# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

# FACULTAD DE DERECHO


Programa de Segunda Especialidad en Derecho Administrativo

El marco de responsabilidad proactiva del Nuevo Reglamento de Protección de Datos Personales

Trabajo académico para optar el título de Segunda Especialidad en Derecho Administrativo

Autor:
Alonso Armando Moreno Alvarez

Asesor:
Dr. Diego Hernando Zegarra Valdivia

Lima, 2025

**Informe de Similitud**

Yo, DIEGO HERNANDO ZEGARRA VALDIVIA, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo Académico titulado “El marco de responsabilidad proactiva del Nuevo Reglamento de Protección de Datos Personales”, del autor(a) ALONSO ARMANDO MORENO ALVAREZ, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 28%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 07/12/2025.

- He revisado con detalle dicho reporte y el Trabajo Académico, y no se advierten indicios de plagio.

- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lima, 11 de diciembre del 2025

<table>
<tr><td colspan="2">DIEGO HERNANDO ZEGARRA VALDIVIA</td></tr>
<tr><td>DNI: 07875295</td><td rowspan="2">Firma:</td></tr>
<tr><td>ORCID:<br>https://orcid.org/0000-0002-8901-1026</td></tr>
</table>

**Sumario:** 1. Introducción, 2. Orígenes y desarrollo histórico del principio de responsabilidad proactiva, 2.1 Su aparición en las directivas de la OCDE, 2.2. Referencias en la Unión Europea sobre el principio de responsabilidad, 2.3. La adopción del principio de responsabilidad en Canadá, 2.4. La recepción del principio de responsabilidad proactiva en la Unión Europea, 3. El principio de responsabilidad proactiva en el Nuevo Reglamento y su comparación con el marco europeo, 3.1. Definición del principio de responsabilidad proactiva en el RGPD, 3.2. El principio de licitud y su relación con la responsabilidad proactiva, 3.3. La responsabilidad proactiva sobre el tratamiento de terceros y el deber de asistencia de los encargados del tratamiento, 3.4. La privacidad desde el diseño a la luz de ambos ordenamientos, 3.5. Regulación de mecanismos de responsabilidad proactiva, 4. Desafíos jurídicos derivados de la inclusión de la responsabilidad proactiva a la luz del Nuevo Reglamento, 4.1. El carácter abierto del concepto de responsabilidad proactiva, 4.2. La inversión de la carga de la prueba y presunción de licitud detrás de la obligación de demostración del cumplimiento, 4.3. La transición de un modelo de gestión a un modelo de responsabilidad, 4.4. La necesidad de incorporar responsabilidad proactiva en la supervisión del tratamiento de terceros, 4.5. La implementación de los mecanismos de responsabilidad proactiva en el entorno nacional, 5. Conclusiones, 6. Bibliografía.

**Resumen**

Tras la incorporación en el Nuevo Reglamento de Protección de Datos Personales del principio de responsabilidad proactiva en el ordenamiento jurídico peruano en materia de protección de datos, aquel que implica tanto aplicar medidas para garantizar el cumplimiento como a su vez demostrar la ejecución del mismo. A partir de la inclusión de dicho principio, el marco normativo en la materia adopta conceptos previamente introducidos por normativa extranjera por el Reglamento General de Protección de Datos de la Unión Europea. De esta forma, el marco jurídico de protección de datos se acopla a los estándares europeos.

Como consecuencia de la inclusión del principio, se eleva el margen de protección, pues garantiza que todo responsable del tratamiento se enfoque en el diseño e implementación de medidas para garantizar dicho cumplimiento, así como en la probanza del mismo. Sin embargo, dicha inclusión también conlleva desafíos jurídicos que deben analizarse para su aplicación práctica: 1) el carácter abierto del principio, 2) la inversión de la carga de la prueba y la presunción de licitud, 3) la transición de un modelo de gestión a uno de responsabilidad, 4) la aplicación del principio en la supervisión de datos de terceros y 5) el fomento de la implementación mecanismos de responsabilidad proactiva en el entorno nacional. Por medio del análisis de cada uno de dichos aspectos, se adaptará el concepto trasladado del ordenamiento europeo a la realidad peruana.

**Palabras claves:** responsabilidad proactiva, medidas de cumplimiento, demostración del cumplimiento.

**Abstract**

Following the addition of proactive accountability principle into the Peruvian legal framework on personal data protection through the New Regulation of Data Protection, which implies both applying measures to guarantee compliance and demonstrating such compliance. With the introduction of this principle, the legal framework acquires concepts previously introduced by foreign regulations as the General Regulation of Data Protection from the European Union. Therefore, the national legal framework aligns with European standards.

As a consequence of the incorporation of this new principle, the protection level margin increased due to the fact that it leads to require to every treatment responsible focusing on strategizing and deploying measures with the aim of both guaranteeing compliance and its proof. Nonetheless, that addition also generates the legal defiances which necessitate to be analyzed for its practical implementation: 1) the open-ended nature of the principle, (2) the reversal of the burden of proof and the presumption of lawfulness, (3) the transition from a management-based model to a responsibility-based one, (4) the application of the principle in the supervision of third-party data, and (5) the promotion of the implementation of proactive accountability mechanisms in the national context. Through the analysis of each of these aspects, the concept transferred from the European framework will be adapted to the Peruvian reality.

**Keywords:** proactive accountability, compliance measures, demonstration of compliance.

## Índice

## 1. Introducción

Actualmente, como señala Esteve Pardo, el desarrollo tecnológico de la misma ha eliminado limitaciones naturales de las personas, pero con el coste de aparezcan nuevos riesgos generados por la propia tecnología empleada para mitigarlos (2003, p.54). En el caso de la protección de datos personales, se parte del hecho de que el empleo de la Big Data permitió superar la incapacidad humana de procesar ingentes cantidades de información de forma simultánea. Sin embargo, también dicha tecnología ocasionó nuevos riesgos, tales como la pérdida de control sobre los datos personales, el flujo incontrolado de datos, en tiempos más recientes, la fuga de dicha información de bases de datos de empresas o entidades estatales.

Ante el avance tecnológico, resulta cada vez más complicado que la legislación baste para garantizar la tutela de los derechos afectados. Por ello, ya no bastará que los administrados se limiten únicamente a cumplir con lo que establece la normativa y a responder cuando incurren en incumplimiento, sino además prevenir cualquier riesgo que pueda vulnerar derechos de terceros, en este caso al de protección de datos personales. En virtud de ello, se inserta el concepto de responsabilidad proactiva por medio de las directrices sobre la privacidad adoptadas en 1980 por la OCDE, en las que se establecía que “todo responsable del tratamiento debía responsabilizarse por el cumplimiento de los principios”.

Posteriormente, dicha figura sería adoptada en la Unión Europea por medio del artículo 5 del Reglamento 2016/679, mejor conocido como Reglamento General de Protección de Datos Personales (en adelante, RGDP). En dicha norma, se resalta que dicha responsabilidad no solo consiste en adoptar medidas de cumplimiento, sino además la obligación de acreditar dicho cumplimiento. Cabe señalar que dicho principio se complementaba con la aplicación de la privacidad por diseño para mejorar la arquitectura de sistemas y el uso de diversos mecanismos para acreditar y documentar el cumplimiento, tales como la evaluación de impacto (art.34), los códigos de conducta (art.40), las certificaciones (art.42) y registros de actividades (art.30).

Por influencia del RGPD europeo, el Ministerio de Justicia y Derechos Humanos, a través del Decreto Supremo 016-2024-JUS, promulga el Nuevo Reglamento de la Ley de Protección de Datos Personales (Ley 29733) e introduce expresamente el artículo IX de su Título Preliminar el principio de responsabilidad proactiva. Como se prevé en la Exposición de Motivos, dicho principio se introduce para que los responsables “actúen de forma diligente y anticipada frente al tratamiento que los otros realicen”. A partir de la inclusion de dicha figura, se eleva el estándar de cumplimiento, pues ya no basta con acatar la norma, sino además prevenir y mitigar posibles riesgos derivados de actividades del tratamiento.

Sin embargo, no toda importación de figura extranjera implica necesariamente una adaptación inmediata al entorno nacional. Por el contrario, su aplicación en

el país puede presentar una serie de desafíos jurídicos a atender: ¿Qué se debe entender por “medidas adecuadas”? ¿La obligación de demostrar implica una inversión de la carga de la prueba para el responsable fiscalizado? ¿Cómo se puede aplicar el principio en un país donde aún subyace un modelo meramente formalista de cumplimiento? ¿Se prevé algún deber por parte del responsible para garantizar el respeto a la normativa vigente en actividades de terceros que operen bajo sus instrucciones? ¿Cómo regular los mecanismos de responsabilidad proactiva?

En el presente trabajo, se analizará la regulación del Nuevo Reglamento sobre dicho principio en virtud de tres puntos. En primer lugar, se reconstruirán los orígenes del principio y su evolución histórica dentro de los diversos ordenamientos en los que se acogió dicho principio. En segundo, se realizará un análisis comparado entre la configuración peruana del principio con aquella establecida en el ordenamiento europeo para determinar cuáles elementos adoptó el Nuevo Reglamento y cuáles no en lo referido a la regulación del principio. Por último, se desarrollarán cada uno de los desafíos jurídicos en materia de Derecho Administrativo y se dará respuesta a los cuestionamientos formulados previamente.

## 2. Orígenes y desarrollo histórico del principio de responsabilidad proactiva

La responsabilidad proactiva, aunque introducida recientemente por el Nuevo Reglamento de Protección de Datos Personales, contenido en el Decreto Supremo 016-2024-JUS. Sin embargo, el origen dicha figura se origina por las Directrices de la Organización para la Cooperación y Desarrollo Económicos (OCDE) de 1980 como “principio de responsabilidad”, por el que se establecía la obligación de los responsables de cumplir con la normativa. Posteriormente, dicha figura fue incorporada y perfeccionada en diversos ordenamientos jurídicos como el de la Unión Europea o el canadiense, en los que a partir de sus normas delimitaron los alcances del principio. Finalmente, la regulación internacional se consolida con la aparición del Reglamento General de la Unión Europea, norma de la que se inspira el ordenamiento peruano.

A partir de la presente sección, se desarrollarán los principales hitos históricos en la evolución del concepto. En la primera sección, se abordarán los orígenes en las directrices de la OCDE y su regulación como “principio de responsabilidad”. Luego, en la segunda sección, se ilustrará lo referido al reconocimiento del principio en la Unión Europea a partir del Convenio 108 y de la Directiva 95/46/EC, normas pioneras en la regulación del principio. Para la tercera sección, se explicará el proceso de la incorporación del principio en el Derecho canadiense y su posterior perfeccionamiento mediante la introducción del enfoque de privacidad desde el diseño. Y, por último, en la cuarta sección se abordará lo referido a los últimos avances en la regulación del principio a partir

de su delimitación tanto en las Normas Internacionales de Madrid del 2009 como en el Reglamento General de la Unión Europea del 2016.

### 2.1. Su aparición en las Directrices de la OCDE

El principio de responsabilidad proactiva surge a partir de "las Directrices de la Organización para la Cooperación y el Desarrollo Económicos que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales" del 23 de septiembre de 1980. A partir de dicha directiva, ante la observancia de los avances tecnológicos que permitían tanto el procesamiento como el flujo de datos entre países miembros, estableció parámetros que garantizaran la protección de la privacidad de sus ciudadanos.

Dentro de dichos parámetros, estableció 8 principios como parámetros para el tratamiento de información personal: 1) limitación a la recogida bajo medios lícitos y consentimiento previo, 2) calidad de datos, 3) especificación de fines del tratamiento, 4) limitación de uso para fines distintos a los cuales se produjo la recolección de datos, 5) principio de seguridad, 6) principio de transparencia, 7) principio de participación individual y 8) responsabilidad. Este último principio, en el que se ahondará en el presente trabajo, se estableció de la siguiente forma:

> *"**Principio de responsabilidad. -** A todo responsable de datos se le deberían pedir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios antes expuestos".*

A partir de dicho principio, se establecieron las bases para la concepción de la responsabilidad proactiva. En virtud del principio de responsabilidad, delimitado en base a las directrices de la OCDE, se evidencia un doble propósito: 1) identificar a la entidad, sea pública o privada, a la que se le puede exigir la adopción de medidas de protección, 2) establecer vías dentro de los países miembros para responsabilizar a dicha entidad por el incumplimiento de dichas medidas (Alhadeff, Van Alsenoy y Dumortier, 2012, p.7).

Al respecto, habría que constatar que dicho principio, tal como se formula en las directivas, si bien alude al cumplimiento de los principios a partir de la "aplicación de los mismos, debe tomarse cuenta que el acento estaba en la implementación de medidas concretas que hagan efectivo el cumplimiento exigido (Cañavete Megías, 2021, p.16). Por ello, desde la introducción del principio de responsabilidad se exigía la utilización de mecanismos o procedimientos mediante los cuales los responsables garantizaran el adecuado tratamiento de los datos personales.

Además, cabe señalar que, aunque la forma en la que se establecía dicho principio en las directices de la OCDE se restringiera única y exclusivamente a la responsabilidad legal de los responsables del tratamiento frente a las autoridades locales, ello no es del todo exacto. Como se resalta en el Memorandum Explicativo sobre las Directices, la responsabilidad exigida de dicho principio no solo estriba en lo referido a las sanciones legales a imponer por las autoridades, sino además a aquella reflejada en la implementación de códigos de conducta (OECD 2023, p.31).De esta forma, se constata que dicho

principio no solo estuvo previsto para requerir a los países miembros que se reprima el incumplimiento, sino además que se empleen mecanismos como los códigos de conducta para promover el cumplimiento voluntario o la acreditación del cumplimiento al servir dichos códigos como prueba del cumplimiento.

### 2.2. Referencias en la Unión Europea sobre el principio de responsabilidad

Como producto de las directrices de la OCDE, en la Unión Europea (en adelante, UE) se celebró el Convenio 108 en Estrasburgo el 28 de enero de 1981. En virtud de dicho convenio, se establecieron reglas y lineamientos comunes aplicables a todos los países miembros de la UE para garantizar la protección de los datos personales de sus ciudadanos, ello ante el riesgo de circulación de la información personal y del auge de las tecnologías de tratamiento automatizado de dicha información.

Dicha convención abarcó diversos principios similares a los previstos en las directrices de la OCDE, tales como la calidad de los datos (artículo 5) o la seguridad de los datos (artículo 7). Sin embargo, dentro de los principios establecidos, no se prevé de manera expresa el principio de responsabilidad, tal como sí se hizo en las directrices. Aún así, estableció en su artículo 4 que cada parte, en su derecho interno, adoptará las medidas necesarias para que se hagan efectivos los principios básicos previstos en el capítulo.

En virtud de dicha disposición, se contemplaba la adopción de mecanismos necesarios para garantizar la observancia de los principios establecidos en la convención en cuestión. No obstante, a partir de dicha disposición, solo se establecía la posibilidad de atribuir a las Administraciones públicas las potestades de control, inspección y sanción para las actividades gestionadas por entidades públicas o privadas (Estepa Montero 2022, p.69), pero sin obligar a estas últimas a establecer medidas para el cumplimiento de la normativa.

Posteriormente, el Parlamento Europeo de la UE expidió la Directiva 95/46/EC el 24 de octubre de 1995. Al igual que las directrices de la OCDE y el Convenio 108, surgió en virtud de la motivación de promover en la Comunidad europea el tratamiento de datos personales por el permanente avance de la tecnología y por el avance en la recopilación de datos personales. Lo resaltante de dicha directiva es que fue la primera directiva en Europa en regular la protección de datos y la libre circulación de los mismos.

En lo que respecta a dicha directiva, se debe destacar que no contiene de manera explícita el principio de responsabilidad a diferencia de las directrices de la OCDE. A pesar de ello, el Grupo de Trabajo del Artículo 29 (en adelante, GT29) considera que existen algunas disposiciones de dicha directiva que sí aluden a dicho principio, por ejemplo, el artículo 6. Dicho artículo señala en su segundo apartado que “el responsable debe cumplir las obligaciones establecidas en el párrafo anterior”, entre ellas la del tratamiento lícito y a partir adecuados, pertinentes y no excesivos para las finalidades por las que se recopilaron (GT29 2010, p.9).

De manera similar, el artículo 17 de dicha directiva señalaba que se requiere de apropiadas medidas técnicas y organizativas para proteger los datos personales contra el tratamiento no autorizado o contra la pérdida o alteración de los mismos. Además, cabe interpretar del artículo 26 que los responsables debían adoptar medidas para cumplir con el requisito de "ofrecer garantías adecuadas en transferencias de datos personales" (GT29 2010, p.10).

