# Perú: retos del derecho fundamental a la protección de datos personales*

## *Peru: challenges to the fundamental right to personal data protection*



✍ Lourdes Zamudio Salinas**

***Resumen***

El presente trabajo tiene como fin abordar los principales retos, que debe afrontar el Perú, con el objetivo de cumplir con garantizar el derecho fundamental a la protección de datos personales; derecho reconocido en el artículo 2, inciso 6) de la Constitución Política de 1993 y regulado por la ley N° 29733, Ley de Protección de Datos Personales. Se establece que, es necesario poner en funcionamiento los

* El Tribunal Constitucional denomina al derecho reconocido en el artículo 2°, inciso 6 de nuestra carta fundamental, como el derecho a la autodeterminación informativa en la gran mayoría de sus sentencias (…) Nuestro alto tribunal señaló que tomó de la doctrina esa denominación del derecho. (…) No obstante no siempre nuestro máximo intérprete de la Constitución (…) también, si bien es cierto en muy contadas ocasiones, lo ha denominado como derecho a la protección de datos personales, (…) la Ley Nº 29733 Ley de protección de datos personales, utiliza la denominación de "derecho fundamental a la protección de datos personales". La Ley Peruana, sigue la tendencia legislativa mayoritaria en Iberoamérica de la denominación del derecho que nos ocupa, como derecho a la protección de datos personales. En atención a lo señalado, será propio en nuestro contexto jurídico, referirnos indistintamente al mismo derecho como derecho a la protección de datos personales (calificación legal) o como derecho a la autodeterminación informativa (calificación del Tribunal Constitucional) (Zamudio 2014: 1159-1162).

** Abogada por la Universidad de Lima. Magíster en Derecho con mención en Derecho Constitucional por la Pontificia Universidad Católica del Perú. Docente en las universidades: Universidad de Lima (pregrado), Esan (posgrado) y UNED (maestría).

tres pilares que conforman la triple base para el debido tratamiento de la información personal, los cuales son: el responsable del tratamiento o titular del banco de datos, la autoridad de control; y el titular del dato. Ello con la finalidad de que en un Estado Constitucional de Derecho se garantice el derecho a la protección de datos personales.

***Palabras clave***

Derecho a la protección de datos personales, protección de información, autoridad de control, Estado Constitucional.

***Abstract***

The purpose of this paper is to address the main challenges that Peru must face in order to comply with the fundamental right to the protection of personal data; a right recognized in Article 2, paragraph 6) of the Political Constitution of 1993 and regulated by Law No. 29733, Personal Data Protection Law. It is established that it is necessary to put into operation the three pillars that make up the triple basis for the proper treatment of personal information, which are: the data controller or owner of the database, the supervisory authority, and the owner of the data. The purpose of this is to guarantee the right to the protection of personal data in a Constitutional State under the rule of law.

***Keywords***

Right to the protection of personal data, protection of information, supervisory authority, Constitutional State.



## *Sumario*



La era digital en la que nos encontramos, nos trae la posibilidad de usar diversas tecnologías que suponen modificaciones y ventajas para atender distintas necesidades de nuestra vida individual y social, a nivel nacional o internacional; tecnologías elegidas por nosotros mismos o dispuestas por el Estado.

Solo como un ejemplo de lo señalado, tomemos en cuenta las tecnologías de la información y de las comunicaciones que, a través de internet, nos permitieron, en el contexto del desarrollo de las estrategias para enfrentar la pandemia del COVID- 19, sustituir entornos presenciales por entornos virtuales en diversos ámbitos; tales como el teletrabajo, la educación virtual a través de distintas plataformas, el incremento del comercio digital, las atenciones de salud a través de

tele consultas, apps, rastreo digital, reuniones y celebraciones sociales de distinta índole, entre muchas otras actividades; las cuales se hicieron posible gracias a la tecnología y al incremento de su uso. Entornos virtuales que, en su mayoría, no se han dejado de utilizar por el retorno a las actividades presenciales.

Debemos ser conscientes que diversas tecnologías suponen el tratamiento de nuestra información personal y que el indebido uso de la misma puede concretarse en riesgos (de distinto grado) para nuestros derechos y dignidad; uno de los que puede resultar afectado es el derecho fundamental a la protección de datos personales. El considerando 6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo –RGPD– lo señala de la siguiente forma:

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, (…).



