La protección de datos personales en el Perú. ¿Un modelo de *compliance* funcional?

Alejandro Vargas*
Universidad CEU San Pablo, España

Recibido: 31 de marzo del 2025 / Aceptado: 10 de abril del 2025

doi: https://doi.org/10.26439/iusetpraxis2025.n060.7848

RESUMEN. La evolución normativa en materia de protección de datos personales en el Perú ha sido clave para consolidar estándares de privacidad y seguridad. Este artículo analiza cómo dicho desarrollo, desde la Ley de Protección de Datos Personales hasta las recientes modificaciones introducidas por su reglamento, configura lo que podría considerarse un programa de cumplimiento especializado. Se examinan los aspectos esenciales de la Ley y los cambios más relevantes del nuevo reglamento, orientados a transformar la cultura de cumplimiento y a elevar los estándares en el contexto global. Finalmente, se presentan los principales desafíos y oportunidades que este régimen plantea para la protección efectiva de los derechos fundamentales de los ciudadanos.

PALABRAS CLAVE: protección de datos personales / *corporate compliance* / programa de cumplimiento / principio de responsabilidad proactiva

* Magíster en Investigación en Ciencias Jurídicas por la Universidad CEU San Pablo. Gerente *senior* de servicios legales de KPMG en Perú.

PERSONAL DATA PROTECTION IN PERU: A FUNCTIONAL COMPLIANCE MODEL?

ABSTRACT. The regulatory evolution of personal data protection in Peru has been key to consolidating privacy and security standards. This article analyzes how this development—from the Personal Data Protection Law to the recent amendments introduced by its regulation—shapes what could be considered a specialized compliance program. It examines the essential aspects of the law and the most relevant changes in the new regulation, aimed at transforming the compliance culture and raising standards in the global context. Finally, it presents the main challenges and opportunities that this regime poses for the effective protection of citizens' fundamental rights.

KEYWORDS: personal data protection / corporate compliance / compliance program / accountability principle

1. INTRODUCCIÓN

En el Perú, la protección de datos personales ha emergido como un componente esencial dentro del *corporate compliance*. A pesar de que su régimen de cumplimiento no cuenta con una designación formal en nuestro ordenamiento jurídico (como programa, modelo o sistema, por ejemplo), hoy por hoy, tras la entrada en vigor del nuevo reglamento de la Ley de Protección de Datos Personales, sus características funcionales —obligaciones preventivas, controles internos, gestión de riesgos y mecanismos de supervisión— lo aproximan a lo que, en la práctica, constituiría un verdadero programa de cumplimiento normativo especializado.

Este artículo analiza la Ley de Protección de Datos Personales y las modificaciones introducidas por el nuevo reglamento, evidenciando cómo estas configurarían un régimen con atributos funcionales de un programa de cumplimiento normativo. El análisis busca evidenciar que la normativa no se limita a imponer obligaciones formales, sino que establece una estructura orientada a la prevención y la gestión de riesgos, con el objetivo de garantizar la protección efectiva de los derechos fundamentales de los ciudadanos.

2. CUESTIONES BÁSICAS: EL ABC QUE TODOS DEBEMOS CONOCER

La Ley 29733, Ley de Protección de Datos Personales (en adelante LPDP), entró en vigencia plena en mayo del 2015. No obstante, el régimen peruano en esta materia se sustenta en un conjunto de disposiciones que conforman la denominada normativa de protección de datos personales (en adelante normativa PDP)[1].

A más de una década de su vigencia, persiste un desconocimiento generalizado, tanto en el sector público como en el privado, sobre el contenido y alcance de la normativa. Esta situación genera una falta de protección adecuada de los derechos relacionados con los datos personales y del cumplimiento de las obligaciones que dicha protección exige.

Es fundamental iniciar este análisis explicando ciertos conceptos y aspectos básicos para comprender el régimen de protección de datos personales y su evolución a lo largo del tiempo, hasta llegar al reciente nuevo reglamento, aprobado por Decreto Supremo 016-2024-JUS (en adelante, el nuevo reglamento), que derogó el anterior y que entró en vigencia el 30 de marzo de este año.

1 Esta comprende normas como el Decreto Legislativo 1353 y su reglamento, aprobado mediante Decreto Supremo 019-2017-JUS; la Resolución Directoral 80-2019-JUS/DGTAIPD, que aprueba la Guía práctica para la observancia del deber de informar; el Decreto de Urgencia 07-2022; la Resolución Directoral 02-2020-JUS/DGTAIPD, que aprueba la Directiva para el tratamiento de datos personales mediante sistemas de videovigilancia; y la Resolución Directoral 023-2025-JUS/DGTAIP, que aprueba la Guía para el tratamiento de datos personales realizado por las juntas de propietarios y administradores.

2.1. ¿Qué son los datos personales?

El nuevo reglamento define a los datos personales como "aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables" (Decreto Supremo 016-2024-JUS, artículo III).

Por otro lado, la normativa reconoce una subespecie de datos personales, denominados datos sensibles, los cuales se definen como

> aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos 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 afiliación sindical, salud física o mental u otras análogas que afecten su intimidad. (Decreto Supremo 016-2024-JUS, artículo III)

2.2. ¿Quiénes son considerados titulares de datos personales?

Son, únicamente, las personas naturales. Esta categoría no discrimina a las personas naturales nacionales o extranjeras, ni entre mayores y menores de edad. De hecho, los menores de edad gozan de un nivel superior de protección en muchos casos, como en el tratamiento de sus datos personales en internet (Decreto Supremo 016-2024-JUS, capítulo IV, artículo 25).