### 2.3. La adopción del principio de responsabilidad en Canadá

En la década de los 90, si bien en Canadá todavía no contaba todavía con legislación en materia de protección de datos personales. Sin embargo, dentro de esa misma década ocurrió un hito relevante: la expedición del informe "Privacy Enhancing Technologies" el año 1995 por la comisionada Ann Cavoukian, en ese entonces comisionada de Información y Privacidad en Ontario, de manera conjunta con John J.Borking, comisionado de la autoridad de datos personales de Países Bajos. Dicho artículo fue importante, pues no solo estableció que, aparte de establecer medidas que aseguren el cumplimiento de los principios, el diseño de tecnologías debe salvaguardar la privacidad de los usuarios (Cavoukian y Borking 1995, p.7). De este último aspecto nació el principio de "Privacy By Design".

Para el año 2000, se expide la primera ley en materia de protección de datos personales a partir del Personal Information Protection and Electronic Documents Act (PIPEDA). En dicha ley, no solo se reconoció legislativamente el principio de responsabilidad, sino que se adoptó y perfeccionó la regulación del principio establecido en las directrices de la OCDE. Mediante la ley, se buscó no solo garantizar la protección de datos personales dentro de dicho país, sino que además se preocupa por la organización de actividades de tratamiento de datos dentro del sector empresarial.

En dicha ley, se estipulan varios principios que aseguran la debida protección de la información personal, dentro de los que resalta particularmente el principio de responsabilidad, denominado en ella como "accountability". A partir de dicho principio, se constata en el artículo 4.1. de la ley que todas las organizaciones deben implementar las siguientes medidas: 1) designar a un responsable del tratamiento dentro de la misma organización, 2) establecer procedimientos para hacer efectivo el cumplimiento de la normativa, 3) prever procedimientos para recibir y responder denuncias y reclamos, 4) entrenar al personal para aplicar las medidas de organización y 5) explicar al mismo personal sobre políticas y procedimientos.

En primer lugar, resalta que en dicho principio se haya preferido el término en inglés "accountability" en lugar de "responsibility" para referirse al concepto de responsabilidad en el tratamiento. En materia de protección de datos personales, mientras que por "responsibiliy" se alude a simplemente limitarse a cumplir la norma y a responder ante los incumplimientos ante las autoridades competentes, "accountability" alude también a la rendición de cuentas en el tratamiento de datos personales, en tanto los responsables del tratamiento cuenten con la

obligación de demostrar el cumplimiento del marco jurídico vigente (De Hert, 2012, p.199).

Asimismo, la presente ley, en comparación con las Directrices de la OCDE, no solo se restringe a señalar que se deben adoptar medidas que garanticen la protección de datos, sino que además señala un catálogo de medidas, dentro de ellas las 5 previamente señaladas. Y aparte, lo particular es que no se limita a señalar que las organizaciones deben responsabilizarse de los datos que procesan, sino que se enfoca en establecer mecanismos de cumplimiento que puede implementar la propia organización supervisada de manera interna (Alhadeff, Van Alsenoy y Dumortier, 2012, p.10). Por ejemplo, las exigencias de explicar a los trabajadores la norma y de capacitar al personal de la propia empresa en la aplicación de los principios son garantías internas que los supervisados pueden implementar para cumplir con la normativa.

Posteriormente, el principio de responsabilidad establecido en la ley canadiense se complementaría con la publicación en el año 2009 del artículo denominado "Privacy by Design:7 Foundational Principles", redactado por la misma Ann Cavoukian. En virtud de dicho artículo no solo se definía a dicho principio como aquel que vela porque la privacidad se instaure desde el diseño de las tecnologías y sistemas, sino que además incorporó un listado de 7 principios a partir de los que se puede alcanzar dicho propósito de la siguiente manera (2009, p.1-5):

- Enfoque proactivo, no reactivo; preventivo, no correctivo: se trata de un enfoque preventivo por anticiparse a las posibles afectaciones a la privacidad antes de que estas ocurran. Y preventivo por no esperar que los riesgos se materialicen para recién tomar acción.
- Privacidad por defecto: la privacidad debe configurarse de manera predeterminada en los dispositivos tecnológicos, lo que implica que la configuración debe garantizar la privacidad de las personas de manera automática y sin que el usuario realice acciones adicionales.
- Privacidad adherida al diseño: implica que los dispositivos deben hallarse diseñados de tal forma que garanticen la privacidad desde su fabricación.
- Funcionalidad total- "Todos ganan"-no "Si alguien gana otro pierde": implica que no se debe priorizar la protección de privacidad en los dispositivos para sacrificar otras obligaciones que deben garantizar los responsables en su funcionalidad, tales como la seguridad de los mismos.
- Seguridad de extremo a extremo-protección del ciclo de vida de los datos: desde el momento en el que los usuarios brindan sus datos hasta el momento en el que se destruyen, es decir, durante todo el ciclo de vida, se garantizará la seguridad de dichos datos en el transcurso de dicho ciclo.
- Visibilidad y transparencia: deben comunicarse de manera abierta las políticas de privacidad, así como cualquier otra operación que involucre el tratamiento de forma clara a los usuarios.
- Respeto por la privacidad de los usuarios: dicha obligación implica adoptar un enfoque que contemple la protección de los datos personales

de usuarios como prioridad, así como optar por la notificación de acciones del tratamiento o por la comunicación al usuario sobre sus derechos y las vías para ejercerlos."

En virtud de dichos principios, se garantizará una protección de los datos no solo que se acople al diseño de los equipos o aplicaciones tecnológicas, sino además aquella de carácter proactivo y preventivo. De esta forma, se establece que los responsables del tratamiento no deben esperar a que los usuarios procedan con algún reclamo o alguna denuncia ante las autoridades respectivas por el defectuoso tratamiento de los datos personales, sino más bien asegurar la privacidad como configuración predeterminada desde el diseño de los dispositivos hasta el fin del ciclo de utilización de los datos proporcionado. Ello efectivamente complementado por un tratamiento amigable a los usuarios a partir desde la transparencia sobre políticas u operaciones sobre los datos hasta el respeto de sus derechos sobre su propia información.

### 2.4. La recepción del principio de responsabilidad proactiva en la Unión Europea

En los últimos años, se han emitido diversas disposiciones en la UE que reconocen la existencia del principio de responsabilidad proactiva. Dentro de ellas, estarían las Normas Internacionales de Madrid, desarrolladas por la Conferencia Internacional de Comisarios de Protección de Datos y Privacidad el año 2009. Por medio de dichas normas, se establecía la siguiente disposición sobre el principio:

*"**Principio de responsabilidad. -La persona responsable debe:***

a. *Tomar todas las medidas necesarias para observar los principios y obligaciones establecidas en este documento y en las normas nacionales respectivas*
b. *Contar con los mecanismos necesarios para hallarse en posición de demostrar ante los titulares de los datos personales y las autoridades locales el cumplimiento de la normativa"*

Como resalta de lo señalado, se establece de manera expresa que el responsable debe adoptar las medidas adecuadas para concretizar el cumplimiento de las obligaciones establecidas, estipulaciones similares a las establecidas por la Directiva 95/46/EC como se señaló con anterioridad. Sin embargo, añade como novedad la obligación de demostrar el cumplimiento de los principios y de obtener los recursos o insumos necesarios para alcanzar dicho propósito.

Adicionalmente, habría que señalar que, en ese mismo año, el GT29, en respuesta a una consulta planteada por la Comisión Europea de la UE, dentro de los nuevos desafíos, propuso la inclusión del principio de responsabilidad proactiva y de mecanismos basados en la rendición de cuentas en la Directiva 95/46/EC, con el objetivo de reforzar el cumplimiento normativo por parte de los responsables del tratamiento (2009, p.20). Cabe señalar que el GT29 replicaría dicha recomendación, toda vez que como se señalaba en el Dictamen 3/2010,

debía llevarse la aplicación de los principios por parte de los responsables de la teoría a la práctica (2010, p.2).

Finalmente, dichas recomendaciones fueron considerados en la elaboración y en la promulgación del Reglamento General de Protección de Datos Personales (en adelante, GPDR) el 17 de abril del 2016. En virtud de dicho reglamento, se incluyó por primera vez dicho principio de manera expresa en el artículo 5 referido a los principios del tratamiento y estableció dos condiciones para su aplicación: 1) que el responsable cumpla con la normativa de protección de datos personales y 2) que será capaz de demostrar su cumplimiento.

Cabe señalar que, en los considerandos de dicho artículo, se estipula en el considerando 78, por un lado, que se deben adoptar las medidas técnicas y organizativas adecuadas no solo como se establecía en el artículo 17 de la Directiva 95/46/EC para cumplir con el principio de seguridad, sino además con el resto de los principios establecidos en dicho reglamento. Pero, por otro lado, se señalaba en ese mismo considerando que el responsable debe demostrar el cumplimiento de la normativa mediante la adopción de políticas internas que permitan velar por el cumplimiento de los principios en un marco de privacidad desde el diseño. Así, se evidencia que el Reglamento no solo estuvo inspirado por las Normas Internacionales de Madrid, sino además por el concepto de privacidad en el diseño establecido en el sistema jurídico canadiense.

Por último, es importante resaltar que el principio de responsabilidad proactiva en dicha normativa no solo se reduce a delimitar dicho principio, sino también a establecer diversos mecanismos que garanticen la aplicación del principio en cuestión. Por ello, se señala en los considerandos que, en observancia del principio, el responsable debe adherirse a códigos de conducta para demostrar que haya cumplido con la normativa (considerando 81), así como un registro de actividades por la necesidad de mantener un control interno sobre el tratamiento de dichos datos (considerando 83) y emplear evaluaciones de impacto para que el responsable no se limite a reaccionar a los riesgos, sino además a preverlos. Sobre dichos mecanismos se comentará en los siguientes puntos del trabajo.

## 3. El principio de responsabilidad proactiva en el Nuevo Reglamento y su comparación con el marco europeo

Por medio del Nuevo Reglamento peruano, se estipula por primera vez en la normativa de datos personales el principio de responsabilidad proactiva. Al respecto, debe tomarse en cuenta en virtud de lo desarrollado en el primer punto del artículo que dicha figura en realidad ya provenía de años de desarrollo en otros ordenamientos jurídicos como el de la Unión Europea. Por ello, la incorporación del principio en el Perú no puede considerarse como una creación espontánea de una nueva figura jurídica, sino más bien inspirada en instituciones jurídicas implementadas en sistemas jurídicos extranjeros, de forma tal que la normativa nacional se acople a las tendencias internacionales en la materia.

A través de la Exposición de Motivos del Nuevo Reglamento peruano, el Ministerio de Justicia y Derechos Humanos (MINJUSDH), entidad que expidió

dicho reglamento, señala respecto a la inclusión del principio de responsabilidad proactiva que se produjo con la intención de asimilar en el ordenamiento nacional principios establecidos por el RGPD europeo y, además, por el hecho de que este principio en concreto permite elevar el estándar de protección de datos personales de forma novedosa y concreta al incentivar que los responsables adopten de oficio y de manera anticipada medidas de cumplimiento normativo (MINJUSDH 2024, p.15). De esta forma, el MINJUSDH incorporó el principio con la finalidad de modernizar el marco normativo de protección de datos en observancia de lo previamente regulado por el Derecho europeo.

En virtud de la inspiración del Nuevo Reglamento del sistema de la Unión Europea en protección de datos, conviene revisar la forma en la que el RGPD regula el principio de responsabilidad proactiva. Por ello, se abordará lo que se prevé en dicha norma sobre diversos temas: a) la definición del principio, b) el principio de licitud, c) el principio de responsabilidad del responsable sobre el tratamiento de terceros, d) la privacidad desde el diseño y e) mecanismos de responsabilidad proactiva. A continuación, se desarrollarán cada uno de dichos puntos y se determinará cuáles son asimilados por la regulación del principio en el Nuevo Reglamento peruano.

### 3.1. Definición del principio de responsabilidad proactiva en el RGPD

En el Nuevo Reglamento, se estableció el principio de responsabilidad proactiva en el artículo IX del Título Preliminar. Dicho principio se encuentra previsto a partir de los siguientes términos:

> *"**Artículo IX.-Principios rectores***
> *Principio de responsabilidad proactiva: En el tratamiento de datos personales se deben aplicar las medidas legales, técnicas y organizativas a fin de garantizar el cumplimiento efectivo de la normativa de datos personales, y el titular del banco de datos personales o quien resulte responsable, debe ser capaz de demostrar tal cumplimiento"*

Por su parte, el RGPD actual, el principio de responsabilidad proactiva se encuentra establecido en el artículo 5.2. A partir de dicha disposición normativa, el Parlamento Europeo se limita a señalar que "el responsable del tratamiento será responsable del cumplimiento de los principios del apartado 1 y que será capaz de demostrarlo («responsabilidad proactiva»)". Como se observa, dicho principio radica en el cumplimiento de los principios del tratamiento (por ejemplo, licitud, consentimiento, finalidad, entre otros), así como en la obligación de acreditar dicho cumplimiento.

A partir de ambos ordenamientos, se desprende que dicho principio implica dos condiciones. Por un lado, este principio implica la obligación asignada a titulares de banco de datos como a responsables del tratamiento de implementar las medidas que garanticen el cumplimiento de sus obligaciones en virtud del marco legal vigente en materia de protección de datos personales. Y, por otro lado, el artículo en cuestión configura una segunda obligación, en este caso la de probar el cumplimiento de la normativa. Esto último se relaciona con la rendición de cuentas, en tanto la acepción de dicho principio involucre el deber de acreditar

de forma permanente la conformidad con la normativa (Vásquez Rodríguez, 2022, p.29).

Sobre la primera obligación, esta implica la adopción de instrumentos que garanticen el cumplimiento de la normativa. Sin embargo, debe considerarse que la particularidad de dicho principio recae en la naturaleza del cumplimiento que se exige: en tanto la responsabilidad sea precisamente “proactiva”, las medidas que se apliquen no solo deben apuntar a acatar la norma, sino además a prever y mitigar riesgos en materia de privacidad (Santamaría Ramos, 2020, p.166). Por ejemplo, no solo se requerirá que el titular del banco o responsable establezca control de accesos, sino que implemente auditorías para comprobar su adecuado funcionamiento.

Por otro lado, está la obligación de demostrar el cumplimiento, en tanto se conciba por este nuevo principio que el responsable debe acreditarlo. En estos casos, se contempla que el responsable debe estar en condiciones de rendir cuentas sobre la diligencia de su actuación ante las autoridades o ante ciudadanos interesados, lo que implica no solo acreditar la conformidad de las actividades, sino además la eficacia de las medidas. De esta forma, la clave del concepto está en que el administrado operador de un banco de datos o responsable del tratamiento pueda probar el debido tratamiento (Estepa Montero, 2022, p.76).

Cabe señalar que, a partir del deber de demostrar, ya no solo será necesario que se actúe en conformidad con la ley, sino que además el responsable del tratamiento cuente con los medios de prueba suficientes para probar dicha conformidad. Por ello, ya no solo debe limitarse, en el caso del consentimiento, a requerirlo, sino además a conservar los formatos, sean físicos o impresos, de la manifestación de la voluntad o, en lo referido al ejercicio de derechos ARCO, mantener registros internos en las empresas que permitan demostrar que se hayan atendido las solicitudes de los titulares (Vásquez Rodríguez, 2022, p.33). Así, se requiere que las entidades públicas o empresas puedan no solo alegar la aplicación de medidas, sino además contar y proporcionar los medios probatorios necesarios para acreditar el cumplimiento normativo.

Además, como se señala en el artículo IX del Título Preliminar del Nuevo Reglamento, el principio contempla la aplicación de tres tipos de medidas: jurídicas, organizativas y técnicas. Sobre las jurídicas, implican la redacción de documentos legales, por ejemplo, diseñar formatos para solicitar consentimiento o la elaboración de políticas de privacidad. En cuanto a las organizativas, están relacionadas con la organización de la empresa, entre ellas las auditorías de cumplimiento normativo o las capacitaciones al personal de la empresa o entidad. Y por técnicas, están aquellas de carácter físico o tecnológico que garanticen un tratamiento acorde a la normativa, tales como el uso de cerraduras o la gestión de contraseñas para evitar accesos no autorizados, el cifrado para velar por la no alteración de la información, y la anonimización para que los datos ya no identifiquen a un individuo en específico (Alvarado, 2016, p.38).

De manera similar, el ordenamiento europeo establece en el artículo 24 del RGPD, en tanto “el responsable aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento”. Esta disposición complementa a la anterior señalada, pues, por un lado, se constata que dicho principio de responsabilidad proactiva no solo se reduce a garantizar el cumplimiento de los principios, sino además de las demás disposiciones del RGPD. Y, por otro, que las medidas técnicas y organizativas a adoptar son instrumentos para el cumplimiento de todo el Reglamento Europeo (Cañavete Mejías, 2021, p.17).

Sin embargo, pese a las similitudes abordadas entre ambos ordenamientos, el mismo artículo 24 del RGPD contempla determinados aspectos no previstos en la definición del Nuevo Reglamento peruano. Por un lado, el RGPD no solo se reduce a estipular que las medidas adoptadas garanticen el cumplimiento como la nueva norma peruana, sino que además detalla que serán apropiadas de acuerdo con “la naturaleza, el ámbito, el contexto y los fines del tratamiento”. Ello es importante destacar, pues a partir de dicha acotación, el RGPD prevé que la aplicación de dicho principio no debe ser rígida, sino más bien adaptable a la situación en concreto (AEPD, 2018, p.4). En este sentido, se reconoce que factores como el volumen o el tipo de datos puede influir en la necesidad o no respecto a adoptar determinadas medidas.