Asimismo, el dinamismo de las distintas tecnologías supera siempre a las normas jurídicas y a la conciencia de lo que su uso supone o puede suponer para los titulares de los datos personales; y es que:

El avance de nuevas tecnologías en el entorno tecnológico actual conlleva modelos de procesamiento de datos personales innovadores, variados e intensivos. (…) el cómputo en la nube; la minería digital; el procesamiento masivo de datos identificado como big data; la conectividad de dispositivos en un internet de todo; el registro confiable y seguro de las operaciones y transacciones a través de la criptografía, aplicaciones blockchain y smartcontract; la automatización de procesos y el uso de algoritmos en la industria y la robótica; (…) la inteligencia artificial[1].

Todo lo cual plantea de manera constante diversos retos para que el uso de estas tecnologías se haga con adecuación a la legislación sobre protección de datos personales y con respeto a la dignidad de las personas, titulares de la información, objeto de tratamiento.

1 Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial. Red Iberoamericana de Protección de Datos. 2019. p. 6.

Estamos convencidos de que la tecnología forma parte de nuestra vida, que su utilización es necesaria para nuestro desarrollo personal y social, y que el uso de nuestros datos personales y su intercambio van involucrados en este proceso en constante crecimiento; pero a la vez, como Estado Constitucional de Derecho debemos hacer todos los esfuerzos para lograr un equilibrio entre su uso y el respeto de los derechos y la dignidad de las personas; así como, entre todos los derechos e intereses constitucionalmente relevantes en juego. Esto constituye un reto que tiene que ser asumido desde diferentes actores y en diferentes ámbitos.

En el presente trabajo vamos a abordar los principales retos, que debe afrontar el Perú, con el objetivo de cumplir con garantizar el derecho fundamental a la protección de datos personales; derecho reconocido en el artículo 2, inciso 6) de la Constitución Política de 1993 y regulado por la Ley N° 29733, Ley de Protección de Datos Personales, en adelante la Ley; la misma que fue objeto de reglamentación a través del D.S. N° 003-2013-JUS,[2] en adelante el Reglamento.

Consideramos importante no perder de vista el contenido del derecho a la protección de datos personales:



> El contenido del derecho a la protección de datos personales se delimita a través de los derechos (ARCO) que le corresponden a su titular y de los principios rectores que deben ser observados por los titulares de los bancos de datos o responsables del tratamiento, así como por los encargados del mismo. Si no se reconocieran estos derechos y no se observaran estos principios se desdibujaría este derecho fundamental y autónomo (Zamudio, 2021 p. 69)

Nosotros sostenemos que para que en un Estado Constitucional de Derecho se garantice el derecho a la protección de datos personales, se deben poner en funcionamiento de manera sinérgica los tres pilares que conforman la triple base para el debido tratamiento de la información personal, cualquiera sea el contexto en que la actividad de tratamiento se realice; los pilares están constituidos por:

– El responsable del tratamiento o titular del banco de datos:
– La Autoridad de Control; y
– El titular del dato.

En atención a lo acabado de delimitar, dividiremos el presente trabajo teniendo en cuenta los tres pilares señalados.

2 Así como por su modificatorias correspondientes.

## I. RETOS PARA LOS RESPONSABLES DEL TRATAMIENTO

La figura del responsable del tratamiento o, en su caso, Titular del banco de datos personales[3] es vital para los efectos de la responsabilidad que va a derivarse del incumplimiento de lo que establece la Ley de Protección de Datos Personales, y el Reglamento[4] frente al titular de la información que está siendo objeto de un indebido tratamiento; y además, frente a la misma autoridad de control administrativa sobre la materia, es decir la Autoridad Nacional de Protección de Datos personales; o en su caso, de la Autoridad jurisdiccional correspondiente.

