y familiar, pue se refiere a circunstancias suscitadas en el ámbito laboral, merecedoras de una sanción.

Respecto a la entrega de información sobre remuneraciones o ingresos económicos, si bien se trata de datos personales sensibles, es preciso señalar el numeral 6 del artículo 14 de la LPDP el cual establece “en caso de datos sensibles (...) Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes del interés público”.

Por ello, si bien las remuneraciones de trabajadores públicos constituyen datos sensibles, pueden tratarse sin consentimiento del titular cuando una ley lo autorice siempre y cuando medie un importante interés público, como es el caso de la Ley de Transparencia y Acceso a la Información Pública.

11. Criterio para el tratamiento de los datos personales en el marco de las sanciones disciplinarias

Mediante el Oficio N° 278-2017-JUS-DGDPD, se absuelve la consulta de una entidad pública, sobre si resulta válido rectificar

el récord administrativo de un trabajador desistiendo de consignar las sanciones disciplinarias dejadas sin efecto por orden judicial o hacer precisión en dicho documento que la sanción fue dejada sin efecto por mandato judicial.

Al respecto, la Dirección de Protección de Datos Personales, menciona las siguientes disposiciones:

- El inciso 12 del artículo 2 del Reglamento de la LPDP define a la rectificación como “acción genérica destinada a afectar o modificar un banco de datos personales ya sea para actualizarlo incluir información en él o específicamente rectificar su contenido con datos exactos”.
- El artículo 27 de la LPDP señala: “Los titulares y los encargados de tratamiento de datos personales de Administración Pública pueden denegar el ejercicio de los derechos de acceso, supresión y oposición por razones fundadas en la protección de derechos e intereses de terceros o cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, a las investigaciones penales sobre la comisión de faltas o delitos, al desarrollo de funciones de control de la salud y del medio ambiente, a la verificación de infracciones administrativas, o cuando así lo disponga la ley”.
- De acuerdo al artículo 21 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, señala: “Es responsabilidad del Estado crear y mantener registros públicos de manera profesional para que el derecho a la información pueda ejercerse a plenitud. En ningún caso la entidad de la Administración Pública podrá destruir la información que posea. La entidad de la Administración Pública deberá remitir al Archivo Nacional la información que obre en su poder, en los plazos estipulados por la Ley de la materia. El Archivo Nacional podrá destruir la información que no tenga utilidad pública, cuando haya transcurrido un plazo razonable durante el cual no se haya requerido dicha información y de acuerdo a la normatividad por la que se rige el Archivo Nacional”.
- Además, el artículo 69 del RLPDP establece: “La supresión no procederá cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular de los datos personales, que justifiquen el tratamiento de los mismos”.

En conclusión, no corresponde suprimir información del récord administrativo de un trabajador de una institución pública, pero sí corresponde actualizar dicho récord conforme al principio de calidad.

Conclusiones

A continuación, un cuadro con el detalle de las opiniones emitidas por la Dirección de Protección de Datos Personales, relacionadas a materia laboral:

Número de oficio / Informe	Materia de consulta
429-2014-JUS-DGPDP	Datos sensibles relacionados con la salud.
569-2014-JUS-DGPDP	Tratamiento de datos personales en redes sociales.
470-2015-JUS-DGPDP	Excepción al consentimiento referida al tratamiento de datos personales necesarios para la ejecución contractual.

569-2015-JUS-DGPDP	Consentimiento como regla general aplicable a las transferencias de datos de salud de una aseguradora a un empleador.
572-2015-JUS-DGPDP	Consentimiento como regla general aplicable a las transferencias de datos personales de una aseguradora a un empleador.
631-2015-JUS-DGPDP	Garantías previstas en la LPDP sobre la intervención de las comunicaciones y/o telecomunicaciones de carácter o uso privado.
610-2016-JUS-DGPDP	Derecho de cancelación en el ejercicio de la relación laboral.
611-2016-JUS-DGPDP	Videovigilancia en centros laborales.
862-2016-JUS-DGPDP	Tratamiento de datos personales contenidos en el marcador de asistencia de un centro laboral.
19-2017-JUS-DGPDP	Criterios para entregar la información sobre el resultado de exámenes médicos en el ámbito del Seguro Complementario de Trabajo de Riesgo.
273-2017-JUS-DGPDP	Condiciones para el tratamiento de datos sensibles en el marco del ejercicio de las entidades públicas.
278-2017-JUS-DGPDP	Criterio para el tratamiento de los datos personales en el marco de las sanciones disciplinarias.