Por otro lado, cabe resaltar que en tanto en el artículo 24.1 como en el considerando 74 del RGPD, a diferencia de la definición del Nuevo Reglamento, señala de manera expresa que, para la aplicación del principio, se deben tomar en consideración “los riesgos de diversa probabilidad y gravedad en la afectación de derechos”. A partir de dicha disposición, no se reduce el ámbito de aplicación del principio al cumplimiento de la normativa, sino con la prevención de futuras contingencias, toda vez que se requiere al responsable evaluar riesgos en cuanto al grado (leve, moderado, grave), en cuanto a la probabilidad de su ocurrencia y sobre qué medidas son más pertinentes para mitigarlo (Piñar Mañas et al., 2016, p.465). De esta forma, se acentúa en mayor medida en el Derecho europeo el enfoque de prevención de riesgos en la delimitación del principio.

Asimismo, sobre dicho enfoque, el considerando 75 desarrolla el concepto de riesgo como cualquier efecto ocasionado por el propio tratamiento de datos personales capaz de derivar en daños que perjudiquen a los derechos y libertades de las personas, entre ellos problemas de discriminación, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, entre otros. Adicionalmente, el GT29 precisa que el enfoque de riesgos de dicho considerando no se restringe a la protección del derecho a la protección de datos o la intimidad, sino también a otros como la prohibición de discriminación, la libertad de pensamiento o consciencia (2017, p.7). Por ejemplo, la deficiente gestión de datos como raza, opinión política, estatus económico y salud no solo puede derivar en una pérdida de control de dichos datos, sino además en discriminación, así como también puede caber afectación al derecho a la imagen en caso de filtración no autorizada de esa misma información confidencial.

Además, debe tomarse en cuenta que el artículo 24.2 del RGPD, a diferencia del ordenamiento peruano, introduce un criterio de proporcionalidad en la exigencia de las medidas de cumplimiento, pues estipula que se incluirán políticas de protección de datos solo si son "proporcionadas" con las actividades del tratamiento. Ello implica que la Autoridad supervisora evalué si le corresponde al responsable o no implementar políticas en observancia no solo de las condiciones del tratamiento (naturaleza, ámbito, contexto o finalidad del tratamiento), sino además con relación a la capacidad para prever y mitigar riesgos (Cañavete Mejías, 2021, p.17). De esta forma, solo se adoptarán políticas internas si las condiciones del tratamiento o el nivel de riesgo lo justifican.

Respecto al criterio de proporcionalidad en la exigencia de las medidas de cumplimiento, está el hecho de que la implementación de medidas debe garantizar un equilibrio entre el derecho a la protección de datos personales de terceros y los intereses legítimos del propio responsable del tratamiento (Barrio Andrés, 2024, p.1328). Por ello, la obligación del responsable de velar o demostrar cumplimiento normativo no debe forzarlo a soportar cargas innecesariamente onerosas para su actividad empresarial. En virtud de ello, el artículo 35.1 del RGPD solamente exige evaluaciones de impacto a aquellas entidades que tiendan a procesar grandes volúmenes de datos, mientras que en los demás casos la adopción de dicha política deviene en facultativa.

Finalmente, debe destacarse de la regulación del principio en el RGPD es no solo se limita, como en el caso del artículo IX del Nuevo Reglamento peruano, a señalar que se adoptarán las medidas para garantizar el cumplimiento, sino que además añade que "dichas medidas se revisarán y se actualizarán cuando sea necesario". A partir de ello, se establece en el ordenamiento de la Unión Europea un requisito temporal para la aplicación de la responsabilidad proactiva, de tal forma que el responsable se preocupe por la mejora de manera continua en lo que se refiere a la protección de los datos personales (Durán Troncoso, 2021, p.1780). En este sentido, se constata que la implementación de medidas no solo debe reducirse a un momento específico, sino que debe hacerse presente durante todo el ciclo de tratamiento, en tanto los estándares técnicos y organizativos de cumplimiento normativo puedan variar a lo largo del tiempo.

### 3.2. El principio de licitud y su relación con la responsabilidad proactiva

Ahora bien, dado el hecho de que el principio de responsabilidad proactiva se focaliza principalmente en el cumplimiento normativo, dicho principio está vinculado con el principio de licitud. Dicho principio exige, como se estipula en el artículo 5 del RGPD, que "los datos sean tratados de manera lícita en relación con el interesado". Ello implica que el tratamiento tiene que contar con respaldo en el ordenamiento jurídico (Puyol 2016, p.141). En este sentido, se requiere que las actividades del responsable se ciñan a lo establecido en la legislación vigente en la materia en beneficio de los titulares de dichos datos.

Similar disposición se encuentra recogida en el artículo 4 la Ley de Protección de Datos Personales peruana (en adelante, LPDP), en tanto se prevea que "el

tratamiento de datos personales se hace conforme a lo establecido por la ley. Se prohíbe la recopilación por medios fraudulentos, desleales o ilícitos". De forma análoga, se entiende por dicha disposición que toda actividad de tratamiento debe operar en observancia de dicha ley y de su respectivo Reglamento. Por esta razón, cualquier vulneración a alguna de las disposiciones legales sobre la materia deviene en vulneración de dicho principio (Zamudio Salinas, 2022, p.79). En este sentido, se puede señalar que dicho principio se centra en la obediencia al ordenamiento jurídico del tratamiento de datos personales.

Sin embargo, el principio de licitud del RGPD no solo se limita a exigir cumplimiento normativo como el principio de legalidad peruano, sino además en la legitimidad del mismo de acuerdo con lo regulado en el artículo 6. En dicho sentido, estipula una serie de bases que legitiman el tratamiento de datos personales:

a) El consentimiento del interesado para uno o varios fines específicos,

b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales

c) El tratamiento es requerido para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

d) El tratamiento sirve para proteger intereses vitales del interesado o de otra persona física

e) El tratamiento contribuye al cumplimiento de una misión realizada en interés público

f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

Como se observa, existen condiciones que se deben cumplir para garantizar dicho principio de licitud. Una de las más resaltantes es la del consentimiento para fines específicos, pues se erige como base legitimadora para el tratamiento de datos personales, en tanto el titular esté facultado a autorizar a terceros para dar tratamiento a partir de su información personal.

Lo interesante de dicha condición es que establece la especificidad del consentimiento, pues el responsable debe limitar el tratamiento únicamente hacia los fines que haya aceptado expresa y concretamente el titular, de forma tal que deberá obtener un nuevo consentimiento para otros fines no especificados de manera previa al tratamiento (Comité Europeo de Protección de Datos, 2020, p.14). Cabe señalar que, aparte de la especificidad del consentimiento, se requiere el mismo consentimiento también debe ser libre, explícito, inequívoco e informado, como se estipula en el artículo 4.11 del RGPD.

Además, dentro del propio artículo, se establecen otras condiciones por las que se puede cumplir dicho principio por las que no se requiera consentimiento previo. Por ejemplo, si se determina que el tratamiento es indispensable para la

propia ejecución del contrato o bien para la aplicación de medidas precontractuales por parte del administrado. Como señala el Tribunal de Justicia de la Unión Europea (en adelante TJUE), para que se cumpla con dicha condición, se requiere que el tratamiento a realizar sea esencial para lograr un fin que sea parte integrante de la relación contractual (Sentencia 4.7.2023, asunto C-252/21, apartado 98).

Ese supuesto se presenta cuando, por ejemplo, se emplean datos proporcionados por el usuario para gestiones de cobranza sobre algún servicio que se le proporcione a su favor. O, en el caso de las medidas precontractuales, cuando el responsable requiere que el titular de los datos proporcione su historial de deudas para evaluar riesgos crediticios previos a la celebración del contrato de préstamo.

Aparte de los señalados, existen supuestos de tratamiento de datos previstos dentro del propio artículo 6, tales como aquellas que involucran el cumplimiento de una obligación legal, la protección de intereses vitales del interesado o la tutela de un interés público. Respecto al primer supuesto, se prevén situaciones como el empleo de datos personales de clientes para detectar pagos fraudulentos o proporcionar información relevante sobre los mismos para investigaciones penales (Mato Pacín, 2020, p.168). Asimismo, los otros dos supuestos pueden estar vinculados entre sí, por ejemplo, cuando el gobierno realiza seguimiento de la población de un país para controlar una epidemia a partir del rastreo de la población contagiada (GT29, 2014, p.25).

Como último de los supuestos del artículo 6 del RGPD, está el supuesto de interés legítimo del responsable. De acuerdo con el GT29, los intereses deben ser: 1) lícitos, en tanto no estén prohibidos por la legislación nacional o de la UE, 2) específicos, pues debe establecerse con claridad cuál es el interés, y 3) reales y actuales, por lo que no deben ser especulativos, sino enfocarse en percibir beneficios actuales o en un futuro próximo (2014, p.29). Ejemplo de ello podría ser cuando una empresa invoca como interés la protección de equipos frente a posibles hurtos a partir de la implementación de sistemas de supervisión de sus trabajadores, pues dicho interés es licitud por no contradecir ninguna norma, específico por la claridad del mismo, y real si ya han ocurrido incidentes previos.

Cabe señalar que, para la aplicación del supuesto de interés legítimo, el TJUE considera necesario evaluar si el tratamiento es necesario para lograr dicho interés y si es que los derechos del titular de los datos prevalecen ante el interés en cuestión (Sentencia 17.6.2021, asunto C-597/19, apartado 106). Por ello, se reconoció en el caso de MICM, empresa proveedora de películas, que contaba con el interés legítimo de cobro de indemnización por propiedad intelectual. Para ello, era necesario que dicha empresa requiriera a los proveedores las direcciones IP de los usuarios que comercializaron sus películas sin su autorización para determinar el domicilio que demandar. Además, el derecho a la confidencialidad no prevalece frente al interés de cobro de indemnización, pues dicha situación desprotege al derecho a la propiedad intelectual de la empresa afectada (Sentencia 17.6.2021, asunto C-597/19, apartado 116).

Por otro lado, cabe señalar que el principio de licitud del artículo 6 del RGPD se relaciona con el principio de responsabilidad proactiva del artículo 5 de la dicha norma. De hecho, en virtud de este último principio, el responsable no solo se limitará a realizar el tratamiento en virtud de alguna de las bases legitimadoras señaladas con anterioridad, sino que además tendrá la obligación de rendir cuentas, de tal forma que se encuentre en condiciones no solo de explicar las razones por las que se aplica dicha base en específico al caso en concreto, sino que además sea capaz de mantener la evidencia de que se haya recurrido a dicha base para el tratamiento (Bacaria 2018, p.25).

En esta misma línea, se dispuso de manera expresa en el artículo 7 que "el responsable debe ser capaz de demostrar que el titular de los datos ha dado su consentimiento para la operación del tratamiento". Precisamente, lo que se ordena con dicha disposición es que se acredite la implementación de una de las bases del tratamiento previamente señaladas, en este caso la del consentimiento del titular.

Para lograr acreditar la implementación de bases del tratamiento, el responsable debe encontrarse en condiciones de constatar que efectivamente ha cumplido con obtener la autorización expresa del titular de los datos, por lo que debe mantener un registro de las declaraciones de consentimiento recibidas que constaten que la autorización haya sido expresa e inequívoca, así como preservar la documentación que se remitió al titular para demostrar que aquel fue informado de manera clara y específica sobre las finalidades del uso de su información personal (GT29, 2017, p.23).

Cabe señalar que el principio de licitud, como se estipula en el artículo 5.1 del RGPD, está ligado al de lealtad y de transparencia, pues se debe informar previamente al titular sobre las condiciones del tratamiento, así como garantizarle que dichas condiciones se vayan a cumplir en la práctica (Pavón Durán, 2024, p.59). Así, se exige que el responsable no solo manifieste al titular cuál de las bases de legitimación del artículo 6 se aplica, sino además velar porque dicha opción se respete durante todo el tratamiento (Comité Europeo de Protección de Datos, 2020, p.24).

Por ello y en línea con el principio de responsabilidad proactiva, el responsable no solo debe conservar formatos en los que se haya informado a los titulares sobre la elección de determinada base, sino además realizar auditorías que verifiquen que esta se implemente en la práctica, de forma tal que se eviten casos en los que se señale que la base legitimadora es el consentimiento, pero se traten datos sin autorización del titular de los datos por la existencia de un interés legítimo no informado previamente.

Por último, cabe constatar que, en el ordenamiento europeo el consentimiento se establece no como la base única base legitimadora, sino que más bien se convierte en una base legitimadora residual, razón por la que incluso cabe que el mismo responsable determine si es que existe otra base aplicable de acuerdo con el contexto del caso (Esteva Garvayo 2020, p.36). Ello podría ocurrir cuando, por ejemplo, como en el caso de la empresa MICM señalado anteriormente, en

el que se alegaba como interés legítimo el demandar por derechos de autor a los usuarios que comercializaron sus películas sin autorización, situación en la que, evidentemente, el responsable determinará como no factible requerir consentimiento ante la probable negativa de los titulares a ser demandados.

### 3.3. La responsabilidad proactiva sobre el tratamiento de terceros y el deber de asistencia de los encargados del tratamiento

Como se había desarrollado previamente, el principio de responsabilidad proactiva del artículo IX del Título Preliminar del Nuevo Reglamento peruano es similar al del RGPD, en tanto prevé nuevas obligaciones para el responsable, dentro de ellas la de adoptar medidas de cumplimiento normativo, así como la de demostrar dicho cumplimiento. En este sentido, estipula deberes que el responsable debe acatar no únicamente para responder ante infracciones normativas, sino además para una adecuada rendición de cuentas frente a la autoridad o los titulares de los datos para acreditar la observancia a la norma en el tratamiento realizado.

Sin embargo, no especifica si es que dicho principio se aplicará solo en virtud del tratamiento que el responsable realice directamente o si también deberá aplicarlo en virtud del tratamiento de terceros. En cambio, el RGPD sí establece en el considerando 74 una previsión al respecto: “debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta”.

Sobre el particular, debe indicarse que, si bien no se señala de forma explícita que el responsable se hará cargo del tratamiento de terceros, cuando se señala que se responsabilizará por tratamientos que se lleven a cabo “por su cuenta” implica que debe asegurarse que no solo el tratamiento de agentes subordinados a sus instrucciones ciña sus actividades del tratamiento a la luz de la normativa (Cañavete Mejías, 2021, p.18). Por ello, es obligatorio que se apliquen medidas para la supervisión de terceros, tales como inspecciones constantes o solicitud de reportes de actividades.

En esta misma línea, se exige que el responsable no solo aplique medidas para asegurarse sobre el cumplimiento de datos personales por parte de encargados o terceros subcontratados, sino que además deberá demostrar que el encargado o tercero designado ofrezca garantías que garanticen que cumplirá con las previsiones exigidas por ley para el tratamiento de datos. Para ello, por ejemplo, el RGPD prevé que el responsable pueda acreditar que los encargados sean idóneos para garantizar el tratamiento de datos, en tanto puedan probar en virtud del artículo 28.1 que el encargado se haya adherido a códigos de conducta o certificaciones de privacidad (Roig Batalla, 2017, p.6). Así, los responsables cumplirán con demostrar que tuvieron la diligencia suficiente para designar encargados capacitados para realizar tratamiento de datos personales.

Asimismo, los responsables también cuentan con otras obligaciones interpretables a la luz del principio de responsabilidad proactiva. Dentro de dichas obligaciones, están la de proporcionar los datos mencionados en el contrato, la de brindar instrucciones relativas al tratamiento de datos y la de

garantizar antes y durante el tratamiento el cumplimiento de las obligaciones impuestas por el RGPD (Comité Europeo de Protección de Datos, 2020, p,40).

Las obligaciones en cuestión pueden documentarse a partir de los contratos celebrados con los encargados para constatar que en ellos se hayan establecido cláusulas por las que los encargados se obliguen a cumplir las normas, las comunicaciones mediante las que se hayan brindado lineamientos sobre el tratamiento a dichos encargados, los registros que acrediten que el responsable haya cumplido con enviar los datos personales materia del contrato y con la conservación de los reportes de cumplimiento remitidos por el encargado.

Ahora bien, cabe señalar que el responsable no solo tiene la obligación de garantizar que los encargados cumplan con la normativa de protección de datos, sino además los subencargados, conocidos como “encargados adicionales” de conformidad con el artículo 28.2 y que suelen ser terceros contratados por el encargado inicial. De hecho, el responsable está obligado a identificar a dichos subencargados del tratamiento, pues solo así podrá informar a los titulares de los datos de manera completa cuáles serán todos los destinatarios de los datos (Comité Europeo de Protección de Datos, 2024, p.11). Dicha identificación resulta de utilidad cuando exista una cadena de tratamiento extensa en la que existan más de un subencargado aparte del encargado inicial, por lo que debe el responsable solicitar al encargado inicial una lista de todos los subencargados.