El responsable es quien decide sobre el tratamiento de los datos personales que se va a realizar. A su vez el encargado de tratamiento será quien realiza la gestión de los datos personales por encargo del responsable, en virtud de una relación jurídica que le vincula con este y delimita el ámbito de su actuación.[5]

La ley, en su Título IV, sobre obligaciones del titular y del encargado de tratamiento de datos personales, en el único artículo que lo conforma, el 28; tiene 9 incisos que señalan obligaciones que le corresponden a ambos; culminado con la declaración genérica, en su último inciso, que dispone que las obligaciones referidas en el presente artículo no terminan en ellas; sino que también son obligaciones las otras establecidas en la Ley y en el Reglamento. Es claro pues que los responsables y encargados de tratamiento deben cumplir con todas las disposiciones establecidas en la Ley y en el Reglamento.[6]



En atención a los límites de este trabajo plantearemos determinadas reflexiones sobre algunas obligaciones derivadas de la legislación sobre la materia en el Perú.

---

3 Ver artículo 2, inciso 17) de la Ley sobre Titular del banco de datos y artículo 2, inciso 14) del Reglamento de la Ley, sobre responsable del tratamiento.

4 Para la Ley peruana, el titular del banco de datos personales será la persona natural o jurídica que determina la finalidad y el contenido del banco de datos personales, así como el tratamiento de éstos y las medidas de seguridad que correspondan. La Ley peruana no incorpora, en su texto, la figura del responsable del tratamiento. El Reglamento de la Ley, incorpora dentro de las definiciones a la figura del responsable del tratamiento como aquél que decida sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos.
Consideramos que la figura del responsable del tratamiento es un concepto más amplio que abarca tanto al titular del banco de datos como a quien decida sobre el tratamiento de datos personales, independientemente de que los datos consten o no en un banco. Coexistirían entonces para legislación peruana la figura del titular del banco de datos con la del responsable del tratamiento. Zamudio salinas, María de Lourdes. El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del sistema de geolocalización GPS. Límites y propuestas P. 49.

5 Reglamento de la Ley art.2, inciso 10).

6 Lo que tiene su correlato a la hora en que la Ley establece las infracciones y las sanciones correspondientes a las mismas.

## 1. Situaciones de incumplimiento

Para el Perú, como para la mayoría de los países en América latina, el eje fundamental sobre el que gira todo el sistema jurídico de protección de datos personales es el consentimiento[7] del titular del dato, como elemento que va a legitimar que su información personal sea tratada por un tercero. Como sabemos, el consentimiento para que sea válido, debe cumplir determinadas características; tales como el ser: libre, informado, expreso e inequívoco.

El responsable del tratamiento, con relación al consentimiento que necesita del titular del dato, debe cuidar que esté debidamente informado de todas las condiciones a las que será sometida su información personal; información detallada en la Ley[8] y el Reglamento[9]. No importando si el medio por el cual se está solicitando el consentimiento sea una página web, telefónicamente, un documento escrito, una vídeo conferencia, etc. Además, el consentimiento debe ser recabado de manera previa al inicio de las operaciones del tratamiento y no una vez iniciado o realizado el mismo.



No siempre los responsables del tratamiento cumplen con informar todo lo que la Ley señala; el incumplimiento muchas veces está no solo porque no se brinda al titular toda la información debida; sino porque la forma en que esta es presentada no le es comprensible; incumpliéndose el objetivo de que quien va a dar el consentimiento sepa exactamente para qué lo va a dar.

La situación se vuelve más compleja si el tratamiento se va a realizar por una tecnología disruptiva, como la inteligencia artificial o el internet de las cosas (loT) lo que en determinadas circunstancias debería suponer, además, que la información que se le dé al titular del dato, le ayude a comprender las consecuencias que el tratamiento de su información va a tener con relación a él.

Los responsables del tratamiento tampoco deberían realizar una recopilación de los datos personales por medios fraudulentos desleales o ilícitos. En nuestra sociedad, y como ejemplo más latente, vemos la venta de bases de datos, como práctica que "no se puede detener" en un mercado que se caracteriza en gran medida por la informalidad; esa forma de recopilación supone que distintos aspectos de la vida de muchas personas estén siendo tratados sin tener control sobre el destino que se dará a esa información, y que en muchos casos, no es

7 Salvo ley autoritativa y con excepción de los supuestos consignados en el artículo 14 de la Ley.

8 Artículo 18.

9 Artículo 12.

un destino o fin lícito; lo cual se traduce o, se puede traducir, en un evidente riesgo para la vida, para la salud y para otros derechos de los titulares de esa información.