2.3. ¿Qué derechos tienen los titulares de datos personales?

Partiendo del derecho fundamental a la protección de datos personales (reconocido en el numeral 6 del artículo 2[2] de la Constitución Política del Perú), los titulares tienen los denominados derechos ARCO (acceso, rectificación, cancelación y posición). Estos incluyen, principalmente, el derecho a ser informados sobre el tratamiento de sus datos, así como a acceder a ellos, rectificarlos, cancelarlos, oponerse a su uso y exigir que se procesen de manera objetiva.

Así, por el derecho a la información, el titular de los datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad del tratamiento de sus datos, los destinatarios, el banco de datos, el responsable, el carácter obligatorio de sus respuestas, la transferencia, el plazo de conservación, las decisiones automatizadas, los mecanismos para ejercer sus derechos, entre otros elementos.

2 Artículo 2, numeral 6: toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Este derecho constituye uno de los ejes prioritarios de interpretación y fiscalización por parte de la Autoridad Nacional de Protección de Datos Personales (en adelante ANPD) en cuanto a su interpretación y desarrollo. Existen numerosas opiniones consultivas al respecto e, inclusive, una *Guía práctica para la observancia del "Deber de informar"* (Ministerio de Justicia y Derechos Humanos, 2019), elaborada con el propósito de orientar de forma práctica y sencilla a los responsables del tratamiento de los datos personales sobre cómo dar cumplimiento al derecho-deber de información establecido en el artículo 18 de la LPDP.

Por otro lado, el derecho al acceso implica que el titular sea informado de manera clara, expresa, indubitable y con un lenguaje sencillo, sobre sus datos personales que son objeto de tratamiento. Esto incluye la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación, quién solicitó dicha recopilación, así como las transferencias realizadas o previstas de esos datos.

El derecho al acceso comprende también el derecho a la portabilidad de datos personales. Este derecho permite al titular solicitar sus datos personales, facilitados a un titular o responsable de banco de datos, en un formato estructurado, de uso común y lectura mecánica, para transmitirlos a otro responsable o titular de banco de datos personales. Esto aplica cuando el tratamiento se basa en el consentimiento, en una relación contractual en la que el titular del dato es parte, o cuando el tratamiento se realiza mediante medios automatizados.

El derecho a la portabilidad de datos ha sido recientemente reconocido en el nuevo reglamento. Sin embargo, hasta la fecha de elaboración de este documento, aún no existen opiniones consultivas de la ANPD que lo desarrollen. No obstante, dada la reciente inclusión de este derecho, resulta pertinente destacar lo señalado por Puccinelli (2017):

> La consagración normativa del derecho a la portabilidad de los datos personales es, por lejos, la novedad tecnológicamente más importante —tanto por su incidencia práctica como por su complejidad técnica— que están incorporando las legislaciones más recientes (afirmación que no niega la importancia de los también noveles principios de privacidad por diseño y por defecto, *accountability*, etcétera). Es cierto que por sus características no puede tener la operatividad plena y directa que caracteriza a los restantes derechos ARCO, y por ello queda un largo camino reglamentario por recorrer que no se vislumbra como sencillo, especialmente a la hora de establecer tanto los parámetros que caractericen los "formatos estructurados comúnmente utilizados" como las normas técnicas, modalidades y procedimientos para la transferencia y la debida protección de datos personales involucrados. (p. 228)

Mediante el derecho a la rectificación, el titular de datos personales puede solicitar la modificación de aquellos datos que sean inexactos, erróneos o falsos. Además, tiene también derecho a solicitar la actualización de los datos que hayan sido modificados

a la fecha del ejercicio del derecho. Asimismo, tiene derecho a solicitar la inclusión o incorporación de sus datos en un banco de datos personales, si considera que existe información faltante, incompleta, omitida o eliminada, y que sea necesaria para el tratamiento de sus datos.

El titular también tiene derecho a la supresión o cancelación de sus datos personales cuando estos hayan dejado de ser necesarios o pertinentes para la finalidad con la cual fueron recopilados, cuando haya vencido el plazo establecido para su tratamiento, cuando haya revocado su consentimiento para el tratamiento, y en los demás casos en los que no estén siendo tratados conforme a la LPDP y al nuevo reglamento. Sin perjuicio de ello, el ejercicio de este derecho se encuentra restringido cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas, de acuerdo con la legislación aplicable, o en las relaciones contractuales entre el responsable y el titular de los datos personales que justifiquen su tratamiento.

El derecho de oposición permite al titular de los datos personales oponerse en cualquier momento al tratamiento de sus datos personales o solicitar su cese, cuando no haya prestado su consentimiento para su recopilación. Incluso si lo hubiera hecho, el titular tiene derecho a oponerse al tratamiento de sus datos si acredita la existencia de motivos fundados y legítimos relacionados con una situación personal concreta que justifique el ejercicio de este derecho.

Por otro lado, a través del derecho al tratamiento objetivo, el titular de los datos personales tiene derecho a no ser objeto de decisiones, automatizadas o no, que le produzcan efectos jurídicos, discriminación o le afecten de manera significativa. Esto incluye aquellas decisiones basadas únicamente en tratamientos automatizados destinados a evaluar, analizar o predecir, sin intervención humana, determinados aspectos personales, como su rendimiento profesional, situación económica, estado de salud, orientación o identidad sexual, fiabilidad o comportamiento, entre otros. Este derecho se exceptúa, por ejemplo, en el marco de la negociación, celebración o ejecución de un contrato, o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo con la Ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.