Además, en cuanto a la actividad de los subencargados, se requiere que el responsable por sí mismo verifique el subencargado cumpla con la normativa. Por un lado, cuenta con la obligación de velar porque la elección de los subencargados cumpla con las garantías adecuadas, por lo que debe exigir al encargado inicial la información necesaria para evaluar la idoneidad de los subencargados previo a la autorización del subencargo y los modelos de contrato celebrados para verificar que las obligaciones estipuladas en el contrato de subencargo sean las mismas que las del encargo inicial (Comité Europeo de Protección de Datos, 2024, p.16).

Y, por otro lado, debe exigir además que el encargado le asista con la supervisión de las actividades de los subencargados y con la remisión de informes de cumplimiento de la normativa de la materia para realizar el debido seguimiento. De esta forma, el responsable se mantendrá no solo estar informado sobre las actividades de estos últimos, sino que además podrá tomar conocimiento aquellos cumplen o no con la normativa de protección de datos en la ejecución del subencargo.

Otro tema relevante es el rol del encargado en el cumplimiento del principio de responsabilidad proactiva. En la LPDP peruana, se estipula en el artículo 12 que el encargado debe observar los principios establecidos en la ley, así como el artículo 28 establece que no solo el responsable, sino además el encargado se encuentra obligado a garantizar el cumplimiento de obligaciones como la de requerir el consentimiento, no realizar tratamiento para finalidades distintas a las que motivaron la recopilación, de almacenar los datos para posibilitar el ejercicio de los derechos de los titulares, entre otros.

Como se observa, el ordenamiento peruano prevé obligaciones de observar la norma para el encargado en actividades de tratamiento. Sin embargo, no establece alguna obligación de asistencia de aquellos para garantizar que el responsable cumpla con la normativa.

En cambio, en el RGPD sí se prevé dicha obligación en el artículo 28.3, literal h), pues se exige que el encargado pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de la normativa. En virtud de dicha obligación, el encargado debe aportar de manera completa la información sobre el modo en el que se realizó el tratamiento, lo que incluye datos sobre el funcionamiento de los sistemas utilizados, las medidas de seguridad y la forma en la que se conservan los datos (Comité Europeo de Protección de Datos 2020, p.45). De forma complementaria, en virtud de ese mismo literal, los encargados tendrán la obligación de colaborar con el responsable al momento que este último realice inspecciones de cumplimiento al garantizar acceso a los sistemas e instalaciones del encargado.

Adicionalmente, existen otras obligaciones previstas en el artículo 28.3 del RGPD que incentivan la aplicación del principio de responsabilidad proactiva. Por ejemplo, se señala en el literal c) que el encargado tomará las medidas necesarias de conformidad con el artículo 32", artículo por el que se prevé la obligación de velar por la seguridad de la información personal. En virtud de dicha disposición, el encargado no solo se ve obligado a implementar las medidas de seguridad o a realizar revisiones periódicas de las mismas, sino además informarle al responsable sobre las medidas adoptadas para la posterior aprobación de aquellas, así como los informes que contengan el resultado de las revisiones para corroborar que brindan un nivel óptimo de salvaguarda de la información personal.

Otra obligación relevante se trata de la de asistir al responsable en la atención de solicitudes que tengan por objeto el ejercicio de derechos de los titulares de los datos personales establecida en el literal e) del artículo 28 del RGPD. Debe considerarse que el responsable debe asumir como una de sus obligaciones dar respuesta a las solicitudes de ejercicio de derechos ARCO. Para que pueda cumplir con ello, se requiere obligar al encargado a comunicarle sobre las solicitudes que conozca para permitir que el responsable tome conocimiento sobre las mismas. Y, una vez aquellas puedan ser respondidas en forma favorable, se requiere que el encargado cumpla con rectificar, actualizar o suprimir la información que resida en sus bases de datos, así como brindar la copia de los datos requeridos en solicitudes de acceso.

Finalmente, cabe precisar que la obligación del encargado es de asistencia, no implica que los responsables se vean exentos de demostrar el cumplimiento del tratamiento o que dicha obligación sea desplazada al encargado. Por el contrario, el supuesto de que la normativa le exija al encargado colaborar en la demostración del cumplimiento normativo indicará que el responsable contará con recursos necesarios para acreditar dicho cumplimiento. Además, está el hecho de que, así como los encargados cumplen con la obligación de apoyarlos

en dicha labor, los responsables también se encuentran obligados a solicitarles información sobre las condiciones en las que se realice el tratamiento cuando aquellos no cumplan con proporcionarla, pues dicho principio precisamente promueve una actitud espontánea y no meramente pasiva del responsable frente al tratamiento de los encargados.

### 3.4. La privacidad desde el diseño

Como se señaló en la parte histórica del trabajo, la privacidad desde el diseño se trata de un concepto que se vincula con la responsabilidad proactiva, en tanto a partir de aquel el responsable se encuentra obligado a garantizar la protección de datos de terceros desde el diseño de productos o servicios digitales. En este sentido, incentiva a velar por la privacidad de manera anticipada a la ocurrencia de afectaciones a la privacidad de los usuarios, en tanto los productos ofrezcan garantías de privacidad en favor de los usuarios incluso antes de que los productos o servicios entren en circulación en el mercado (Mato Pacín 2020, p.171). De esta forma, mediante dicho concepto, se promueve una actitud proactiva en los responsables, pues deben asegurar que los dispositivos estén en condiciones para realizar tratamiento debido de información de usuarios.

Ahora bien, pese su importancia para velar por la protección anticipada de la privacidad, todavía no se encuentra desarrollado de manera expresa en la normativa de protección de datos de Perú. En el ámbito nacional, este principio está previsto en el artículo 5 de la Ley de Gobierno Digital como un principio rector. Sin embargo, dicha norma tiene un ámbito de aplicación reducido, pues según su artículo 2 solo se restringe a los sistemas de entidades públicas o a personas jurídicas que se rigen bajo derecho público. Asimismo, en el Nuevo Reglamento de Datos, aquel que también es aplicable a instituciones del sector privado, no se encuentra regulación sobre dicho concepto.

En cambio, el RGPD europeo, norma en la que se inspiró para la regulación del principio de responsabilidad proactiva, entendía que dicho principio se encuentra no distanciado, sino ligado a la noción de “privacy by design”. En este sentido, el considerando 78 no solo se limita a establecer que los fabricantes elaboren productos que no comprometan la privacidad de los usuarios, sino que indica que, “para demostrar conformidad con el Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que garanticen la protección de datos desde el diseño”. A partir de ello, se entiende que la obligación de aplicar medidas de cumplimiento no se separa de la idea de garantizar privacidad desde el diseño, en tanto el responsable puede demostrar el cumplimiento de la normativa si acredita que el diseño de dispositivos emplea métodos de minimización del tratamiento y anonimización de datos.

Asimismo, cabe resaltar que el propio considerando 78 estipula que, en la adopción de políticas internas y en la aplicación de medidas de cumplimiento, estas deben cumplir en particular con los “principios de protección de datos desde el diseño y por defecto”. A partir de la referencia de los “principios” de privacidad desde el diseño, se aprecia que el RGPD reconoce jurídicamente el valor jurídico de las 7 premisas establecidas por la excomisionada Ann

Cavoukian en su escrito “Privacy by Design:7 Foundational Principles” y que fueron explicadas previamente en la primera parte del trabajo: a) proactividad, no reactividad, b) privacidad por defecto, c) privacidad incrustada en el diseño, d) suma positiva, e) seguridad de extremo a extremo, f) visibilidad y transparencia y g) respeto a la privacidad del usuario.

Además, el RGPD sí regula dicho concepto en el artículo 25.1. A partir de dicho artículo, se dispone que “el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas”. Dicha consigna, entendida sistemáticamente con el artículo 24, implica que el responsable no solo debe cumplir con la normativa durante el tratamiento, sino además en un momento previo, en este caso la elección de los sistemas en los que este se llevará a cabo (Martínez Martínez, 2018, p.16). Y para ello, se requiere que los responsables evalúen la idoneidad de dichos sistemas, en tanto la privacidad esté incrustada en su arquitectura y que la configuración predeterminada pretenda tratar el mínimo número posible de datos.

Adicionalmente, el artículo 25.1 establece determinados parámetros para la aplicación de dicho principio. Dentro de ellos, están los ya establecidos en el artículo 24 en lo referido a la responsabilidad proactiva como “la naturaleza, el ámbito, contexto y fines del tratamiento” o “los riesgos de diversa probabilidad y gravedad para los derechos y libertades de personas físicas”. Sin embargo, aparte de los ya señalados, prevé otros como “el estado de la técnica” y “el coste de aplicación”. Mientras que el primero alude al deber del responsable a estar atento a las novedades tecnológicas que garanticen la eficacia de la protección de la privacidad, el segundo se refiere a la capacidad de soportar los costos para velar por la privacidad en el diseño, aquellos que pueden ser no solo económicos, sino también logísticos o de personal (Gil Miñano, 2020, p.33).

Aparte de lo ya señalado, debe destacarse que en el artículo 25.1 se hace particular énfasis a la minimización y a la seudonimización de los datos personales. En cuanto a la minimización, deriva del principio de minimización de datos establecido en el artículo 5 del RGPD, aquel que se refiere a que el responsable debe de abstenerse de obtener o utilizar datos que no sean necesarios para alcanzar la finalidad del tratamiento (De Miguel Asensio, 2024, p.4). Y, en lo que refiere a la seudonimización, esta herramienta es útil para una reutilización de datos, recurrentemente para fines estadísticos, pues con ello se garantiza la disociación (González, 2017, p.122). Por la seudonimización, se logra separar la información obtenida de su titular, de forma que la información se establezca a partir de patrones no relacionados con dicha información.

Cabe señalar que, para la disociación de los datos, no solo se puede acudir a la técnica de disociación, sino además a la técnica de la anonimización de datos. La diferencia entre ambas estriba en el hecho de que, cuando se acude a la seudonimización, el titular pueda ser reidentificado si se obtiene información adicional, lo que en la anonimización no resulta posible, en tanto la disociación sea absoluta e irreversible (Polo Roca, 2021, p. 20). Ello es importante señalar,

puesto que influye en la forma en la que el responsable deba probar la eficacia del método de disociación.

Al respecto, debe destacarse que, mientras que para el caso de la seudonimización, el responsable debe demostrar que no exista posibilidad de reidentificación alguna sin información adicional mediante ciertas garantías como no emplear una misma clave de cifrado para todos los datos o no guardar claves frente a bases que se pueden descifrar, para el caso de la anonimización se requerirá probar la robustez de las técnicas informáticas para impedir que pueda existir riesgo alguno de reidentificación sobre los datos (Comunidad de Madrid, 2023, p.5).

Ahora bien, en lo referido al artículo 25.2, ya no solo se alude a la privacidad desde el diseño, sino más bien a la privacidad por defecto. La distinción entre ambos conceptos parte del hecho de que, si la privacidad desde el diseño implica la integración de la privacidad en los sistemas o dispositivos de tratamiento de datos personales, la privacidad por defecto conlleva a que, dentro de las diversas alternativas de tratamiento, se opte por la más respetuosa al usuario, salvo que este último manifieste lo contrario (AEPD, 2019, p.8). En este sentido, el responsable del tratamiento debe optar por una configuración predeterminada que respete el derecho de cada usuario al control sobre el tratamiento de su información personal.

En esta línea, debe resaltarse sobre la privacidad por defecto que, tal como se estipula en el artículo 25.2, el responsable debe asegurar que "solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento". Como se aprecia de lo señalado, la privacidad por defecto también se vincula con el principio de minimización de datos, en tanto solo deben tratarse aquellos datos que sean esenciales para las finalidades del tratamiento. Sobre el particular, existen algunos parámetros que deben cumplirse para aplicar el concepto de privacidad por defecto: a) la cantidad de datos personales recogidos, b) la extensión del tratamiento, c) su plazo de conservación y d) su accesibilidad. Al respecto, el Comité Europeo de Protección de Datos señala lo siguiente (2019, p.13):

- Cantidad de datos personales: los responsables deben tener en cuenta el volumen de datos y el tipo de datos que se recopilen. En caso se recopile un nivel inmenso de datos, lo recomendable sería que el propio responsable evalúe cuáles son los datos esenciales para alcanzar la finalidad concreta, de forma tal que se cumpla con retirar de los sistemas aquellos que son prescindibles para el fin del tratamiento.
- La extensión de su tratamiento: los responsables deben considerar que no solo los datos que se recopilen deben resultar necesarios, sino además que las operaciones que se realicen con ellos también deberían serlo. Por ello, está la obligación de abstenerse a implementar cualquier operación que exceda la finalidad.
- Su plazo de conservación: la configuración predeterminada de los sistemas debe garantizar que los datos no se almacenen en ellos más allá

del plazo que resulte necesario. En este sentido, los datos deben ser suprimidos o anonimizados de manera automática cuando transcurra el plazo.

- Su accesibilidad: el responsable del tratamiento tiene la obligación de controlar quiénes tienen acceso a los datos personales y a qué tipo de datos. Asimismo, debe garantizar que el titular de los datos intervenir antes de que sus datos sean de acceso público, situación en la que conviene que el propio titular pueda configurar el acceso a los mismos.

Finalmente, cabe especificar que, tanto en lo que respecta a la aplicación de los conceptos de privacidad por diseño y privacidad por defecto, los fabricantes podrán tomar en consideración dichos conceptos en la elaboración de productos o prestación de servicios tecnológicos para permitir a los responsables cumplir con la normativa en materia de protección de datos personales, tal como se alude en el considerando 78 del RGPD (Gil Miñano, 2020, p.33). No obstante, el responsable del tratamiento, tal como se reconoce en el artículo 25, es el sujeto obligado a observar la privacidad por diseño y por defecto es el responsable, puesto que no solo él es quien contrata los sistemas o dispositivos de tratamiento, sino además ellos son quienes realizan el tratamiento de datos de usuarios en la práctica.

### 3.5. Regulación de mecanismos de responsabilidad proactiva

Ahora bien, en cuanto a garantizar la observancia del principio de responsabilidad proactiva, el RGPD alude a diversos mecanismos a implementar por los responsables del tratamiento. Dentro de ellas, destacan las evaluaciones de impacto, los códigos de conducta, las certificaciones y los registros de actividad de tratamiento. A partir de la implementación de dichos mecanismos y tal como se explicará en este punto del análisis, no solo se ofrecen garantías adecuadas en el tratamiento, sino también sirven de insumos para los responsables para probar la licitud del mismo.

En primer lugar, están las evaluaciones de impacto. Según el artículo 35.1, se trata de un análisis previo al tratamiento en el que se determine el impacto de las operaciones de tratamiento en la privacidad de los titulares de los datos. Ello se complementa con lo establecido en el considerando 77, en tanto que, para la realización de dicho análisis, se exige que previamente el responsable identifique los riesgos que puedan generar las operaciones a las que se someten a tratamiento, para posteriormente determinar el origen, la naturaleza, la probabilidad y la gravedad de los mismos. De esta forma, el responsable no solo se ve incentivado a prever posibles riesgos, sino además que, mediante la evaluación respectiva, el responsable se encuentra en mejores condiciones para decidir si se aceptan, se evitan o se mitigan los riesgos (Gadea Soler, 2020 p.50).

Asimismo, existen dos objetivos detrás de la implementación de dichas evaluaciones. Por un lado, contribuyen a fomentar una protección de datos más activa por parte del responsable y, por otro lado, permite evitar posibles daños a la reputación e imagen institucional por tratamiento inadecuado de información personal (Puyol, 2018, p.9). Ello se relaciona particularmente con la

responsabilidad proactiva, pues promueve a que el responsable se anticipe a los riesgos al tener la obligación de identificarlos y analizarlos previamente para evitar incurrir en posibles infracciones. Cabe señalar que la utilización de dichas evaluaciones permite demostrar que se adoptaron medidas adecuadas para el cumplimiento normativo.

Por otro lado, debe tomarse en cuenta que dichas evaluaciones centran el foco de análisis en las operaciones del tratamiento. Tal como se detalla en el apartado 1 del artículo 35 contempla que la evaluación pueda incidir sobre una única operación o pueda abarcar múltiples operaciones similares entre ellas, ello siempre y cuando se emplee tecnología similar de recopilación de datos utilizados para los mismos fines de operaciones anteriores (GT29, 2017, p.8).

El escenario previamente señalado ocurre en casos en los que se pretenda instalar un sistema de videovigilancia dentro de varias instalaciones de una empresa bajo el único propósito de supervisar a los trabajadores de la empresa. Además, aparte del control de operaciones, el apartado 1 del artículo 35 enfatiza en que una evaluación de impacto también puede girar sobre la introducción de nuevas tecnologías, supuesto útil cuando no se tenga certeza de la repercusión de dichas tecnologías sobre los derechos de los titulares (AEPD, 2021, p.13).