Otra forma de inobservancia de la Ley, por parte de los responsables, es que una vez recabado el consentimiento decidan utilizar la información para una finalidad diferente a la autorizada por el titular. Esto se puede producir, por ejemplo, por el uso de una nueva tecnología para el tratamiento de los datos que ya se estaba realizando; o porque incorporó otra finalidad que resulta beneficiosa para el cumplimiento de los objetivos o intereses del responsable, sin tomar en cuenta el derecho del titular de la información[10].

El responsable del tratamiento también debería implementar protocolos o mecanismos adecuados para garantizar que los datos personales que están tratando sean exactos estén completos y sean actualizados; de lo contrario, se afectaría la calidad del dato y eventualmente también el cumplimiento de la finalidad para la cual fueron recabados[11].

Otro aspecto fundamental, sin el cual no hay debido tratamiento de datos personales, es el cumplimiento de las medidas de seguridad organizativas técnicas y legales[12] que deben implementarse teniendo en cuenta: los datos que son materia de tratamiento, las actividades de tratamiento y las tecnologías que se usarán para dicha actividad; evaluando los riesgos que puedan producirse durante todo el ciclo de vida de los datos personales que van a ser objeto de tratamiento con el fin de implementar las medidas necesarias para garantizar la confidencialidad la integridad y disponibilidad de la información.



Son de distintas clases las medidas de seguridad que se deben implementar; por lo tanto, si estas no se determinan y aplican, se incurriría en un incumplimiento.

Habría que preguntarse si los responsables del tratamiento se han encargado de que todas las personas de su organización, que entran en contacto con los datos personales, han sido debidamente capacitadas en la legislación sobre la materia y sobre su aplicación a las actividades del tratamiento de datos personales en las que estarán participando (medida de seguridad organizativa).

10 Principio de finalidad. Artículo 6 de la Ley.

11 Principio de calidad. Artículo 8 de la Ley.

12 Principio de seguridad. Artículo 9 de la Ley.

Asimismo, si se han implementado medidas de seguridad técnicas y si esas son las adecuadas; pues no serán las mismas aquellas elegidas para proteger los datos personales sensibles que para proteger un dato personal de categoría general; o, si los datos son objeto de transferencia nacional o flujo transfronterizo; además, si dichas medidas son objeto de una revisión o auditoría periódica.

Con relación a las medidas de seguridad legales como: los contratos con el personal autorizado para alguna actividad de tratamiento; las cláusulas de información para la obtención del consentimiento; o las de confidencialidad; así como los protocolos correspondientes; primero se tendrá que ver si se han tomado en consideración y, luego, analizar si su implementación es adecuada a lo que dispone la legislación.

¿Qué consecuencias puede tener para el titular del dato si su información personal está siendo conocida por una persona no autorizada?; o, si ha sido modificada indebidamente?; o, si ¿ha sido borrada?

Muchas de las consecuencias no se pueden prever; y al margen de que puedan suponer afectaciones (de diversa gravedad) para algunos de los derechos, en el presente o en el futuro; no realizar el tratamiento de los datos con la debida seguridad; así como otros incumplimientos de la legislación sobre protección de datos, afecta directamente al contenido esencial del derecho que nos ocupa; pues dentro de su contenido, se encuentra que el titular debe poder controlar lo que se está haciendo con su información personal y; en todo caso, si esta se hubiese perdido, debe poder recuperarla.



Este tema trae a consideración que uno de los deberes fundamentales del responsable consiste en que debe almacenar y tratar los datos personales de tal forma que se puedan ejercer los derechos ARCO[13] que le competen al titular de la información, como mecanismo fundamental para que este no pierda el control que le corresponde, independientemente de la tecnología que se esté utilizando.

Hay normativas más garantistas que nuestra legislación sobre la materia, referida a diversos aspectos regulados; un ejemplo de lo que señalamos es que nuestra Ley no incluye la obligación de notificar, en determinados supuestos, las vulneraciones de seguridad a la Autoridad Administrativa de Control sobre la materia, ni al titular cuya información ha sido afectada; como si lo dispone el RGPD[14]

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

14 RGPD Artículo 33.

de la unión europea; los Estándares de Protección de Datos Personales para los Estados Iberoamericanos [15], entre otros cuerpos normativos internacionales[16].