Finalmente, se reconoce el derecho a la tutela, mediante el cual el titular puede recurrir a la ANPD o al Poder Judicial en caso de que el titular o el encargado del banco de datos personales deniegue, total o parcialmente, el ejercicio de los derechos ARCO. Además, el titular tiene derecho a ser indemnizado en caso de verse afectado por el incumplimiento de las obligaciones establecidas en la normativa PDP.

2.4. ¿Qué se entiende por tratamiento de datos personales?

Es cualquier operación o conjunto de operaciones, automatizadas o no, que se realicen sobre los datos personales o conjuntos de datos personales. El tratamiento de datos personales comprende la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia, difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

2.5. ¿Qué es un banco de datos personales?

Es el conjunto organizado de datos de personas naturales, computarizado o no, y estructurado conforme a criterios específicos, que permite acceder sin esfuerzos desproporcionados a los datos personales, ya sea que el banco esté centralizado, descentralizado o repartido de forma funcional o geográfica. Los bancos de datos personales no se restringen a un soporte específico, pues pueden encontrarse en soporte físico, magnético, digital, óptico u otro.

2.6. ¿A quiénes aplica la LPDP y su reglamento?

La normativa resulta aplicable a las personas naturales, entidades públicas o instituciones del sector privado que realicen tratamiento de datos personales, considerando los supuestos de excepción previstos en el artículo 3 de la LPDP y en el artículo V del nuevo reglamento. De acuerdo con ello, la normativa reconoce tres sujetos (obligados) que pueden participar en el tratamiento de los datos personales:

- El titular del banco de datos personales es la persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, su tratamiento y las medidas de seguridad.
- El responsable del tratamiento es la persona natural, persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y medios del tratamiento de datos personales. El responsable no necesariamente es el titular del banco de datos, puede ser cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se encuentre en un banco de datos personales.
- El encargado del tratamiento de datos personales es la persona natural, persona jurídica o entidad pública que realiza el tratamiento de datos por cuenta u orden del responsable del tratamiento o del titular del banco de datos personales.

Finalmente, es importante señalar que la norma no tiene una restricción territorial para su aplicación; comprende, inclusive, a sujetos no establecidos dentro del territorio peruano, conforme lo indica el artículo VI del nuevo reglamento.

2.7. ¿Cuáles son las principales obligaciones en materia de protección de datos personales?

Los sujetos mencionados deben cumplir con ciertas obligaciones previstas en la normativa PDP para garantizar el tratamiento adecuado de los datos personales. Así, el titular de los bancos de datos o el responsable del tratamiento deben cumplir, entre otras, con la obligación de inscribir sus bancos de datos ante el Registro Nacional de Protección de Datos Personales, informar a la ANPD sobre la realización de flujo transfronterizo de datos personales, atender los pedidos de tutela que formulen los titulares de datos personales sobre los derechos ARCO, cumplir con el deber de confidencialidad, cumplir con el derecho-deber de informar, obtener el consentimiento de manera previa al tratamiento, cuando corresponda, implementar las medidas de seguridad necesarias para garantizar la protección de los datos personales, designar un representante en el territorio peruano o para el territorio peruano, notificar a la autoridad y registrar incidentes de seguridad, contar con un documento de seguridad, designar, cuando corresponda, a un oficial de datos personales, elaborar un código de conducta (voluntario), y realizar una evaluación del impacto relativo a la protección de datos personales (voluntario).

Habiendo desarrollado los conceptos y aspectos básicos de la normativa PDP, es pertinente abordar las principales modificaciones al régimen de protección de datos personales introducidas por el nuevo reglamento.

3. EL CAMBIO DE *MINDSET*: EL NUEVO REGLAMENTO

El nuevo reglamento entró en vigencia el 30 de marzo del 2025, e introdujo nuevas disposiciones que refuerzan significativamente el régimen de protección de datos personales en el Perú. Estas modificaciones nos acercan a estándares de protección más elevados, como los desarrollados en la Unión Europea. Por ello, es necesario abordar los principales cambios incorporados en este documento.

3.1. Nuevos principios rectores

Se desarrollan dos nuevos principios rectores:

– El principio de transparencia implica que el tratamiento de datos personales debe ser comunicado de manera permanente, clara, fácil de entender y accesible al titular de datos personales. Se debe informar las condiciones del tratamiento y sus derechos.

– El principio de responsabilidad proactiva implica que el tratamiento de datos debe incluir medidas legales, técnicas y organizativas para cumplir efectivamente la normativa, y que el titular del banco de datos personales —o quien resulte responsable— debe demostrar el cumplimiento.

El principio de responsabilidad proactiva, también llamado *accountability,* ha sido recién introducido en nuestro ordenamiento por el nuevo reglamento[3]. Este principio es fundamental para el cambio de enfoque que se busca en el cumplimiento de las obligaciones en materia de protección de datos personales.

El término *accountability* proviene del mundo anglosajón y, a pesar de las diferentes acepciones que pueda tener, en la arena de la protección de datos se refiere al modo en el que una organización debe cumplir en la práctica las regulaciones sobre la materia y a la manera en la que debe demostrar que lo hecho es útil, pertinente y eficiente (Remolina Angarita & Álvarez Zuluaga, 2018).

Por otro lado, esta actitud proactiva se podría resumir en la frase que ha popularizado la Agencia Española de Protección de Datos, según la cual "no incumplir ya no será suficiente" (Estepa Montero, 2022, p. 72). Se trata, más bien, de asegurar un compromiso elevado de cumplimiento que permita garantizar el necesario respeto a los derechos de los particulares, a la vez que facilitar el incremento incesante del flujo de datos que circula entre los entes públicos, las corporaciones y los particulares.