Aparte de los aspectos ya señalados, está el hecho de que el propio artículo 35 estipule supuestos en los que resulte necesario acudir a una evaluación de impacto cuando se proceden a realizar las siguientes actividades: a) evaluación exhaustiva de datos por medios automatizados, b) tratamiento a gran escala de datos personales de categoría especial (artículo 9) o de aquellos relativos a condenas penales o infracciones, y c) observación sistemática de datos a gran escala en zonas de acceso público. Sobre dichos supuestos, el GT29 establece las siguientes consideraciones (2017, p.10):

a) La evaluación exhaustiva de datos por medios automatizados se vincula con la elaboración de perfiles, método a partir del que se analiza información proveniente de la situación o del comportamiento de los usuarios para el ofrecimiento de servicios diversos, tal como podría ser cuando un hospital pretende realizar pruebas personalizadas a sus pacientes para predecir posibles contagios o con los perfiles que se elaboran sobre los consumidores para a partir de su actividad en línea brindarles publicidad personalizada.

   Asimismo, la evaluación también puede implicar la toma de decisiones con efectos excluyentes, tal como los bancos respecto a evaluaciones crediticias en las que, a partir de historial de deudas, se determine si el cliente está apto o no para recibir el préstamo

b) En cuanto a los tratamientos sobre categorías especiales, debe advertirse que el tratamiento se considerará de riesgo elevado cuando involucre recopilación y procesamiento de los siguientes datos personales: opiniones políticas, convicciones religiosas o filosóficas, origen racial, afiliación, información financiera o aquella vinculada

tanto a la salud como a la vida sexual de las personas. Asimismo, están los datos relacionados con condenas o infracciones penales.

El tratamiento de dichos datos puede revestir de riesgo elevado, en tanto puedan afectar a derechos fundamentales, tal como el caso de no discriminación por opiniones políticas o convicciones religiosas; así como por las graves repercusiones a la vida cotidiana de los titulares de los datos si aquellos son tratados de manera indebida, tal como en el caso de filtración de datos bancarios que permitan el uso indebido de hackers para la comisión de fraudes.

c) Sobre la observación sistemática en zonas de acceso público, se entiende que este tratamiento se enfoca en el monitoreo de las personas supervisadas en sitios o espacios abiertos.

   Este escenario suele ocurrir en el caso de videovigilancia de los individuos en parques o plazas por parte de autoridades policiales para velar por la seguridad ciudadana. Este tratamiento se entiende de particular riesgo, pues los propios titulares de los datos pueden no ser conscientes de cómo se recopilan los datos o de siquiera evitar su recopilación cuando transiten por los espacios supervisados.

Cabe señalar que, para el caso de las evaluaciones de impacto, se requiere que el tratamiento de datos sea “a gran escala”. Al respecto, si bien la norma en cuestión no especifica sobre lo que se deba entender por dicho término, el GT29 también especifica que, para que el tratamiento pueda ser considerado como tal, se debe tomar en cuenta factores como el número de titulares afectados, el volumen de los datos o la variedad en relación a los tipos de datos, la duración y alcance geográfico de la actividad de tratamiento (2017, p.11). Un ejemplo de este tipo de tratamiento es el del banco, pues contiene información sobre miles de clientes, utiliza datos tanto identificativos (ej. nombre o DNI) como financieros (ej. números de cuentas o ingresos) o biométricos (ej. reconocimiento facial para autentificación), esos datos se conservan durante toda la relación contractual con la institución y el tratamiento suele cubrir todo el territorio nacional.

Por otro lado, el artículo 35 establece en su apartado 7 el contenido mínimo de las evaluaciones de impacto: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, b) una evaluación de la necesidad y de la proporcionalidad de las operaciones con respecto a la finalidad, c) una evaluación de riesgos para los derechos y libertades de los interesados y d) las medidas previstas para afrontar los riesgos, incluidas garantías, como las medidas de seguridad que garanticen la protección de datos. Para la aplicación de dicho contenido, se debe tomar en cuenta lo siguiente (Gadea Soler, 2020, p.60):

a) Para una descripción detallada, debe indicarse en la evaluación el detalle de las actividades de manipulación de datos personales (captura, filtrado, borrado), los datos tratados, los intervinientes involucrados (responsables, encargados, subencargados) y las

tecnologías con las que se realizará el tratamiento, es decir, los dispositivos o las técnicas relevantes para el tratamiento.

b) En cuanto al análisis de necesidad y proporcionalidad, se requiere, por un lado, asegurar que el tratamiento recaiga sobre aquellos datos que sean estrictamente necesarios para el tratamiento de conformidad con las finalidades previstas. Y por otro, evaluar si la finalidad se pueda alcanzar por otros medios, por ejemplo, a partir de tecnologías menos invasivas o reduciendo el universo de titulares afectados.

c) Para la evaluación de riesgos, se deben identificar amenazas que puedan desencadenar daños potenciales a los titulares respecto al menoscabo de su privacidad, tal como podrían ser el acceso ilegítimo a los datos o su modificación no autorizada, en tanto perjudiquen la confidencialidad como la integridad de la información respectivamente.

d) Las medidas de control a implementar tienen como finalidad mitigar el riesgo identificado. Como ejemplo de medidas, están las de establecer políticas de protección de privacidad en la adquisición de nuevos productos o para atender reclamos de usuarios, el establecimiento de compromisos de confidencialidad con los que tendrán acceso a los datos, capacitación al personal, entre otras.

Ahora bien, este mecanismo también se incorporó al Nuevo Reglamento peruano. En el artículo 2.13, se establece que el propósito de la evaluación es la de realizar un análisis de riesgos del tratamiento, de forma que replica lo estipulado en el artículo 35.1 del RGPD.

Asimismo, en el artículo 40, se establecen supuestos similares de aplicación de la evaluación de impacto a los señalados en el artículo 35.3 del RGPD, pues se prevé que dicha evaluación se realiza en el tratamiento de datos sensibles (supuesto equivalente a los datos de categorías especiales), en la elaboración de perfiles (técnica de tratamiento por medios automatizados) y además en lo referido a al tratamiento de grandes volúmenes de datos (término inspirado en el de “tratamiento a gran escala”). Aparte, también indica como el considerando 75 del RGPD que la evaluación de impacto se emplea para el tratamiento de datos de grupos vulnerables, sean niños o poblaciones indígenas.

Sin embargo, la evaluación de impacto en el Nuevo Reglamento peruano es facultativa de acuerdo con el mismo artículo 40. Ello dista de la regulación del RGPD, puesto que, si bien el artículo 35 no señala explícitamente la obligatoriedad de su implementación, se establece como infracción en el artículo 83.4 el no realizar dicha evaluación.

Sin perjuicio del carácter facultativo, la evaluación de impacto se establece como atenuante en el artículo 125, por lo que incentiva a las organizaciones a anticiparse a los riesgos, aunque bajo la posibilidad de que no se elimine completamente el riesgo (Chávez Bravo, 2025). De esta forma, el Nuevo Reglamento no incentiva a la aplicación de la evaluación mediante sanciones,

sino más bien por medio de incentivos de persuasión como la atenuación de responsabilidad administrativa.

Además, la regulación peruana, en contraste con la adoptada en el RGPD, no ofrece garantías de seguridad jurídica en la realización de dichas evaluaciones. Es más, el Nuevo Reglamento no estipula el contenido mínimo de dicha evaluación, sino que solo se limita a señalar que las evaluaciones se realizarán de acuerdo con los lineamientos establecidos tanto en estándares internacionales como aquellos emitidos por la ANPDP.

Aparte de ello, tampoco prevé la autoridad de control publique una lista sobre las operaciones que requieran evaluaciones de impacto y otra en relación con las operaciones que no requieran dicho tratamiento, así como se prevé en los apartados 4 y 5 del artículo 35 del RGPD, siendo dicha publicación una garantía al responsable para conocer plenamente en qué casos se recomienda recurrir a esta herramienta de gestión de tratamiento de datos.

Ahora bien, aparte de las evaluaciones de impacto, existe otro mecanismo reconocido por el RGPD que fomenta la responsabilidad proactiva, en este caso los códigos de conducta. El artículo 40.1 reconoce que “los códigos están destinados a la correcta aplicación del presente Reglamento”, pero sin brindar una definición específica sobre dicho código.

No obstante, la doctrina europea ha estipulado que dicho código se trata precisamente de un acuerdo de buenas prácticas dentro del seno de una misma organización, sujeto a aprobación por la autoridad competente y que contiene la lista de medidas a partir de las que se logrará la adecuada aplicación de la normativa a las operaciones de tratamiento (Díaz Romeral, 2016, p.1728). Cabe señalar que, una vez con la adhesión al código, los responsables y encargados se comprometen a cumplir lo establecido en él y, por ende, a aplicar las prácticas que este mismo indica.

Además, en relación con dichos códigos, debe constatarse que aquellos son una muestra de autorregulación, pues al ser las propias organizaciones responsables del tratamiento quienes los elaboran de manera voluntaria, se promueve que aquellas establezcan de manera autónoma las reglas que regirán en las actividades del tratamiento (Real Pérez, 2012, p.13). Sin embargo, la autorregulación promovida por dichos códigos no debe ser pura, sino más bien someterse a la corregulación, en tanto deban existir una serie de reglas que garanticen una eficacia mínima de las buenas prácticas definidas por los propios responsables (Ornelas Núñez, 2013, p.19). Precisamente, el RGPD apunta a esto último, pues el propio RGPD establece el contenido de dichos códigos

Respecto al contenido de los códigos, se prevé en el artículo 40.2 del RGPD que todo código debe desarrollar los siguientes aspectos: a) el tratamiento leal y transparente, b) los intereses legítimos perseguidos por los responsables, c) el proceso de recogida de los datos personales, d) la seudonimización de los datos, e) la información proporcionada al público, f) el ejercicio de los derechos de los titulares, g) los aspectos sobre el tratamiento de datos de menores, h) las

medidas de seguridad aplicadas, i) la notificación de violaciones, j) la transferencias y k) los procedimientos de resolución de conflictos entre responsables y titulares.

Mediante dichos requerimientos, se busca precisamente que el responsable pueda diseñar lineamientos para el cumplimiento de la normativa de datos personales. Es más, la obligación de tratamiento leal y transparente, así como la de brindar información proporcionada al público e informar sobre la existencia de un interés legítimo, refieren a que el responsable deberá comunicar bajo un lenguaje sencillo y al mínimo detalle la identidad de los sujetos del tratamiento, la base legitimadora del tratamiento, las operaciones a realizarse y los fines, así como el compromiso de que las condiciones del tratamiento informadas serán ejecutadas en la práctica por el responsable a cargo (Helguero Sainz, 2010, p.1735). Así, el código permite la adecuación de las actividades de tratamiento a la normativa, toda vez que incorpora obligaciones legales como la de informar sobre el tratamiento, así como principios como el de transparencia y lealtad.

En esa misma línea, las especificaciones sobre aplicación de medidas de seguridad o transferencias permiten acreditar que el tratamiento brindado por los responsables otorga garantías suficientes en materia de protección de información personal, como se señala en los artículos 32.3 y 46.2 del RGPD respectivamente. De hecho, los códigos pueden ser empleados para demostrar que el responsable haya implementado medidas de seguridad o, en el caso de transferencias internacionales, probar que existen garantías suficientes para poder llevar a cabo un flujo de datos personales entre países.

De esta forma, los códigos de conducta se vinculan con el principio de responsabilidad demostrada. Como se reconoce en el artículo 24.3 del Reglamento, código se convierte en un elemento de prueba para probar la voluntad de proteger los datos de las personas afectadas por el tratamiento (Serrano Pérez, 2021, p.159).

Por otro lado, está la publicidad de los códigos de conducta establecida en el RGPD. De conformidad con el artículo 40.6, la autoridad competente no solo aprobará los códigos propuestos por las organizaciones responsables del tratamiento de ser conformes con el ordenamiento, sino que además procederá con la publicidad del mismo. Dicha publicidad garantiza que no solo que los sujetos afectados por el tratamiento accedan al contenido del código, sino que además tomen conocimiento sobre el ejercicio de sus derechos y el control sobre sus datos personales (Helguero Sainz, 2010, p.1735).

Por ello, es crucial que en los códigos publicados contengan información sobre la definición de sus derechos y los procedimientos de resolución de conflictos, de forma tal que los titulares puedan formular reclamaciones en el supuesto de haber un tratamiento que incumpla con los parámetros establecidos por la normativa vigente. Así, el código se vuelve instrumento para exigir cumplimiento sobre una norma.

Ahora bien, este mecanismo de responsabilidad proactiva del ordenamiento europeo fue también recogido en el Nuevo Reglamento peruano. Como se estipula en el artículo 59 de dicho reglamento, se establece también que el código se trata de un instrumento de cumplimiento normativo voluntario. Y al igual que en el RGPD europeo, estipula en dicho artículo que la implementación de dicho código permitirá demostrar el cumplimiento de las obligaciones reconocidas normativamente.

Cabe señalar que, a partir del artículo previamente señalado del reglamento peruano, la implementación de dichos códigos también servirá para atenuar la responsabilidad Dicha disposición similar a la del artículo 83.2 del RGPD europeo cuando se señala que, para la imposición de las multas, uno de los factores para atenuar la responsabilidad administrativa del responsable en caso de incurrir en infracciones.

Además, el artículo 60 del Nuevo Reglamento peruano prevé requisitos en el contenido similares a los del artículo 40 del RGPD europeo. Por un lado, están aquellas por las que los responsables se comprometen a cumplir la normativa de datos, tales como las disposiciones de cumplimiento de los principios de la normativa, el establecimiento de procedimientos para el ejercicio de los derechos o la determinación de transferencias nacionales como internacionales. Y por otro, existe otro contenido exigido por el mismo artículo para la demostración del cumplimiento, tales como las cláusulas para informar a los titulares sobre el tratamiento respectivo, las cláusulas para obtención del consentimiento en caso de transferencias, los formatos para las reclamaciones por ejercicio de derechos ARCO o para la contratación de encargados del tratamiento.

A pesar de dichas similitudes entre el Nuevo Reglamento peruano y el RGPD europeo. En primer lugar, se señala en el artículo 58 de la norma peruana que los códigos pueden formularse de manera sectorial por organizaciones representativas del mismo. En cambio, en el caso del artículo 40.1 del RGPD, se redactarán los códigos de acuerdo con el sector y en base a las necesidades de las micro, pequeñas y medianas empresas, razón por la que la normativa europea reconoce que la diferenciación en la elaboración de códigos no solo debe limitarse a la identificación del sector, sino además del tamaño de la empresa. Además, tampoco se estipula, como en el caso europeo, la publicidad de los códigos de conducta en el reglamento peruano, por lo que los titulares del tratamiento no podrán conocer ni mucho menos exigir el cumplimiento del contenido de los códigos a las entidades que los elaboraron.

Sin embargo, la diferencia más notoria radica en la supervisión del cumplimiento del código. En el artículo 59 del Nuevo Reglamento peruano, solo se señala de manera general que la organización que elabora el código deberá estipular en él mecanismos de supervisión. No obstante, el artículo 41 del RGPD prevé mecanismos concretos como la adopción de procedimientos de evaluación de cumplimiento o la implementación de aquellos para tramitar responsabilidades por vulneraciones al código (Miralles López, 2019, p.17).

Asimismo, según el artículo previamente señalado, se prevé que el agente designado por la organización redactora del código para supervisar su aplicación se someta a una evaluación previa ante la autoridad competente para acreditar que cuenta con la pericia e independencia requeridas para la supervisión del código. E incluso la autoridad competente procede con la revocación de la acreditación si el agente no desempeña sus labores (Roig Batalla, 2017, p.8). Por tanto, el marco de supervisión en el ordenamiento europeo se encuentra detallada y rigurosamente regulado en el RGPD en comparación con el Nuevo Reglamento peruano.

Finalmente, existen otros mecanismos a partir de los que se puede aplicar el principio de responsabilidad proactiva reconocidos en el RGPD y que no fueron incorporados al Nuevo Reglamento peruano. Por ejemplo, está el caso de la figura de la certificación. En el ámbito de dicha certificación, el reglamento europeo contempla la aplicación de sellos o marcas de protección de datos, a partir de los que se busca demostrar que tanto los responsables como los encargados del tratamiento cumplen con la normativa vigente, como se prevé en el artículo 42 del RGPD (Jiménez Asensio, 2019, p.354).

En este sentido, las certificaciones, al igual que los códigos de conducta, sirven para acreditar el cumplimiento de obligaciones legales, así como también para probar la observancia del principio de privacidad por diseño, tal como se prevé en el artículo 25.3 (Miralles López, 2019, p.19). De esta forma, las certificaciones brindan garantías de protección de datos mediante equipos informáticos y procesos idóneos para el tratamiento de la información personal.