Otra forma de incumplimiento puede generarse cuando el responsable decide utilizar una nueva tecnología (con relación a la que venía utilizando para el tratamiento) que le proporciona más información personal que la que él necesita para cumplir el fin legítimo que habilitó el tratamiento y que lo legitimó a actuar como tal[17]; con lo que el titular del dato quedará en ignorancia sobre el uso de esa información excesiva que le concierne; imposibilitándosele a él, el realizar el control que le corresponde.

Podríamos seguir detallando muchísimas situaciones de incumplimiento de la legislación sobre protección de datos personales, lo que no es el objetivo de este trabajo; por ello y frente a ello plantearemos lo que se puede hacer para actuar como responsables y encargados del tratamiento, de conformidad con lo que dispone la legislación sobre la materia.

## 2. Principal mecanismo para actuar dentro de la Ley



Las leyes sobre protección de datos personales son de carácter general; es decir no desarrollan sus disposiciones para cada uno de los distintos sectores de la actividad privada y pública donde se realizan las actividades de tratamiento de datos personales; no existen disposiciones específicas para el tratamiento de los datos personales en distintos ámbitos, tales como los de la educación; financiero; de salud; migratorio; de telecomunicaciones; de comunicaciones electrónicas; agrario; minero; laboral; comercial; farmacéutico, entre muchos otros.

A esto se suma el incremento del uso de diversas tecnologías para el tratamiento de la información personal con capacidades de procesamiento con características cada vez más potentes y variadas en cada uno de los distintos sectores.

Entonces ¿cómo pueden hacer los responsables y los encargados para concretar las disposiciones de la Ley a las actividades de tratamiento que les corresponde realizar, y avanzar con seguridad respetuosa de la normativa y de los derechos involucrados?

15 RIPD Artículo 22.

16 La notificación del incidente de seguridad fue incluida como propuesta en el proyecto de Ley N° 7870/2020-PE, presentado por el Poder Ejecutivo.

17 Principio de proporcionalidad. Artículo 7 de la Ley.

El mecanismo o medio más útil con el que pueden contar los responsables y encargados de los tratamientos son los Principios Rectores de la protección de datos personales.

La Ley peruana con carácter enunciativo, consagra los siguientes ocho principios rectores[18]: legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición de recurso y nivel de protección adecuado.

Sobre los principios, Zamudio (2021) indica:

> De conformidad con lo señalado en el artículo 12 de la Ley, los principios constituyen guías para la actuación de los titulares de los bancos de datos personales, así como de los responsables y encargados de su tratamiento y, en general, de todos los que intervengan en alguna actividad de tratamiento con relación los datos personales; sirven de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su Reglamento; constituyen parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia.
>
> Los principios servirán como parámetro obligatorio para determinar el nivel suficiente de protección de los datos personales; la Autoridad Nacional



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

> de Protección de Datos Personales tiene como una de sus funciones explícitas velar por el respeto de los principios; y para cerrar el círculo, se establecen infracciones pasibles de sanción al tratamiento de datos personales contraviniendo los principios consagrados en la Ley (pp. 44-45).

Es importante tener en cuenta que la observancia de los principios no es solo a modo de guía; sino que son parámetros de obligatorio cumplimiento en todos los tratamientos de datos personales; esto es lo que en gran medida determinará si se está frente a un debido o indebido tratamiento.

El reto claro y urgente consiste en la observancia y debido cumplimiento de los principios rectores a la hora de cada actividad de tratamiento; lo que pasa porque los responsables no solo conozcan la existencia de los principios, sino que los entiendan de tal manera que estén en capacidad de aplicarlos, ellos y todas las personas que intervienen en actividades de tratamiento de información personal al interior de sus organizaciones.

Parte del reto para los responsables del tratamiento es instaurar una cultura organizacional de la protección de datos personales, como política transversal y holística al interior de sus organizaciones.



No obstante lo señalado, en la era digital ya no basta con el mero cumplimiento de la legislación sobre protección de datos personales; se requiere ir más allá; hacia un cumplimiento ético de la misma.