3.2. Nuevas obligaciones

Se desarrollan nuevas obligaciones para los titulares de los bancos de datos personales y los responsables del tratamiento:

– Notificación de incidentes de seguridad. Se incorpora la obligación de notificar a la ANPD los incidentes de seguridad que afecten a los titulares de datos personales dentro de las 48 horas posteriores de conocerlos o constatarlos. Dentro de la notificación se debe informar la naturaleza del incidente; el nombre y los datos del oficial de datos personales u otro contacto; las posibles consecuencias del incidente; las medidas adoptadas o propuestas para poner remedio a la violación de seguridad e incluso, si corresponde, las medidas adoptadas para mitigar los posibles efectos negativos.

  A su vez, se establece que en caso el titular del banco de datos o el responsable del tratamiento adviertan que el incidente de seguridad de datos personales afecta al titular de estos en otros de sus derechos, deben comunicarlo al propio titular, dentro de las 48 horas, sin dilación indebida, en un lenguaje sencillo y claro para su comprensión, junto con las medidas adoptadas para mitigar sus efectos.

3 Sin embargo, este principio es reconocido internacionalmente desde hace mucho tiempo, y ha sido desarrollado en diversas normativas, como en el *Reglamento General de Protección de Datos* de la Unión Europea.

Es importante considerar que esta obligación, al igual que otras previstas en el nuevo reglamento, presenta vacíos que dificultan su aplicación óptima. Por ejemplo, no existe una definición precisa sobre qué constituye la "exposición de grandes volúmenes de datos personales" o "la afectación a un gran número de personas". Esta falta de claridad obliga a los titulares de bancos de datos personales a interpretar la norma para determinar si se encuentran ante un incidente de seguridad que deba ser notificado[4].

– Evaluación del impacto relativo a la protección de datos personales. Aunque es facultativa, el nuevo reglamento recomienda su realización[5] ante supuestos como el tratamiento de datos sensibles, de datos con fines para crear perfiles, el tratamiento de grandes volúmenes de datos, entre otros. La evaluación de impacto se puede elaborar tomando como referencia la guía, lineamientos y procedimientos establecidos en las normas técnicas peruanas sobre seguridad de la información y gestión de riesgos en su edición vigente (NTP-ISO/IEC 27005 y NTP-ISO 31000, respectivamente) u otros estándares relacionados con el análisis y la evaluación de riesgos para la protección de datos personales. Contar con una evaluación de impacto implementada de manera previa al inicio de un procedimiento administrativo sancionador es considerado un atenuante de responsabilidad sobre el tratamiento cuestionado.

– Designación de representante. El titular del banco de datos personales o quien resulte responsable del tratamiento y que no se encuentre establecido en territorio peruano debe proveer los medios necesarios para el cumplimiento de sus obligaciones y designar un representante en el territorio peruano, o para el territorio peruano, quien será el punto de contacto con la ANPD. La designación del representante puede realizarse de manera pública, a través de su inclusión en la política de privacidad, o comunicándola directamente a la ANPD.

– Implementación de procedimiento de disociación[6]. El titular del banco de datos o el responsable del tratamiento debe seleccionar la técnica adecuada para realizar el procedimiento de disociación, considerando siempre el tipo de datos objeto de

4 A la fecha de elaboración de este artículo, la ANPD no se ha pronunciado sobre este vacío normativo, que sí es recogido por otras jurisdicciones como, por ejemplo, en la Unión Europea, con el *Reglamento General de Datos* y las directrices 9/2022 sobre la notificación de violaciones de la seguridad de los datos personales.

5 En la Unión Europea, la evaluación de impacto relativa a la protección de datos personales es obligatoria cuando el tratamiento de datos pueda entrañar un alto riesgo para los derechos y libertades de las personas, requiriéndose en algunos casos la evaluación sistemática y exhaustiva de aspectos personales, el tratamiento a gran escala de datos sensibles y la observación sistemática a gran escala en zonas públicas.

6 Es el procedimiento que impide la identificación del titular de los datos personales; sin embargo, este procedimiento es reversible.

tratamiento, el número de titulares de datos, el factor de riesgo (gravedad, probabilidad, consecuencias para el responsable y el titular) y los que la ANPD determine para tal efecto.

– Contar con un documento de seguridad. El responsable del tratamiento debe elaborar un documento de seguridad, el cual debe ser aprobado formalmente y contar con fecha cierta. Este documento debe estar actualizado y contener, como mínimo, los procedimientos de gestión de accesos, la gestión de privilegios y la verificación periódica de privilegios asignados para los sistemas de información utilizados en el tratamiento de datos personales.

  El documento de seguridad puede ser elaborado utilizando como referencia los lineamientos, requisitos y controles de la NTP-ISO/IEC 27001 vigente u otros estándares reconocidos en el sector. Además, este debe incluir políticas para la gestión y tratamiento de datos personales, que abarquen su obtención, uso y posterior supresión, y contener un inventario de los datos personales y los sistemas utilizados, que especifique si se trata de datos sensibles.

– Contar con un código de conducta[7]. Es un mecanismo de responsabilidad proactiva que permite demostrar el cumplimiento de las obligaciones establecidas en la LPDP y el nuevo reglamento para el tratamiento de datos personales. Aunque su implementación es voluntaria, tener uno antes del inicio de un procedimiento administrativo sancionador se considera como un atenuante de responsabilidad. Los códigos de conducta deben redactarse en términos claros y accesibles, y deben incluir al menos los once aspectos regulados en el artículo 60 (capítulo VII) del nuevo reglamento.