En cuanto a las certificaciones, debe tomarse en cuenta ciertas consideraciones adicionales. Dichas certificaciones son de carácter voluntario y que deben ser aprobados por una entidad independiente a la organización interesada, ya sea la autoridad con competencia nacional en materia de protección de datos u otro organismo de certificación acreditado por la autoridad para otorgar el sello o marca de privacidad respectiva.

Además, se promueve dentro del Derecho europeo el uso de dichas certificaciones, pues aparte de acreditar cumplimiento, sirven para que los titulares de los datos evalúen previamente el nivel de protección a la privacidad ofrecidos por las empresas de los productos y servicios correspondientes (Viguri Cordero, 2018, p.7). Sin embargo, a pesar de dichos beneficios, el responsable no se encuentra exonerado de posteriores fiscalizaciones o eventual responsabilidad por incumplimiento del RGPD, tal como se estipula en el artículo 42.

Finalmente, están los registros de actividades de tratamiento. En virtud del artículo 30 del RGPD, se contempla, en caso se trate de entidades o empresas de más de 250 trabajadores, la obligación de elaborar y mantener una constancia de las operaciones del tratamiento en los que deben figurar los datos de contacto del responsable, los fines de tratamiento, la categoría de los datos y operaciones de tratamiento, los sujetos a los que se les comunicarán los datos personales y las medidas de seguridad a implementar. Estos registros constituyen

efectivamente, como señala Sanz Marco, la piedra angular del principio de responsabilidad proactiva, pues de lo señalado en el registro se podrán proporcionar evidencias del cumplimiento del RGPD en todo momento (2018, p.251).

Respecto a dichos registros, debe señalarse que dicho registro no se trata de uno de ficheros, sino de uno de tratamientos. Ello pues, en contraste con los registros de ficheros, los de actividades no se centran en la obligación de notificar a la autoridad en materia de protección de datos personales dónde o en qué soporte se almacena la información, sino más bien qué operaciones se realizan con los datos y qué medidas son empleadas para mitigar los riesgos que puedan ocasionar dichas operaciones (Jiménez Asensio, 2019, p.19). De esta forma, los registros de actividades no son meros documentos de trámite a partir de los que se le señala a la autoridad la ubicación de los datos, sino que se emplean como instrumento de gestión de datos personales.

Por último, cabe señalar que, a diferencia del ordenamiento europeo, el Nuevo Reglamento peruano no incorpora algún registro similar al establecido en el artículo 30 del RGPD. Si bien en el artículo 43 estipula que deben inscribirse tanto los bancos de datos de administración pública como aquellos de administración pública ante el Registro Nacional de Protección de Datos Personales, precisamente dicha obligación se enfoca en el registro de un banco, es decir el soporte en el que se almacena la información, en lugar de los tratamientos realizados en ellos. Por tanto, en el ordenamiento peruano todavía subsiste el trámite de declarar ante la autoridad los archivos en los que la información se encuentra almacenada.

## 4. Desafíos jurídicos derivados de la inclusión de la responsabilidad proactiva a la luz del Nuevo Reglamento

A partir del Nuevo Reglamento peruano, como se ha comentado previamente, se incorpora el principio de responsabilidad proactiva en el ordenamiento nacional por medio del artículo IX del Título Preliminar. Asimismo, cabe resaltar que dicho principio se incluyó por inspiración en la regulación europea, puesto que, al igual que los artículos 5 y 24 del RGPD, comprende igualmente dentro de su definición la obligación de aplicar medidas de cumplimiento o de demostrar la observancia de la normativa en materia. Por medio de dichas obligaciones y como se había desarrollado previamente, adopta un marco de protección de datos que no solo se restrinja a la obediencia del ordenamiento, sino que además implique la previsión de futuros riesgos y la acreditación de manera espontánea de la implementación de medidas de cumplimiento normativo.

No obstante, pese a la utilidad de la inclusión de dicho principio para garantizar una actitud proactiva en la gestión del tratamiento de la información personal, la incorporación de dicha figura deriva en determinados desafíos a afrontar en el ámbito jurídico: a) El carácter abierto del concepto de responsabilidad proactiva, b) la inversión de la carga de la prueba y presunción de licitud detrás de la obligación de demostración del cumplimiento, c) la transición de un modelo de gestión a un modelo de responsabilidad, d) la necesidad de incorporar

responsabilidad proactiva en la supervisión del tratamiento de terceros y el deber de colaboración de dichos terceros, e) la implementación de los mecanismos de autorregulación en el entorno nacional. A continuación, se procederá a explicar y desarrollar cada uno de estos puntos.

### 4.1. El carácter abierto del concepto de responsabilidad proactiva

Como se había revisado de la regulación de la definición del principio en el artículo IX del Título Preliminar del Nuevo Reglamento, se prevé expresamente que “se deben aplicar las medidas legales, técnicas y organizativas a fin de garantizar el cumplimiento efectivo de la normativa de protección de datos personales”. Sin embargo, no se especifican cuáles medidas se deben aplicar el responsable.

Asimismo, cuando se señala que el responsable “debe ser capaz de demostrar tal cumplimiento”, no se listan los medios probatorios con los que se acredite la observancia del marco jurídico en lo concerniente a protección de datos personales. En este sentido, el margen de aplicación del principio incorporado a la normativa peruana es de carácter abierto, en tanto los alcances de aplicación del principio no estén plenamente determinados.

Ante dicha circunstancia, el concepto de responsabilidad proactiva, en virtud de la forma en la que se haya configurado en el Nuevo Reglamento, se trataría de un concepto de carácter abierto enmarcado dentro del ámbito de los “conceptos jurídicos indeterminados”. Por concepto jurídico indeterminado, se entiende aquellos que no se establecen de manera precisa e inequívoca, sino más bien de forma ambigua, pues no se determinan claramente sus detalles o en qué consisten (Carbajo Cobos, 2020, p.765). Ello ocurre efectivamente en la delimitación del término de responsabilidad proactiva en el Nuevo Reglamento, pues se limita a exigir implementación de medidas y demostración del cumplimiento, pero sin detallar la forma en la que el responsable deberá hacerlo.

Además, está el hecho de que dichos conceptos pueden contener una textura abierta, es decir, una zona de penumbra o incertidumbre en la que resulta muy difícil discernir si la subsunción del supuesto de hecho en el concepto es factible (Estepa Montero 2022, p.76). Ello podría evidenciarse en la posible aplicación del principio de responsabilidad proactiva, pues, así como está establecido en el Nuevo Reglamento, se entiende que deben adoptarse medidas adecuadas para garantizar el cumplimiento de la normativa, pero sin señalarse de manera expresa qué medidas debe adoptar el responsable del tratamiento. Ahí es donde radica la zona de penumbra.

Adicionalmente, debe tomarse en cuenta que todo concepto indeterminado cumple con una determinada estructura: 1) la existencia de un núcleo fijo o zona de certeza positiva, 2) zona de penumbra o de incertidumbre y 3) una zona de certeza negativa. Por certeza positiva se refiere a lo que el sujeto está obligado a hacer, por zona de penumbra el elemento que no está previamente delimitado, y por certeza negativa, lo que el individuo se encuentra prohibido de hacer o no hacer (Cassagne, 2009, p.88).

Los elementos señalados están en la regulación de dicho principio en el artículo IX del Título Preliminar, y del artículo se comprende con claridad que el responsable debe implementar medidas de cumplimiento y a demostrarlo (zona de certeza positiva), por lo que a dicho responsable se le prohíbe omitir la aplicación de medidas y abstenerse de obtener los medios necesarios para probar el cumplimiento (zona de certeza negativa). Y en este caso, la zona de penumbra radica en la forma en la que se debe probar o en la falta de precisión sobre las medidas a aplicar.

En esa misma línea, se desprende de los conceptos jurídicos determinados que precisamente la falta de determinación de los mismos impide su aplicación mecánica. No obstante, esta particularidad es relevante, puesto que ello implica que la indeterminación en cuestión aluda a una realidad que no es factible de abarcar en un solo enunciado, de forma tal que dicha indeterminación deba entenderse en virtud del momento de su aplicación (Zegarra Valdivia, 2016, p.701). Por ello, dicho principio debe ser entendido no de forma estática, sino más bien y flexible, en tanto su aplicación pueda adaptarse a las circunstancias del contexto específico. Así, el responsable deberá evaluar la pertinencia de la medida a aplicar de acuerdo con sus circunstancias particulares.

En esa misma línea, en lo que concierne al principio de responsabilidad proactiva, debe señalarse que es imposible establecer un listado específico de medidas, pues el avance de la tecnología supera a lo establecido para un período o situación específica (Cavoukian 2009, p.1). De esta forma, se contempla que en virtud de dicho principio se pueda exigir la aplicación de medidas sin establecer cuáles, pues el cambio tecnológico obliga a que los responsables del tratamiento no se limiten a implementar medidas estipuladas expresamente en la normativa, en tanto puedan surgir nuevas tecnologías. Ello podría manifestarse con el surgimiento de la toma de decisiones automatizada por medio de algoritmos en los últimos años, lo que obliga a las empresas o entidades públicas emplear auditorías ya no solo el tratamiento de datos de sus trabajadores, sino además por aquel realizado por dichos algoritmos.

De manera adicional, en virtud de la infinidad de casos que se presentan en la realidad, el legislador no puede regularlo todo con precisión y detalle, en tanto se requerirá que el legislador pueda conocer de antemano todos los casos concretos de cada uno de los administrados (Desdentado Daroca, 1997, citado en Zegarra Valdivia 2006, p.42).

Este aspecto es importante resaltarlo, pues, para la aplicación de un principio como el de responsabilidad proactiva, debe evaluarse cuál es la situación actual de cada uno de los administrados. Por ejemplo, en el caso de empresas del sector salud se priorizará la protección en el cifrado extremo por el hecho de que traten datos sensibles. Sin embargo, en hoteles o restaurantes, al ser espacios de concurrencia públicos, la protección se centrará más en políticas de videovigilancia en lugar de la custodia de datos, puesto que a diferencia de las empresas de salud no tienden a tratar datos sensibles. Por ello, como señala

Qurioga León, las medidas a implementar tienen que adaptarse al modelo o diseño de negocio de cada empresa (2021, p.16).

Ahora bien, en lo que respecta a la falta de precisión, también habría que señalar que aquella puede colisionar con la seguridad jurídica, aquel que implica precisamente el principio por el que se exige que las normas sean claras, de forma tal que los ciudadanos sepan a qué atenerse (Rodríguez-Arana, 2007, p.254). Precisamente, a partir de la inclusión de la responsabilidad proactiva, cabe cuestionar que el artículo IX del Título Preliminar se limite a señalar qué es lo que se busca con ese principio (el cumplimiento y la probanza del mismo), pero no cómo se alcanza el mismo (en este caso, las medidas a implementar). Por ello, los responsables no tendrán certeza en virtud del enunciado normativo la forma específica en la que se aplicará el principio.

Sin embargo, no considero que el reconocimiento de la zona de incertidumbre detrás del principio de responsabilidad proactiva devenga en una estricta e inquebrantable protección de la seguridad jurídica. De hecho, lo que suele ocurrir con conceptos como el de responsabilidad proactiva es que no determinan de antemano la acción a adoptar, sino que asignan al destinatario el poder y deber de proponer dicha acción (Lifante Vidal, 2020, p.136). En este sentido, el artículo IX deriva el deber al responsable de determinar cuál es la medida más idónea para garantizar el cumplimiento y qué medios probatorios empleará para acreditar dicho cumplimiento.

Dicha situación, lejos de ser perjudicial para la concreción del principio, dicha incertidumbre fomenta efectivamente el surgimiento de un nuevo paradigma del responsable con iniciativa, diligente y que no se limite a incumplir una norma por el hecho de que la solución no se encuentre establecida en ella (Piñar Mañas et al., 2016, p.465). Así, el responsable ya no se restringirá a subsumir la norma, sino más bien a proponer espontánea y rigurosamente medidas para evitar nuevos riesgos.

Por otro lado, debe velarse por mantener el carácter abierto del principio, toda vez que garantiza la accesibilidad de sus destinatarios. Es decir, si las normas establecen de manera específica qué acciones o qué medidas implementar para cumplirlas, lo más probable es que las medidas establecidas no puedan ser ejecutadas por la totalidad de sujetos obligados (Lifante Vidal, 2020, p.143).

En materia de protección de datos, las pequeñas y medianas empresas será complicado si se exigen complejos sistemas de control de acceso o técnicas de anonimización robustas o auditorías algorítmicas para el cumplimiento del principio. No obstante, pueden limitar el acceso a información delicada a través de llaves, pestillos o cuadernos de control (Quiroga León, 2021, p.19). Por ello, la indeterminación sobre la forma en la que se cumplirá el principio garantizará que todas las entidades que realicen tratamiento de datos se encuentren en condiciones para aplicarlo.

Finalmente, cabe indicar que, como lo señala Zegarra Valdivia, dado que la incertidumbre en la aplicación de principios implica un margen de

discrecionalidad por el hecho de que no exista una única razón correcta, se requiere que dicho margen se encuentre no establecido de manera arbitraria, sino que debe estar respaldada con una motivación técnica suficiente y con sustento normativo (2006, p.48). Así, la autoridad competente deberá sustentar si se observa o no dicho principio de acuerdo con el caso preciso al que se pretenda resolver.

Ejemplo de ello está en la Resolución Directoral 655-2022-JUS/DGTAIPD-DPDP, en la que la Autoridad Nacional de Protección de Datos Personales (en adelante, ANPDP) resolvió un caso en el que el personal de la Superintendencia Nacional de Migraciones obtenía copias de reportes migratorios de personas públicas para compartirlas en grupos de Whatsapp con otros empleados. En este caso, la autoridad no solo había determinado que no se habían adoptado las medidas necesarias para evitar dicho incidente, pues había identificado que la información se transfería por el hecho de que las computadoras no contaban con controles de acceso(como se establece en el artículo 51 del Nuevo Reglamento), sino también advirtió que la entidad no logró probar la implementación de dicha medida, pues no había controles de acceso a puertos USB y correos institucionales, soportes que contenían datos personales (2022, p.27). Por ello, la autoridad no solo detalló cuál era la medida aplicable, sino además si el responsable había demostrado efectivamente la aplicación de dicha medida.

### 4.2. La inversión de la carga de la prueba y presunción de licitud detrás de la obligación de demostración del cumplimiento

Como se había señalado previamente, el principio de responsabilidad proactiva establecido en el artículo IX del Título Preliminar del Nuevo Reglamento determina que el responsable no solo debe garantizar el cumplimiento de la normativa a través de la implementación de medidas pertinentes, sino además "ser capaz de demostrar tal cumplimiento". En virtud de dicha obligación, el responsable deberá probar efectivamente que ha cumplido con sus obligaciones legales, de tal forma que exista una rendición de cuentas sobre la observancia de las condiciones mínimas exigidas por la normativa en materia de protección de datos personales en el tratamiento de la información personal de terceros.

Ahora bien, lo particular de dicho principio radica precisamente en el hecho de que genera una inversión de la carga de la prueba. En este caso, lo que se avala es precisamente que, cuando corresponda evaluar el cumplimiento de las obligaciones en el contexto del procedimiento administrativo sancionador, ya no sea la misma autoridad (en el caso peruano, la ANPDP) la encargada de acreditar que el responsable haya incumplido sus obligaciones legales, sino más bien le corresponderá a dicho responsable demostrar su propio cumplimiento (Cañavete Mejías, 2021, p.18). Por tanto, será el propio administrado quien se encuentre obligado a obtener los medios probatorios necesarios para acreditar la licitud del tratamiento.

Al respecto, dentro del ámbito del Derecho Administrativo, un principio de suma relevancia es el de debido procedimiento establecido en los artículos IV.1.2 del Título Preliminar y el 248.2 del TUO de la LPAG. A partir de dicho principio, se

reconoce que, en todo procedimiento, los administrados las garantías para que un procedimiento pueda considerarse justo. Y precisamente dentro de dichas garantías del procedimiento se establece la presunción de inocencia, lo que implica según el Tribunal Constitucional que “no puede trasladarse la carga de la prueba quien precisamente soporta la imputación, pues eso significaría que lo que se sanciona no es lo que está probada en el proceso o procedimiento, sino lo que el imputado, en este caso, no ha podido probar como descargo en defensa de su inocencia” (Expediente 00156-2012-PHC/TC, fundamento 45). Por tanto, la carga de la prueba debe asumirla quien alega la imputación.

En el ámbito administrativo, el principio de presunción de inocencia se conoce como presunción de licitud, a partir del que las entidades deben presumir que los administrados actuaron de conformidad con sus obligaciones mientras no se cuente con evidencia en contrario. Y como señala Morón Urbina, dicha presunción solo cabe romperla si es que la entidad acopia la entidad suficiente sobre los hechos y su autoría ante el contexto de un procedimiento administrativo sancionador (2023, p.464). A partir de lo señalado, se desprende que el principio de presunción de licitud no solo implica tratar al administrado como inocente durante el transcurso del procedimiento, sino además funciona como un criterio de asignación de carga de la prueba, en tanto determine como regla que la carga no debe recaer en el administrado, sino en la Administración.