## II. RETO PARA LAS AUTORIDADES DE CONTROL ADMINISTRATIVAS

La Autoridad Nacional de Protección de Datos Personales recae en la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, dentro del Ministerio de Justicia y Derechos Humanos. Garantiza el derecho fundamental a la protección de datos personales, velando por el cumplimiento de las normas sobre la materia. Ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.

La existencia de la autoridad de control administrativa, persigue darle sentido pleno a la legislación sobre la materia, en la medida que viene a fortalecer el marco de garantías que el proceso jurisdiccional del Hábeas Data ya otorgaba antes del año 2011, en que se promulga la Ley; y, que se consideraba insuficiente para el debido tratamiento de la información personal, en el contexto de la era digital, teniendo en cuenta las exigencias de la protección que el Estado le debe dar a un derecho fundamental de última generación, como el que nos ocupa.

Son muy importantes y diversas las funciones que la Ley le asigna a la Autoridad Nacional de Protección de Datos Personales[19].

19 Ley: Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales
La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

1. Representar al país ante las instancias internacionales en materia de protección de datos personales.
2. Cooperar con las autoridades extranjeras de protección de datos personales para el cumplimiento de sus competencias y generar mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse debido auxilio mutuo cuando se requiera.
3. Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.
4. Publicitar, a través del portal institucional, la relación actualizada de bancos de datos personales de administración pública y privada.
5. Promover campañas de difusión y promoción sobre la protección de datos personales.
6. Promover y fortalecer una cultura de protección de los datos personales de los niños y de los adolescentes.
7. Coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas.
8. Supervisar el cumplimiento de las exigencias previstas en esta Ley, para el flujo transfronterizo de datos personales.
9. Emitir autorizaciones, cuando corresponda, conforme al reglamento de esta Ley.
10. Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.
11. Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante.
12. Emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.
13. Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.
14. Celebrar convenios de cooperación interinstitucional o internacional con la finalidad de velar por los derechos de las personas en materia de protección de datos personales que son tratados dentro y fuera del territorio nacional.
15. Atender solicitudes de interés particular del administrado o general de la colectividad, así como solicitudes de información.
16. Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento.
17. Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.
18. En el marco de un procedimiento administrativo en curso, solicitado por la parte afectada, obtener de los titulares de los bancos de datos personales la información que estime necesaria para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones.
19. Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley.
20. Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.

Para el cumplimiento adecuado de las mismas, las Autoridades; y en específico la nuestra, deben gozar de autonomía e independencia necesarias.

Tener una estructura organizacional correspondiente a la importancia de las diversas funciones asignadas; contar con los recursos humanos, logísticos y económicos necesarios e idóneos, que le permitan también desarrollar estrategias para enfrentar los retos del uso de las variadas tecnologías utilizadas para el tratamiento de los datos personales tanto a nivel nacional como internacional.

La Autoridad debe contar con lo necesario para cumplir de manera adecuada su rol fiscalizador con el fin de asegurar el cumplimiento de las normas sobre la materia.

Sería importante que desarrolle un rol protagónico en la sociedad para difundir el conocimiento y la toma de conciencia del derecho a la protección de datos personales; así como de la legislación sobre la materia; que brinde el asesoramiento y aplique las sanciones cuando correspondan para garantizar de manera más efectiva el respeto y vigencia de la normatividad sobre protección de datos, entre otros retos.



La Autoridad de control debe fortalecerse y consolidarse como garante de la efectiva protección de los datos personales.

Creemos que existe un reto normativo que debe ser impulsado desde la Autoridad para fortalecer la legislación y actualizarla a la luz de legislaciones más garantistas y a los estándares internacionales sobre la materia; y en aras de caminar hacia una armonización, que permita una respuesta internacional o global a los problemas y riesgos del uso de la tecnología y del tratamiento internacional de los datos personales.

Dentro del reto de la actualización y fortalecimiento de nuestra normativa creemos que deben incorporarse varias instituciones que están recogidas en los estándares internacionales sobre la materia. Algunos derechos, como el de portabilidad de los datos personales[20]; algunos principios rectores como los de Lealtad, Transparencia y el de Responsabilidad Proactiva.