– Designación de un oficial de datos personales. El titular del banco de datos o responsable y el encargado de tratamiento deben designar a un oficial de datos personales en los siguientes casos: cuando el tratamiento sea realizado por una entidad pública; cuando se traten grandes volúmenes de datos personales (en cantidad, tipo de datos, o que puedan afectar a un gran número de personas); y cuando las actividades principales o de giro de negocios incluyan el tratamiento de datos sensibles.

  El oficial de datos personales debe ser designado en función de sus cualificaciones profesionales, especialmente su conocimiento y experiencia acreditada en materia de protección de datos personales. Este cargo puede ser asumido por una persona interna o externa a la organización, sin necesidad de dedicación exclusiva, siempre

7 En la Unión Europea, los códigos de conducta en materia de protección de datos personales son instrumentos de autorregulación voluntaria que permiten a sectores específicos adaptar y aplicar el *Reglamento General de Protección de Datos*, debiendo ser aprobados por la autoridad de control competente de cada país miembro.

que cuente con la capacidad técnica para ejercer sus funciones. Entre estas se incluyen: informar y asesorar a los responsables y al personal sobre sus obligaciones legales; verificar el cumplimiento de la normativa y de las políticas internas, lo que incluye la formación del personal y la realización de auditorías, y cooperar con la ANPD, actuando como punto de contacto institucional en todo lo relacionado con el tratamiento de datos personales. Además, debe desempeñar sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento y considerando su naturaleza, alcance, contexto y finalidad.

Consideramos que la regulación del oficial de protección de datos incluida en el nuevo reglamento resulta insuficiente, lo cual genera vacíos normativos que deben ser abordados por la ANPD. En particular, se requiere mayor claridad con respecto a la obligación de designación en casos de tratamientos que impliquen una observación habitual, sistemática y continua de datos personales a gran escala, pues actualmente no existe una definición normativa precisa de qué se entiende por "grandes volúmenes de datos"[8], lo que dificulta su aplicación práctica. Asimismo, es necesario establecer lineamientos funcionales que aseguren el ejercicio efectivo del cargo, garanticen su autonomía e independencia, prevengan conflictos de interés, y obliguen a la alta dirección a asumir seriamente el rol del oficial como figura clave en el cumplimiento normativo[9].

3.3. Otras incorporaciones

Además de lo mencionado, el nuevo reglamento incorpora nuevas disposiciones relacionadas al tratamiento de datos personales para publicidad y prospección comercial, al tratamiento de datos personales de niños, niñas y adolescentes en internet, nuevos elementos en la comunicación de consentimiento informado, nuevas medidas y controles de seguridad. Asimismo, se desarrollan el derecho a la portabilidad de datos personales, los requisitos para determinar si un país cuenta con un nivel adecuado de protección de datos en caso de flujo transfronterizo, la fiscalización en gabinete como nueva modalidad de fiscalización, nuevas atenuantes de responsabilidad, nuevas medidas correctivas e infracciones, entre otros.

8 El concepto de "grandes volúmenes de datos", que no ha sido desarrollado o explicado en el Perú, puede equipararse al de tratamiento a "gran escala" desarrollado por la Unión Europea. Esto brinda criterios para su aplicación, como los que desarrolló el Grupo de Trabajo del artículo 29 del RGDP (GT29), cuya postura mantiene el Comité Europeo de Protección de Datos.

9 Otras jurisdicciones han abordado este tema con mayor profundidad. Por ejemplo, la Ley Orgánica 3/2018 de España y el *Reglamento del Delegado de Protección de Datos Personales* del Ecuador han desarrollado marcos normativos más robustos, que fortalecen la figura del oficial (o delegado) de protección de datos, dotándolo de mayores garantías para el cumplimiento efectivo de sus funciones.

4. EL *COMPLIANCE* Y LA PROTECCIÓN DE DATOS PERSONALES

La normativa peruana reconoce distintos programas de cumplimiento, dentro de los cuales se encuentran[10], por ejemplo, el Sistema de Prevención de Lavado de Activos y Financiamiento del Terrorismo (SPLAFT), el Modelo de Prevención de Delitos, el Programa de Cumplimiento de las Normas de Libre Competencia y el Programa de Cumplimiento Normativo en Materia de Protección al Consumidor y Publicidad Comercial.

Todos estos programas (o la mayoría)[11] comparten elementos que, a nivel doctrinario y normativo, son reconocidos como esenciales[12] para la composición de un programa de cumplimiento. Así, por ejemplo, la *Guía de Programas de Cumplimiento de las Normas de Libre Competencia* (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 2021) ha reconocido los siguientes elementos comunes a todos los programas de cumplimiento:

1. Compromiso real de cumplimiento por parte de la alta dirección
2. Identificación y gestión de riesgos, tanto actuales como potenciales
3. Procedimientos y protocolos internos
4. Capacitación para los trabajadores
5. Actualización constante y monitoreo del programa de cumplimiento
6. Auditorías al programa de cumplimiento
7. Procedimientos para consultas y denuncias
8. Designación de un oficial o comité de cumplimiento

Al respecto, aunque existen regulaciones que desarrollan estos elementos, es importante tener en consideración que un programa de cumplimiento no se limita a lo que dictan las normas, guías o lineamientos emitidos por el Estado, sino que va más allá. Un programa de cumplimiento

10 Adicionalmente, se reconocen otros programas de cumplimiento sectoriales, como el de gobierno corporativo y gestión integral de riesgos para entidades supervisadas por la Superintendencia de Banca, Seguros y AFP (SBS) (Resolución SBS 272-2017), gestión de riesgos de lavado de activos y financiamiento del terrorismo (LA/FT) para entidades supervisadas por la SBS (Resolución SBS 26602015), prevención de LA/FT de entidades reguladas por la Superintendencia del Mercado de Valores (SMV) (Resolución 033-2011-EF/94.01.1), entre otras.