Además, la presunción de licitud se configura de forma que la obligación de la Administración de probar la responsabilidad del administrado le libera a este último de la necesidad de actuar y defenderse, hasta que la entidad competente presente los medios probatorios necesarios para acreditar la imputación de incumplimiento (Baca Merino, 2020, p.271). En este sentido, se constata que, ante un procedimiento sancionador, se entiende que el administrado no lo que corresponde demostrar los hechos, sino más bien será la autoridad competente quien en la fase instructiva se encargue de realizar todas las actuaciones necesarias para comprobar la culpabilidad del administrado en la comisión la infracción.

A partir de lo ya señalado, se constata que la regla de carga probatoria en el procedimiento administrativo reside en la Administración y no en el administrado. No obstante, está el fenómeno conocido como “inversión de la carga de la prueba”, por medio del que la Administración impone sanción por el hecho de que el individuo no haya acreditado la realización de la conducta exigida (Magide Herrero y González Prada Arriarán, 2020, p.329). Este riesgo es precisamente el que ocurre si se contempla el principio de responsabilidad proactiva para procedimientos administrativos sancionadores ante la ANPDP, ya que por la existencia de la obligación de demostrar el cumplimiento cabe el riesgo de que dicha autoridad impute responsabilidad por no mostrar la documentación que acredite el cumplimiento.

Cabe señalar que dicho fenómeno se sustenta en la carga de la prueba dinámica, es decir, cuando el que prueba no es el que afirma, sino más bien aquel que se encuentre en mejor capacidad de probar el mismo (Bustamante Alarcón, 2001,

p.186). Al respecto, se podría alegar en materia de protección de datos personales que correspondería no a la autoridad, sino al responsable acreditar la eficacia de las medidas de cumplimiento, pues él en mayor medida los procesos internos de tratamiento de la información personal de sus usuarios. Sin embargo, como señala Macassi Zavala y Salazar Ortiz, ello no es posible en vía administrativa, pues atentaría en contra del principio de legalidad, toda vez que el artículo 173 del TUO de la LPAG exige expresamente que la carga de la prueba le corresponde a la autoridad instructora (2020, p.352).

Asimismo, la utilización de la carga de la prueba dinámica vulnera el principio de impulso de oficio. En virtud de dicho principio, estipulado en el artículo IV.1.3 del TUO de la LPAG, implica precisamente que le corresponde a la Administración llevar a cabo cualquier actuación necesaria para el desarrollo del mismo. Dicho principio es relevante en cuanto a la carga de la prueba en procedimientos administrativos, puesto que a través del mismo se desprende la noción de oficialidad de la prueba. Ello implica, como indica Guzmán Napurí, que la Administración se encuentra obligada a adquirir la mayor cantidad de medios o datos posibles para adoptar la decisión (2013, p.524). Por tanto, implicaría una vulneración al mismo si la Administración no adquiere medios probatorios y decide sancionar al administrado por incumplimiento de la normativa solo a partir de las pruebas ofrecidas por este último en el procedimiento.

En virtud de lo ya señalado, cabe desestimar el uso de la carga dinámica de la prueba. Sin perjuicio de ello, a partir del principio de impulso de oficio, la Administración cuenta con la facultad, así como se dispone en el artículo previamente señalado del TUO, de ordenar la práctica de los actos que resulten convenientes para el esclarecimiento de las cuestiones necesarias para resolver, lo que habilita a la entidad a realizar requerimientos de información a los administrados (Maccasi Zavala y Salazar Ortiz, 2020, p.352).

A la luz del principio de responsabilidad proactiva establecido en el Nuevo Reglamento, la ANPDP requerirá al administrado la remisión de información que acredite tanto las medidas de cumplimiento como la eficacia de las mismas. Así, se puede paliar la falta de recursos de la Dirección de Fiscalización e Instrucción (en adelante, DFI) para conocer sobre los procesos internos de cada responsable del tratamiento fiscalizado.

Por ejemplo, está el caso concerniente a la Resolución Directoral 655-2022-JUS/DGTAIPD-DPDP que, como se señaló en el punto anterior, versa sobre un caso en el que se había advertido que reportes migratorios de personajes públicos eran obtenidos por personal de la Superintendencia Nacional de Migraciones. En este caso, la DFI, como autoridad instructora, necesitaba corroborar que la institución en cuestión había implementado medidas de seguridad exigidas para evitar el flujo de información, en este caso los controles de accesos y las gestiones de privilegios sobre los datos personales contenidos en los sistemas informáticos. Y dado a que quien estaba en mejor condición era la administrada por el hecho de que su información estaba en sus sistemas, la ANPDP requirió que se envíe la documentación que contenía dicha información.

Y fue a partir de la misma que se determinó que no se establecían controles para el acceso a reportes migratorios.

Además, en lo referido a la carga probatoria, debe observarse el principio de verdad material, estipulado en el artículo IV.1.11 del Título Preliminar del TUO de la LPAG, aquel que implica que la Administración debe verificar plenamente que los hechos alegados correspondan con la realidad. En virtud de dicho principio, "la Administración no debe contentarse con lo aportado por el administrado, sino que debe actuar para obtener pruebas y averiguar los hechos a partir de los que se alcance la verdad objetiva" (Guzmán Napurí, 2009, p.245). Por ello, en el ámbito de la aplicación del principio de la responsabilidad proactiva, no solo se requiere que la ANPDP reciba la documentación de los administrados en los que se acredita el cumplimiento de la normativa, sino también se requiere que la Administración revise si es que en efecto dicho cumplimiento se da en la realidad.

Como ejemplo de caso en el que se aplicó el principio de verdad material en materia de protección de datos personales, está el recaído en la Resolución Directoral 1254-2025-JUS/DGTAIPD. En dicho caso, se le abrió un procedimiento administrativo sancionador a un banco por no cumplir con informar aspectos exigidos por el artículo 18 de la LPDP a los clientes de la institución, en este caso, si existían transferencias internacionales y cuáles eran los destinatarios de las mismas. Sobre el particular, la ANPDP advierte que dicho banco cumplió con enviarle un formulario en el que sí se requerían dichos datos. Sin embargo, la entidad, al revisar la página web de la empresa, verificó que el formulario enviado no era el que figuraba en dicha página, sino era otro que no informaba sobre dichos datos (2025, p.29). Por ello, determinó que, en la realidad, dicho administrado no cumplía con el deber de informar.

Por otro lado, resulta crucial relacionar los principios de impulso de oficio y de verdad material con la presunción de licitud del TUO de la LPAG. Por presunción de licitud, el procedimiento sancionador debe partir del hecho de que las conductas de los administrados son lícitas. Y para romper dicha presunción, se deben observar tanto los principios de impulso de oficio como el de veracidad material, toda vez que a la Administración no solo le corresponde impulsar la actividad probatoria, sino además contar con todos los medios posibles para poder alcanzar la verdad objetiva y, de esta forma, plantear una decisión sustentada tanto jurídica como fácticamente (Baca Merino, 2020, p.274). De esta forma, la entidad competente demostrará la responsabilidad del administrado.

En lo concerniente a la aplicación del principio de responsabilidad proactiva, cabe sostener que no debe afectar el principio de presunción de licitud. Sobre el particular, se advierte el riesgo de que la obligación de demostrar el cumplimiento de la normativa puede generar una presunción iuris tantum de incumplimiento, ya que puede interpretarse dicha exigencia de forma que se presuma el incumplimiento del responsable pruebe lo contrario (Martín Faba 2024, p.134). Sin embargo, dicho supuesto es contrario a la presunción de licitud, ya que, aunque el responsable cuente con la posibilidad de desvirtuarla, la autoridad no

debe permitir que la actividad probatoria recaiga únicamente en el responsable, sino además comprobar, en la línea con los principios de impulso de oficio y verdad material, por sus propios medios la culpabilidad de este último.

En relación con la inobservancia del principio de presunción de licitud, está el caso recaído en el Expediente PAS 158-2020-JUS/DGTAIPD-PAS, aquel que involucra a un prospecto de cliente que había sido contactado por una compañía de seguros para promocionar sus programas de salud sin su consentimiento. En dicho caso, la ANPDP señaló en el Informe Final de Instrucción 069-2021-JUS/DGTAIPD-DFI consideraba que el primer contacto tampoco era lícito, pues el número de la persona contactada no había sido obtenido de fuentes de acceso público por el hecho de que la compañía no pudo demostrar lo contrario (ANPDP, 2021, p.16). No obstante, se vulneró el principio de presunción de licitud, dado que la Administración no constató en dicho informe medio probatorio alguno que desvirtúe la ilicitud del primer contacto.

Finalmente, cabe entender que la presunción de licitud no se aplica para la actividad de fiscalización realizada por la DFI respecto al tratamiento realizado por empresas o entidades públicas fiscalizadas. Sin embargo, ello no significa que en la fiscalización se recomiende en el acta de inspección el inicio de un sancionador sin contar con el acervo probatorio suficiente. Al respecto, si bien en la actividad de fiscalización es un procedimiento, las actas deben dictarse en virtud del principio de verdad material, lo que implica que obtendrá todos los medios probatorios que brinden indicios sólidos de incumplimiento (Villegas Vega, 2022, p.170). Por ello, no se puede recomendar el inicio de un sancionador solo por el hecho de que el administrado no haya mostrado la documentación necesaria para cumplir con las obligaciones de la norma.

### 4.3. La transición de un modelo de gestión a un modelo de responsabilidad

El principio de responsabilidad proactiva, como se encuentra estipulado en el artículo IX del Nuevo Reglamento, reside en velar por el cumplimiento espontáneo de la normativa. Sin embargo, como se señaló en la comparativa con el RGPD europeo, no se desprende del principio en el ordenamiento peruano, al menos de manera expresa, que su aplicación no solo debe reducirse velar por la observancia de la normativa, sino que además debe prevalecer un enfoque de prevención de riesgos, dada la obligación del responsable de evaluar de manera previa las contingencias que podrían derivarse de las actividades de tratamiento y, en virtud de dicho análisis, determinar tanto la probabilidad de ocurrencia de dichas contingencias como las medidas de mitigación idóneas.

Para el caso peruano, la falta de previsión expresa sobre un enfoque de prevención de riesgos en lo concerniente a la regulación del principio de responsabilidad proactiva no solo frustra la oportunidad de introducir una aproximación preventiva al principio, sino que además mantiene el tradicional y caduco modelo de gestión de la información. Dicho modelo implica que el responsable garantice el control del cumplimiento de la normativa vigente (Goñi Sein, 2018, como se citó en Zegarra Valdivia, 2019), por lo que en la práctica se

trata de un sistema de “checklist” en el que dicho responsable se limita a verificar si cuenta con los requisitos necesarios para cumplir con el ordenamiento jurídico.

A la luz de dicho modelo, el responsable cumple con la normativa a partir de diversas acciones: la elaboración de formatos de consentimiento, la redacción de políticas de privacidad y la tramitación de registros de bancos de datos. No obstante, el problema radica en el hecho de que, a partir de la implementación de dichas medidas, no existe como tal una gestión de riesgos, sino únicamente de requisitos para poder sujetarse a las exigencias de la legislación en materia de datos personales (Piñar et al, 2016, p.17). Y ello, en efecto, no garantiza la aplicación plena del principio de responsabilidad proactiva, en tanto la aplicación mecánica de la ley impide valorar la idoneidad de las medidas de acuerdo con la probabilidad y el impacto en la privacidad de terceros.

En contraste, el modelo de responsabilidad exige que el responsable no solo controle el cumplimiento de la normativa, sino además analice el surgimiento de posibles contingencias como consecuencia de las actividades de tratamiento. Al respecto, se concibe que al responsable le corresponde la labor de ponderar los tratamientos para evitar riesgos sobre la privacidad y realizar evaluaciones de impacto cuando exista probabilidad de que la afectación a los datos procesados sea elevada (López Calvo, 2019, como se citó en Zegarra Valdivia, 2019). De esta forma, el modelo en cuestión privilegia la anticipación de los riesgos sobre la mera reacción del responsable, toda vez que no se espera a que la autoridad advierta el incumplimiento, sino que el responsable haya podido evaluar el riesgo y mitigarlo mediante la medida correspondiente.

Asimismo, sobre el enfoque de gestión de riesgos, cabe señalar que el responsable no debe restringirse al uso de “checklists de cumplimiento”. Aunque dichas herramientas contribuyan a advertir los requisitos exigidos por la normativa, dicho enfoque requiere también que el responsable reflexione sobre la relación entre los riesgos y las medidas implementadas, la idoneidad de dichas medidas para mitigarlos y aplique una monitorización que permita verificar la evolución del riesgo conforme el transcurso del tiempo (Grupo de Trabajo del Artículo 29, 2014, p.2). En este sentido, el nuevo modelo requiere de responsables que no solo conozcan la norma, sino que además se encuentren en condiciones de fundamentar la pertinencia en la elección de medidas y la mejora continua en la aplicación de las mismas.

Ahora bien, debe tenerse en claro que el modelo de responsabilidad se complementa a partir del ya desarrollado “privacidad desde el diseño”. A partir de dicho concepto, como se había señalado previamente, vela por la prevención, pues se garantiza la protección de datos desde el momento en el que diseñen o se elaboren dispositivos, productos o servicios tecnológicos.

No obstante, pese a la utilidad del concepto, el Nuevo Reglamento peruano opta por no introducirlo. Dicha omisión impide efectivamente la transición a un modelo de responsabilidad, toda vez que no solo permite analizar los riesgos, sino además implementar las configuraciones necesarias para evitarlos, así como monitorear su efectividad en el ciclo de vida del dato (Cavoukian, 2012, p.13).

Sin perjuicio de dicha omisión, la LPDP regula los procedimientos de anonimización y disociación en los artículos 2.14 y 2.15 respectivamente. Para ambos, la ley indica que a partir de ellos se impide la identificación del individuo, solo que la disociación es reversible y la anonimización no.

Como se observa, la ley peruana, a diferencia del RGPD, no contempla el procedimiento de seudonimización en materia de protección de datos personales. Pese a ello, cabe asociar la disociación con la seudonimización, en tanto dicho término implique la separación de la información de la persona a la que pertenezca, pero bajo la posibilidad de reidentificarla, pues no se elimina el dato (Cano Galán, 2020, p.43). Por ello, la disociación, en tanto sea un procedimiento reversible, corresponde considerarlo como seudonimización en el ordenamiento peruano.

No obstante, la inclusión de la anonimización y disociación no basta para plasmar el concepto de privacidad por diseño en la normativa peruana. Por un lado, todavía no se ha reconocido jurídicamente el principio de minimización de datos personales, aquel que como se había explicado previamente, implica el deber del responsable de abstenerse a recoger datos innecesarios para alcanzar la finalidad.

Actualmente, en el ordenamiento peruano ya contempla el principio de calidad en el artículo 8 de la LPDP, aquel que vela que los datos a tratar sean pertinentes y necesarios para el cumplimiento del propósito de su recopilación. Sin embargo, dicho principio se limita a determinar la idoneidad de los datos recopilados, más no a delimitar el volumen máximo de recopilación o la frecuencia en la que deba recopilarse. Por tanto, es necesario que ambos principios se complementen.

Y, por otro lado, para la aplicación de dicho concepto, el responsable no solo debería emplear técnicas de anonimización o seudonimización, sino además debe garantizar que, desde la configuración de aplicaciones, los propios usuarios puedan controlar el tratamiento cuando sea necesario. Para ello, se prevén diversas herramientas en el interfaz de aplicativos que permitan dicho control, ya sea para activar/desactivar mecanismos de seguimiento, cambiar sus preferencias, descargar la información con un solo clic (portabilidad), corregir datos (rectificación) y opciones de borrado (supresión) (AEPD, 2019, p.22). Dichas configuraciones refuerzan el cumplimiento normativo, pues son medidas que vinculan el cumplimiento con la arquitectura del sistema.

Ahora bien, otro tema relevante en lo referido al modelo de responsabilidad es la exigencia de una constante actualización en materia de protección de datos personales. Como señala Zegarra Valdivia, dicho modelo se trata de una respuesta al proceso de transformación tecnológica en los medios en los que se procesan los datos personales, de forma tal que la protección de la información personal deba ceñirse a la irrupción de nuevas tecnologías como el Big Data, la inteligencia artificial y la elaboración de perfiles (2019, p.176). Este contexto de constante avance tecnológico exige efectivamente al responsable una constante innovación en el cumplimiento. Y precisamente dicha innovación implica apartarse del cumplimiento formal de las obligaciones.

En primer lugar, está la observancia del principio de consentimiento. Como se establece en el artículo 5 de la LPDP, se trata de la principal causa de legitimación del tratamiento. Asimismo, se establecen en el artículo 13 de la ley parámetros para la obtención del consentimiento válido, entre ellos que el consentimiento sea libre, previo, expreso e inequívoco e informado. En un modelo formalista del cumplimiento, el responsable procederá a realizar un checklist de todos esos parámetros al limitarse a revisar que en aquellos se incluyan casillas de aceptación y se informe sobre las principales condiciones del tratamiento (Vásquez Rodríguez, 2022, p.32). Bajo dicho sistema, el cumplimiento de la obligación de consentimiento se convierte en una labor mecánica, en tanto el responsable se restrinja a cumplir requisitos formales.