En la medida que la Responsabilidad Proactiva se da para y en función de los otros principios rectores, con el fin de ir más allá del cumplimiento formal

20 Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Red Iberoamericana de Protección de Datos. Punto 30. Derecho que ya se incluyó en el proyecto de Ley N° 7870/2020-PE, presentado por el Poder Ejecutivo.

de la normativa existente; es decir ir hacia un cumplimiento real y ético, que es parte del reto para los responsables y encargados del tratamiento al que hicimos mención en el acápite correspondiente, haremos referencia a este este principio.

Para un cumplimiento más efectivo de la normativa sobre protección de datos personales, estándares internacionales sobre la materia, tales como el Reglamento General de Protección de Datos, artículo 5.2; los Estándares de Protección de Datos Personales para los Estados Iberoamericanos-RIPD, artículo 20; y el Convenio para la protección de las personas con respecto al tratamiento de datos personales actualizado (Convenio 108 Plus), artículo 10.1; entre otros, reconocen el Principio de Responsabilidad o de Responsabilidad Proactiva.

El Grupo de Trabajo de Protección de Datos del Artículo 29, en su Dictamen 3/2010. P.3 sobre el principio de Responsabilidad señalaba: "(…) un principio reglamentario de responsabilidad requeriría expresamente que los responsables del tratamiento de datos aplicaran medidas adecuadas y eficaces para poner en práctica los principios y obligaciones de la Directiva y demostrar este extremo cuando se les solicitara".



Perú, no tiene incorporada a la Responsabilidad Proactiva dentro de los ocho principios rectores; no obstante, creemos que un aspecto fundamental del fortalecimiento normativo de la protección de datos sería la incorporación de este principio. La Responsabilidad proactiva supondrá una mayor implicación de los responsables y encargados del tratamiento en el cumplimiento normativo; y exigirá la implementación de medias apropiadas, efectivas y verificables que acrediten el real y correcto cumplimiento de la normatividad.

Dentro de las medidas apropiadas, efectivas y verificables que acreditarían un correcto cumplimiento de la normatividad sobre la protección de datos personales, se encuentran: los análisis de riesgos; las evaluaciones de impacto; la protección de datos desde el diseño y por defecto; el oficial de protección de datos; la notificación de incidentes de seguridad; la adhesión a códigos de conducta; los mecanismos de certificación.

## III. RETOS PARA LOS TITULARES DE LA INFORMACIÓN

La existencia de una normativa actualizada y reforzada sobre el derecho a la protección de datos personales, que vaya hacia una armonización a la luz de los estándares internacionales sobre la materia, es necesaria; que los responsables y encargados del tratamiento cumplan, de manera ética y demostrable, con la Ley y el Reglamento; también es necesario; pero no suficientes.

El tercer pilar para el debido tratamiento de los datos personales lo constituyen los titulares de la información.

Las personas naturales difunden cada día más información que les concierne y lo hacen a través de redes sociales; del uso del internet de las cosas; de las app; del comercio digital; de diversas plataformas tecnológicas; y de cada vez más variadas y modernas tecnologías que atienden necesidades y brindan facilidades; siendo que estas lo hacen con una apariencia de brindar esos servicios de forma gratuita; pero en la mayoría de los casos, esto no es así; pues se cobran con el uso de los datos personales de los usuarios.

El ceder el uso de nuestra información personal es mucho más valioso y riesgoso que pagar con nuestro dinero; pues, se van poniendo bajo el control de terceros, diversos aspectos la vida (personal y familiar) sobre los cuales en la práctica se suele perder el control.

Es imprescindible que se instaure y desarrolle la cultura de la protección de datos personales en nuestro país; donde los titulares de la información conozcan su derecho, tomen conciencia de la importancia y lo que significa el ceder el uso de su información personal; que estén en capacidad, por un lado, exigir el respeto hacia su información personal; pero, a la vez, que ellos también traten respetuosamente la información a la que acceden y que les concierne a terceras personas.



La era digital exige titulares de la información responsables a la hora en que gestionan su información personal; que actúen de manera informada y ejerzan los derechos que les corresponden para no por no perder el control sobre la información que les concierne.