11 El SPLAFT, el Modelo de Prevención de Delitos y el Programa de Cumplimiento de las Normas de Libre Competencia requieren la designación de un oficial o encargado del programa, mientras que el Programa de Cumplimiento Normativo en Materia de Protección al Consumidor y Publicidad Comercial no recomienda expresamente tal designación.

12 Además de los señalados, algunos también reconocen la designación de recursos (ISO 19600) y el sistema disciplinario (*Evaluation of Corporate Compliance Programs*, del Departamento de Justicia de Estados Unidos) como elementos del *compliance*.

> es un conjunto de normas internas, procesos, procedimientos, buenas prácticas y políticas que las empresas implementan, en el ejercicio de su autorregulación, para identificar, evaluar y mitigar los riesgos legales asociados a las actividades económicas que realizan, contribuyendo así al desarrollo de una cultura de cumplimiento en el interior de las organizaciones. (Torres Robles et al., 2021, p. 8)

Asimismo, con relación al ejercicio de autorregulación, Bacigalupo (2021) menciona que

> el *compliance* surge y se utiliza en el contexto del "marco de autorregulación" y de la libertad para decidir la organización interna de las sociedades mercantiles de Derecho privado orientada a la prevención de los riesgos provenientes de su actividad empresarial. (p. 265)

Corresponde analizar si la normativa PDP incorpora los elementos esenciales —o los deriva a lo referido en las Normas Técnicas (NTP-ISO) señaladas en el nuevo reglamento— para poder desarrollar un programa de cumplimiento. En tal sentido, a continuación detallaremos algunos supuestos contenidos en el nuevo reglamento (y las NTP-ISO en él referidas) que nos llevarán a determinar la existencia —o no— de un programa de cumplimiento en materia de protección de datos personales (ver la Tabla 1).

Tabla 1

Elementos del programa de cumplimiento en protección de datos personales

Elemento	¿Cómo se manifiesta en el nuevo reglamento?
Compromiso real de cumplimiento por parte de la alta dirección	Aunque la LPDP y el nuevo reglamento no especifican explícitamente la participación de la alta dirección en el cumplimiento de las obligaciones de protección de datos personales, existen varias obligaciones que implicarían su participación: 1. Mediante la aprobación formal del documento de seguridad (capítulo VI, artículo 47 del nuevo reglamento), que puede elaborarse tomando como referencia la NTP-ISO/IEC 27001, la cual resalta la responsabilidad de la gerencia a través de su compromiso evidenciado con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del Sistema de gestión de seguridad de la información. 2. Mediante la realización de la evaluación del impacto relativo a la protección de datos personales, pues se señala que esta puede elaborarse tomando como referencia la guía, lineamientos y procedimientos establecidos en la NTP-ISO/IEC 27005 y la NTP-ISO 31000 (capítulo V, artículo 40 del nuevo reglamento). Esta última NTP-ISO señala que la alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización y deberían demostrar liderazgo y compromiso. 3. Mediante la designación del representante (artículo VI del nuevo reglamento). Si bien no se señala que la alta dirección debe nombrar a dicho representante, su nombramiento debería realizarse a través de los mecanismos internos apropiados (por ejemplo, sesión de directorio u órgano análogo), debiéndose otorgarle las facultades suficientes para el ejercicio de la representación. 4. Mediante la designación del oficial de datos personales (capítulo V, artículo 38 del nuevo reglamento). Si bien no se señala que la alta dirección debe nombrar a la persona que ejercerá dicho cargo, su nombramiento debería realizarse a través de los mecanismos internos (por ejemplo, sesión de directorio, junta general de accionistas u otro órgano facultado), debiéndose otorgarle las facultades suficientes para el ejercicio de la representación. 5. Mediante la aprobación del código de conducta (capítulo VII, artículo 60 del nuevo reglamento), documento que debería ser aprobado por la alta dirección, como ocurre en otros programas de cumplimiento.
Identificación y gestión de riesgos[13], tanto actuales como potenciales	1. Mediante la solicitud a la ANPD para la emisión de una opinión sobre si el flujo de datos transfronterizo cumple o no con lo establecido en la LPDP y el nuevo reglamento (capítulo III, artículo 21 del nuevo reglamento). 2. Mediante el ejercicio de las funciones del oficial de datos personales, el cual debe prestar especial atención a los riesgos asociados a las operaciones de tratamiento de datos personales, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines de tal tratamiento (capítulo V, artículo 39.2 del nuevo reglamento). 3. Mediante la realización de la evaluación del impacto relativo a la protección de datos personales, que puede elaborarse tomando como referencia la guía, lineamientos y procedimientos establecidos en la NTP-ISO/IEC 27005 y la NTP-ISO 31000 en su edición vigente u otros estándares relacionados con el análisis y la evaluación de riesgos para la protección de datos personales (capítulo V, artículo 40 del nuevo reglamento). 4. Mediante la elaboración del documento de seguridad, que debe encontrase siempre actualizado y puede elaborarse tomando como referencia la NTP-ISO/IEC 27001 (capítulo VI, artículo 47 del nuevo reglamento), la cual considera, por ejemplo, la realización de un informe de evaluación de riesgos y un plan de tratamiento del riesgo.