Además de afrontar los retos que le corresponden a los responsables del tratamiento; así como, a la Autoridad de Control; lo cual redundará en un fortalecimiento de la cultura de protección de datos personales; creemos que sumaría a este objetivo, el incluirse al derecho a la protección de datos personales en el marco del cumplimiento de lo que dispone la Constitución Política de 1993 en el artículo 14 donde señala que "(…) la formación ética y cívica y la enseñanza de la Constitución y de los derechos humanos son obligatorias en todo el proceso educativo civil o militar (…)"; pues la protección de los datos personales es de suma importancia en la era digital en la que nos encontramos.

Lo señalado va en consonancia con una de las funciones que la Ley le asigna a la Autoridad Nacional de Protección de Datos Personales, en el artículo 33, inciso 7) "Coordinar la inclusión de información sobre la importancia de la vida

privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas."

En un Estado Constitucional de Derecho como el nuestro coexisten distintos derechos fundamentales e intereses constitucionalmente relevantes; por lo que el derecho a la protección de datos personales y las normas que regulan, lo que buscan es avanzar en esta era digital, a través de un equilibrio respetuoso entre los distintos intereses en juegos, tanto de los responsables del tratamiento como de los titulares de los datos personales, teniendo en cuenta que independientemente del contexto y de la tecnología que se utilice el respeto de la persona, sus derechos y dignidad deben perseverar.

## IV. CONCLUSIONES

- Los responsables del tratamiento deben observar y cumplir debidamente los principios rectores de la protección de datos personales a la hora de cada actividad de tratamiento, independientemente de la tecnología que usen y del sector donde operen sus organizaciones.



- Los responsables del tratamiento deben instaurar una cultura organizacional de la protección de datos personales, como política transversal y holística al interior de sus organizaciones.

- En la era digital, ya no basta el mero cumplimiento de la legislación sobre protección de datos personales; se requiere ir más allá; hacia un cumplimiento ético de la misma.

- Existe un reto normativo que debe ser impulsado desde la Autoridad para fortalecer la legislación y actualizarla a la luz de legislaciones más garantistas y a los estándares internacionales sobre la materia.

- Dentro de la necesaria actualización y fortalecimiento de nuestra normativa deben incorporarse varias instituciones que están recogidas en los estándares internacionales sobre la materia; tales como: el derecho de portabilidad de los datos personales; principios rectores como los de: Lealtad, Transparencia y el de Responsabilidad Proactiva.

- Es necesario que se instaure y desarrolle la Cultura de la Protección de Datos Personales en nuestro país; pues la era digital exige titulares de la información responsables a la hora en que gestionan su información personal;

que actúen de manera informada y ejerzan los derechos que les corresponden para no perder el control sobre la información que les concierne.

- Sería pertinente el incluir al derecho a la protección de datos personales en el marco del cumplimiento de lo que dispone la Constitución Política de 1993 en el artículo 14, donde señala que "(…) la formación ética y cívica y la enseñanza de la Constitución y de los derechos humanos son obligatorias en todo el proceso educativo civil o militar (…)"; pues la protección de los datos personales es de suma importancia en la era digital en la que nos encontramos.

## BIBLIOGRAFÍA

Consejo de Europa. (2012). *Convenio para la protección de las personas con respecto al tratamiento de datos personales*. (Convenio 108 Plus). 1680968478 (coe.int).

Red Iberoamericana de Protección de Datos. (2019). *Estándares de protección de datos personales para los Estados Iberoamericanos*.

Red Iberoamericana de Protección de Datos. (2019). *Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de inteligencia artificial*.

Unión Europea. (2010). *Grupo de Trabajo de Protección de Datos del Artículo 29*. Dictamen 3/2010. Sobre el principio de Responsabilidad.

Unión Europea. (2016). *Reglamento de la Unión Europea*. Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Zamudio Salinas, M. (2014). *La Ley de protección de datos personales peruana. Reflexiones comparativas. Régimen Jurídico de los datos personales*. T. II. Abeledo Perrot.

Zamudio Salinas, M. (2021). *El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del sistema de geolocalización GPS. Límites y propuestas*. Tesis para optar el grado académico de magíster en derecho con mención en Derecho Constitucional. PUCP.