(*continúa*)

13 Inclusive, la Agencia Española de Protección de Datos elaboró una guía para la gestión de riesgos y evaluación de impacto en tratamiento de datos personales, en la que se desarrollan varios aspectos relacionados a la gestión de riesgos derivados del tratamiento de este tipo de datos.

(*continuación*)

Elemento	¿Cómo se manifiesta en el nuevo reglamento?
Procedimientos y protocolos internos	1. Mediante la documentación de incidentes de seguridad (capítulo V, artículo 35 del nuevo reglamento). 2. Mediante la implementación de medidas de seguridad (capítulo VI del nuevo reglamento). 3. Mediante la elaboración del documento de seguridad, el cual debe contener políticas internas para la gestión y el tratamiento de los datos personales que tomen en cuenta el contexto y el ciclo de vida de los datos personales (capítulo VI, artículo 47 del nuevo reglamento). 4. Mediante la elaboración del código de conducta (capítulo VII, artículo 60 del nuevo reglamento), el cual debe desarrollar los procedimientos que faciliten el ejercicio de los derechos ARCO.
Capacitación para los trabajadores	1. Mediante la función del oficial de datos personales de informar y asesorar al titular del banco de datos personales o al responsable del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales respecto de las obligaciones de la LPDP (capítulo V, artículo 39.1.1 del nuevo reglamento). 2. Mediante la función del oficial de datos personales de sensibilizar y formar al personal (capítulo V, artículo 39.1.2 del nuevo reglamento). 3. Mediante la elaboración del documento de seguridad, respecto del cual se señala que el responsable de su elaboración debe determinar las medidas necesarias para que el personal conozca adecuadamente las consecuencias de su incumplimiento y aplique las medidas de seguridad necesarias para su sustento (capítulo VI, artículo 47 del nuevo reglamento). Asimismo, la NTP-ISO/IEC 27001, que puede ser tomada en consideración para la elaboración del documento se seguridad, señala que todo el personal al que se le asigna responsabilidad debe encontrase capacitado. 4. Mediante la elaboración del código de conducta (capítulo VII, artículo 60 del nuevo reglamento), el cual debe contener las acciones de fomento y difusión en materia de protección de datos personales dirigidas a quienes los traten.
Actualización constante y monitoreo del programa de cumplimiento	1. Mediante la elaboración del documento de seguridad, respecto del cual se menciona que debe encontrase actualizado, y que puede elaborarse tomando como referencia la NTP-ISO/IEC 27001 (capítulo VI, artículo 47 del nuevo reglamento), la cual prevé la realización de procedimientos de monitoreo. 2. Mediante el monitoreo y revisión periódica de las medidas de seguridad (capítulo VI, artículo 46 del nuevo reglamento).
Auditorías al programa de cumplimiento	1. Mediante la elaboración del documento de seguridad, respecto del cual se menciona que debe encontrase actualizado, y que puede elaborarse tomando como referencia la NTP-ISO/IEC 27001 (capítulo VI, artículo 47 del nuevo reglamento), la cual prevé la realización de auditorías internas en intervalos planificados. 2. Mediante la función del oficial de datos personales de verificar e informar sobre el cumplimiento de las autorías que se realicen en materia de protección de datos personales (capítulo V, artículo 39.1.2 del nuevo reglamento).
Procedimientos para consultas y denuncias	1. Mediante el procedimiento establecido para el ejercicio de los derechos ARCO (título II, capítulo I del nuevo reglamento). 2. Mediante la función del oficial de datos personales de informar y asesorar al titular del banco de datos personales o al responsable del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales respecto de las obligaciones que les incumben (capítulo V, artículo 39.1 del nuevo reglamento).

(*continúa*)

(*continuación*)

Autorregulación	Normativa de protección de datos personales
Designación de un oficial de cumplimiento	Mediante la designación del oficial de datos personales (capítulo V, artículo 37 del nuevo reglamento).
Ejercicio de autorregulación	1. Mediante la aplicación del principio de responsabilidad proactiva[14] (artículo IX del nuevo reglamento). 2. Mediante la elaboración del código de conducta (capítulo VII, artículo 60 del nuevo reglamento). 3. Mediante la realización de la evaluación del impacto relativo a la protección de datos personales (capítulo V, artículo 40 del nuevo reglamento).

De esta manera, aunque el régimen de cumplimiento de la normativa PDP no cuenta con una denominación formalmente asignada —como ocurre con otros programas reconocidos por ley—, su cumplimiento exige la implementación de normas internas, procesos, procedimientos, buenas prácticas y políticas que derivan directamente de la LPDP y su reglamento, así como del ejercicio de autorregulación empresarial impulsado por el principio de responsabilidad proactiva. El análisis de las disposiciones del nuevo reglamento evidencia que este régimen reúne todos los elementos esenciales para estructurar un programa de cumplimiento, incluyendo la identificación de riesgos, la adopción de medidas preventivas y correctivas, y el monitoreo continuo para garantizar la protección efectiva de los datos personales.

En consecuencia, más allá del nombre que se le asigne —sistema, modelo o programa de cumplimiento—, el nuevo reglamento introduce un cambio de enfoque que transforma la gestión de los datos personales y configura un régimen especializado. La incorporación del principio de responsabilidad proactiva, junto con obligaciones estructurales —como la elaboración del documento de seguridad y la designación del oficial de datos personales—, exige una gestión integral del riesgo legal. A ello se suman mecanismos voluntarios como los códigos de conducta y las evaluaciones de impacto, así como la referencia a estándares internacionales (NTP-ISO/IEC 27001, 27005 y 31000), que refuerzan el carácter técnico y preventivo del régimen, alejándolo de un enfoque meramente sancionador y alineándolo con los estándares globales de *corporate compliance*.

Si bien el nuevo reglamento representa un avance hacia la consolidación de este modelo, aún requiere ajustes para su implementación efectiva. Es necesario definir con precisión qué se entiende por "tratamiento de grandes volúmenes de datos", establecer criterios técnicos claros y fortalecer el marco funcional del oficial de datos personales,

14 El *Reglamento General de Protección de Datos* de la UE describe este principio (llamado también *accountability*) como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento es conforme con el *Reglamento*.

garantizando su independencia y rol estratégico. Asimismo, el legislador y la ANPD deben observar críticamente la evolución normativa internacional, especialmente el *Reglamento General de Protección de Datos* de la Unión Europea, que ha consolidado un modelo exigente y maduro.

Finalmente, la consolidación del régimen exige que la ANPD evolucione hacia un rol institucional más estratégico, orientado al desarrollo normativo, técnico y metodológico del cumplimiento. En ese marco, se identifican al menos tres líneas de acción prioritarias que podrían fortalecer su capacidad regulatoria y operativa: (i) la emisión de guías técnicas vinculantes sobre conceptos clave como "grandes volúmenes de datos", "riesgo alto" o "medidas de seguridad adecuadas"; (ii) el establecimiento de criterios interpretativos oficiales y metodologías de evaluación de riesgos que permitan aplicar el principio de responsabilidad proactiva de forma verificable; y (iii) la implementación de un sistema nacional de indicadores de cumplimiento, que permita monitorear la adecuación normativa, identificar brechas estructurales y orientar políticas públicas basadas en evidencia, siguiendo modelos como los del Comité Europeo de Protección de Datos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en México y la Agencia Española de Protección de Datos en España. Paralelamente, las organizaciones deben asumir un rol activo en la implementación del régimen, adoptar un enfoque basado en riesgos, fortalecer la gobernanza interna mediante la designación de oficiales de datos personales con autonomía funcional, y documentar sus medidas de cumplimiento a través de políticas, protocolos, registros y mecanismos de formación continua. Estas acciones, articuladas desde la regulación y la práctica, permitirán consolidar un modelo de cumplimiento efectivo, verificable y alineado con los estándares internacionales.

5. CONCLUSIONES

El nuevo reglamento de la LPDP marca un hito en la evolución del *corporate compliance*, lo que promueve un cambio de mentalidad hacia un enfoque preventivo y proactivo. La incorporación del principio de responsabilidad proactiva, junto con nuevas obligaciones, definiciones y referencias a estándares internacionales, refuerza la necesidad de implementar programas de cumplimiento robustos y adaptados a las exigencias actuales.

Este cambio normativo no solo busca alinear al Perú con los estándares más exigentes, como el RGPD, sino que configura un programa de cumplimiento normativo especializado, cuya implementación exige que las organizaciones integren la protección de datos en su sistema de gobierno corporativo mediante políticas, procesos y controles orientados a prevenir riesgos, garantizar derechos y demostrar cumplimiento. Este enfoque redefine el cumplimiento legal e impacta directamente en la gestión reputacional, contractual y operativa, posicionando la protección de datos como un eje transversal del gobierno corporativo.

REFERENCIAS

Bacigalupo, S. (2021). Compliance. *Eunomía. Revista en Cultura de la Legalidad*, (21), 260-276. https://doi.org/10.20318/eunomia.2021.6348

Decreto Supremo 016-2024-JUS. Reglamento de la Ley de Protección de Datos Personales. 30 de noviembre del 2024. Diario Oficial El Peruano. https://www.gob.pe/institucion/smv/normas-legales/6426760-016-2024-jus

Estepa Montero, M. (2022). El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas. *Anuario Jurídico y Económico Escurialense*, (55), 67-90. https://dialnet.unirioja.es/descarga/articulo/8244518.pdf

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2021). *Guía de Programas de Cumplimiento de las Normas de Libre Competencia*. https://www.gob.pe/institucion/indecopi/informes-publicaciones/2115530-guia-de-programas-de-cumplimiento-de-las-normas-de-libre-competencia

Ministerio de Justicia y Derechos Humanos (2019). *Guía práctica para la observancia del "Deber de informar"*. https://www.gob.pe/institucion/minjus/informes-publicaciones/353793-guia-practica-para-la-observancia-del-deber-de-informar

Puccinelli, O. R. (2017). El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances. *Pensamiento Constitucional*, *22*(22), 203-228. https://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/view/19945

Remolina Angarita, N., & Álvarez Zuluaga, L. F. (2018). *Guía GECTI para la implementación del principio de responsabilidad demostrada* —accountability— *en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos.* Universidad de los Andes; Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI).

Torres Robles, M., Calderón, L., Echeandia, D., Molina, P. X., Flores, V., Fernández, C. J., Durán, J. R., Serrano, T., Macein, I., Ávila, A., Samayoa Estrada, J., Letzkus Palavecino, M., Abarca, C. A., & Vicens, A. (2021). *Estructura de un Programa de Compliance*. World Compliance Association. https://bibliotecacompliance.com/wp-content/uploads/2021/03/fasc.2_ESTRUCTURA-DE-UN-PROGRAMA-DE-COMPLIANCE_V5.pdf