Sin embargo, la mera solicitud del consentimiento deviene en insuficiente para la protección de la información personal ante la irrupción de nuevas tendencias tecnológicas. Actualmente, el sector empresarial recurre a la inteligencia artificial predictiva, aquella que permite por algoritmos inferir los gustos y preferencias de sus clientes a partir del análisis de su actividad o comportamiento en línea (Caicedo Consuegra et al. 2023). Este modelo de negocio incide de forma negativa el cumplimiento de la obligación del obtener consentimiento válido, ya que no resulta factible obtener autorización previa, puesto que las inferencias se generan después del momento de la recolección. Además, tampoco puede exigirse una autorización plenamente informada, ya que ni siquiera quienes diseñan dichos sistemas pueden anticipar qué atributos serán inferidos ni a partir de qué patrones se dará dicha inferencia (Ramos Contreras, 2025, p.84).

Ante dicho escenario, no bastará que el responsable emplee formularios para acreditar el cumplimiento, sino que, en aplicación del enfoque de prevención de riesgos, deberá aplicar evaluaciones de impacto para analizar si es que el diseño de dicho algoritmo está programado para depurar (eliminar) automática de aquellos datos obtenidos irrelevantes para la finalidad consentida por el usuario o para anonimizar dicha información (Gamero Casado y Berning Prieto, 2025, p.75). Asimismo, pese a la dificultad del responsable para prever todas las implicaciones derivadas del tratamiento, lo que se recomienda no solo es informar al usuario de forma previa a la recopilación, sino con posterioridad y de manera periódica sobre el rendimiento de los algoritmos para que tome conocimiento sobre los resultados del algoritmo y, de ser el caso, sugerirle el ejercicio de sus derechos de revocación, oposición o rectificación.

En segundo lugar, está la obligación estipulada en el artículo 18 de la LPDP de informar al titular de los datos sobre el tratamiento. Al respecto, la norma exige informar diversos aspectos, tales como la finalidad del tratamiento, los destinatarios, la existencia del banco, la identidad del titular del banco, las posibles transferencias, entre otros más requerimientos. Asimismo, se prevé en el artículo 7 del Nuevo Reglamento que la publicación de políticas de privacidad son formas de cumplir con dicha obligación. Por tanto, ello implicaría que, en un sistema de mera gestión de cumplimiento, el responsable se restrinja a redactar las políticas y emplear los requerimientos normativos como checklist para verificar que ningún aspecto relevante a informar falte en la política.

No obstante, en un mundo cada vez más digital, resulta crucial atender a los patrones oscuros, diseños de interfaz que incitan al usuario a compartir sus datos sin hallarse plenamente informados (Mato Pacín, 2024, p.52). Ejemplos podrían ser el “laberinto de privacidad” (el usuario debe navegar por tantas páginas al punto de ignorar parte de la información proporcionada), “ocultar a primera vista” (cuando por estilo visual, sea por tamaño de letras o color oscuro de interfaz, se esconde información relevante para el tratamiento) o la “redacción ambigua” (utilización de términos difusos al proporcionar información de usuarios) (Gastañaudi Ramírez, 2024, pgs.74-77). Ante la aparición de dichos patrones y para cumplir con el deber de informar, se recomienda a los revisar la interfaz de sus sitios web y erradicar las configuraciones que desinformen a los usuarios sobre el uso de sus datos.

Y en último lugar, está la obligación de registro de banco de datos personales. Hasta ahora, permanece todavía dentro del ordenamiento peruano la obligación de inscribir la creación, la modificación y cancelación de banco de datos en el Registro Nacional de Protección de Datos Personales, registro a cargo de la ANPDP, tal como se dispone en el artículo 29 de la LPDP y en el artículo 43 del Nuevo Reglamento. Además, en ambos artículos se prevé que la finalidad del registro en cuestión es la de garantizar la publicidad de la existencia, finalidad, identidad y domicilio del responsable, el ejercicio de derechos ARCO e incluso la adopción de medidas de seguridad a adoptar.

Ahora bien, respecto a la publicidad de las medidas de seguridad, permite determinar que el responsable ha previsto mecanismos para velar por la confidencialidad de la información de los titulares. Sin embargo, debe tomarse en consideración que, tal como advierte Zegarra Valdivia, esta inscripción no pasa de ser un mero formalismo, ya que en virtud de dicha inscripción no se suele garantizar que los responsables del tratamiento hayan logrado implementar las medidas establecidas en los bancos inscritos (2019, p.184). En este sentido, cabe cuestionar que la obligación de inscripción no brinda garantías reales para la seguridad de datos, en tanto dicha obligación resulte de carácter meramente declarativo y cuya presentación efectiva solo representa el mero cumplimiento de un trámite administrativo.

Cabe señalar que, como se señaló previamente en el artículo, la obligación de registro del Derecho peruano se relaciona con la obligación ya extinta en la Unión Europea de “inscripción de ficheros”, aquellos que también favorecen el conocimiento público de la finalidad, la identificación del responsable y encargado, existencia de transferencias, entre otros más (Pons Buigues, 2017, p.48). No obstante, hasta el RGPD se ha desprendido de dicha obligación y ha preferido la del “registro de actividades”, aquel que implica mantener inventario ya no de bancos, sino de actividades. Ello es relevante, toda vez que ya no se requiere señalar en los registros el fichero al que pertenece la información, sino más bien las actividades que implican el tratamiento de la misma.

Finalmente, cabe señalar que el registro de actividades no solo se reduce únicamente a una forma distinta de organizar la información, sino que también

garantiza en mayor medida la aplicación del principio de responsabilidad proactiva. Por un lado, al tratarse de un documento de gestión interna y no sometida a un procedimiento administrativo previo para su inscripción, deviene en un reflejo de la autosupervisión del propio responsable sobre las actividades de tratamiento. Y por otro, garantizará no solo que las medidas sean adecuadas para los riesgos identificados, sino que también dicho registro puede ser empleado como elemento probatorio para el cumplimiento de la normativa (Estepa Montero, 2022, p.88). Por ello, es pertinente que el ordenamiento peruano sustituya los registros de bancos por los registros de actividades.

### 4.4. La necesidad de incorporar responsabilidad proactiva en la supervisión del tratamiento de terceros

El principio de responsabilidad proactiva, tal como se encuentra previsto en el artículo IX del Nuevo Reglamento, implica la obligación del titular del banco de datos o responsable del tratamiento de garantizar el cumplimiento de la normativa vigente. Sin embargo, debe tomarse en cuenta que cabe la posibilidad de que el responsable no realice directamente el tratamiento, sino que dicho tratamiento sea delegado a un tercero. Ante dicha situación, corresponde al responsable supervisar a dichos terceros para garantizar el cumplimiento normativo dentro de las actividades que estos últimos efectúen.

Al respecto, como se reconoce en la normativa vigente de datos personales, los sujetos que cuentan con la capacidad de control sobre el tratamiento son tanto el titular del banco como el responsable del tratamiento. Sobre el titular, se señala en el artículo 2.17 que “determina la finalidad y contenido del banco de datos personales y sobre el tratamiento de estos”. De manera similar, se prevé en el artículo 2.22 del Nuevo Reglamento que “decide sobre la finalidad y los medios del tratamiento” y que dicha categoría abarca a “cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se realice en un banco de datos personales”. Interpretadas dichas disposiciones de manera sistemática, cabe concluir no solo que ambos tienen control sobre el tratamiento, sino que ambos deciden sobre el tratamiento realizado en un banco de datos (como el titular) o sobre aquel realizado sin contar con él (como el responsable).

Asimismo, es relevante tomar en consideración que tanto el titular como el responsable pueden emplear el poder de decisión no solo para gestionar el tratamiento que efectúen ellos mismos, sino además el efectuado por terceros. Según Durán Cardo, el objetivo de atribuir tanto al titular del fichero (banco) como al responsable la facultad de control sobre el tratamiento es la de poder asignar responsabilidad al sujeto que decide de facto sobre el tratamiento (2015, p.215). Ello es importante a la luz del principio de responsabilidad proactiva, ya que reconoce que, por más que el tratamiento se realice en bancos de datos de terceros, el responsable no se desprende de la obligación de adoptar medidas que garanticen el cumplimiento normativo.

Cabe señalar que, en el caso de actividades de terceros, el responsable podrá adoptar diversas medidas de cumplimiento. Por un lado, podrá estipular en los contratos de encargo instrucciones para aplicar la normativa en sus actividades

de tratamiento y para ordenar la implementación de medidas de cumplimiento correspondientes. Y, por otro, el responsable podrá garantizar en todo momento el cumplimiento de la normativa a partir del monitoreo constante de las actividades de los encargados o terceros subcontratados (Piñar Mañas, 2019, p.165). Así, se requiere que el responsable no solo se restrinja a establecer compromisos contractuales, sino evaluar que en la práctica se cumpla a partir de auditorías, reportes de cumplimiento, entre otros mecanismos.

Sin embargo, como se señaló en la sección de “responsabilidad proactiva sobre actividades de terceros”, el problema en la práctica estiba en el hecho de que el artículo IX del Título Preliminar no reconoce expresamente que el responsable se encargará del cumplimiento de las obligaciones del tratamiento que realice por sí mismo o bajo su dirección, tal como se estipula expresamente en el considerando 74 del RGPD. Ello traería como consecuencia el hecho de que los responsables no implementen medidas para vigilar a los terceros, lo que implicaría no asumir responsabilidad efectiva sobre sus actividades de tratamiento.

En la práctica, dicho problema podría generar que los terceros incurran en infracciones por la falta de supervisión de los responsables. Como caso de ejemplo, está el del Expediente PAS 158-2020-JUS/DGTAIPD-PAS. En dicho caso, una aseguradora requirió la contratación de diversos call centers para realizar llamadas promocionales. Un prospecto denunció haber sido contactado sin su consentimiento, pese a que en una primera llamada había manifestado su negativa a recibir publicidad. Lo que verificó la ANPDP no solo fue que los call centers incurrieron en la infracción de realizar tratamiento de datos sin consentimiento, sino que, además la aseguradora no cumplió con ejercer un control diligente sobre las actividades de los call centers al no solicitar reportes de la denegatoria de consentimiento (Resolución Directoral 3439-2021-JUS/DGTAIPD-DPDP, fundamento 105). En consecuencia, la ANPDP le atribuyó responsabilidad a la aseguradora por la infracción cometida.

Al respecto, cabría señalar que en principio no corresponde atribuir responsabilidad a administrados por actuaciones de terceros, puesto que por principio de causalidad solo correspondería atribuir a quien incurrió en la conducta infractora, más no en un tercero (Guzmán Napurí, 2013, p.673). Sin embargo, también debe considerarse que dicho principio también implica que la acción u omisión sea idónea y tenga la aptitud suficiente para producir lesión y no tratarse simplemente de un hecho de un tercero (Morón Urbina, 2023, p.459). Por tanto, se tendría que evaluar si es que la omisión de adoptar medidas de supervisión del responsable desencadenó o no la comisión de la infracción de los terceros a su cargo.

En aplicación del criterio al caso señalado, se determinó que la aseguradora no cumplió con adoptar las medidas de supervisión, toda vez que no cumplió con implementar un sistema de comunicación eficiente entre call centers. La ANPDP advirtió que dicho sistema era necesario para prevenir el contacto sin consentimiento, toda vez que el denunciante fue contactado por dos call centers

distintos, situación en la que el segundo optó por contactar nuevamente al cliente por el hecho de desconocer que había denegado su consentimiento ante el primero (Resolución Directoral 3439-2021-JUS/DGTAIPD-DPDP, fundamento 108). Al respecto, la la aseguradora tuvo que haber aplicado sistemas de reportes de incidencias, pues ello hubiera permitido que, ni bien el primer call center le comunicara sobre la denegatoria de la persona contactada, proceda a contactarse con los demás call centers para evitar un segundo contacto.

Adicionalmente, se ha reconocido que resulta necesario la existencia de medios rápidos y eficaces para poner en conocimiento sobre cualquier incidencia ocurrida en el tratamiento, a fin de adoptar las acciones pertinentes para mitigar cualquier situación perjudicial que pudiera vulnerar la privacidad de los usuarios (Opinión Consultiva 01-2022/DGTAIPD, fundamento 45). En este caso, de haberse no solo elaborado, sino además ejecutados protocolos de comunicación de incidencias, la aseguradora hubiera tomado conocimiento de la primera llamada y ordenado el cese del contacto, lo que hubiera permitido mitigar el riesgo de generar llamadas no consentidas.

En base a todo lo señalado y a la luz del presente caso, se debe tomar en cuenta que la falta de previsión normativa de una responsabilidad proactiva para terceros puede desencadenar no solo en que los responsables del tratamiento adopten un rol meramente pasivo frente a las actividades que ellos realicen, sino que además la omisión en la supervisión genera supuestos de incumplimiento. Por tanto, se recomienda que se añada al principio de responsabilidad proactiva regulado en el Nuevo Reglamento que debe garantizarse tanto el cumplimiento del propio responsable como de los encargados y subcontratados que se encuentren a su cargo.

### 4.5. La implementación de los mecanismos de responsabilidad proactiva en el entorno nacional

A partir del Nuevo Reglamento, no se logra introducir el principio de responsabilidad proactiva, sino además dos mecanismos reconocidos expresamente como de responsabilidad proactiva: la evaluación de impacto (artículos 2.13 y 40) y los códigos de conducta (artículos 59 y 60). En virtud de dichos instrumentos, se contempla que los responsables no solo gestionen sus actividades para cumplir con la normativa vigente, sino que además permiten la adecuada gestión de riesgos y la demostración del cumplimiento normativo.

En el caso de la evaluación de impacto, de acuerdo con el artículo 2.13 del Nuevo Reglamento, se debe emplear de forma previa para analizar el impacto del tratamiento o los riesgos que se desprendan del mismo. En la implementación de dichas evaluaciones, se requiere que el responsable contemple las posibles contingencias que pueda generar el tratamiento tras identificarlas y evaluar tanto la gravedad y probabilidad de su ocurrencia (Goñi Stein, 2018, citado en Zegarra Valdivia, 2019).

Al respecto, resulta acertada la inclusión de dicho mecanismo. Como se había mencionado en el apartado previo de “regulación de mecanismos”, garantiza la aplicación del principio de responsabilidad proactiva, pues priorizan la

anticipación frente a los riesgos que podrían generarse en caso de realizar alguna actividad de tratamiento. De esa forma, el responsable puede no solo prever las repercusiones de sus operaciones de tratamiento, sino además evaluar las medidas más idóneas para mitigarlos. Cabe señalar que dichas evaluaciones permiten demostrar el cumplimiento, pues cuentan como evidencia para determinar que el responsable ha tomado las previsiones para evitar riesgos a la privacidad de terceros.

Asimismo, está el hecho de que la implementación de dicho instrumento se trate de una condición atenuante de responsabilidad en procedimientos sancionadores según el artículo 125 del Nuevo Reglamento. Entendiéndose por condición atenuante como aquella que supone la existencia de una menor gravedad de la conducta del infractor (Morón Urbina, 2023, p.536), resulta pertinente incluir a la implementación de dicha evaluación como causal atenuante, dado que su aplicación en las actividades de tratamiento supone que el responsable haya adoptado previamente todas las medidas correspondientes para evitar que se produjera el daño. Como consecuencia, ello fomenta que de manera facultativa los responsables presenten dichas evaluaciones para solicitar disminución de multas.

Sin embargo, cabe discrepar de la regulación establecida en el artículo 40 del Nuevo Reglamento. La implementación de dicho mecanismo no puede resultar facultativa en todos los casos, ya que impediría que el responsable mitigue el impacto de aquellos tratamientos que puedan considerarse de alto riesgo. Como señala Santamaría Ramos, las evaluaciones de impacto no solo se enfocan en garantizar el cumplimiento, sino además a proteger los derechos y libertades de los afectados (2020, p.166). Por tanto, se requerirá emplear dichos instrumentos para no generar desprotección de los derechos de los afectados.

En esta misma línea, el Nuevo Reglamento estipula diversas circunstancias como el tratamiento en grandes volúmenes, el tratamiento de datos sensibles, la creación de perfiles y utilización de información de personas en situación de vulnerabilidad (niños, población indígena, personas con discapacidad). Cabe señalar que a partir de dichos supuestos no solo pueden generarse riesgos exponenciales asociados a la vulneración al derecho de protección de datos, por ejemplo, filtraciones de ingentes cantidades de datos o exposición de información sensible, sino además hacia otros derechos como la igualdad, en tanto la creación de perfiles, en virtud de sesgos de discriminación presentados en algoritmos sobre la edad, raza, etnia, discapacidad entre otras causas. Ante dichas contingencias, corresponde adoptar controles distintos que al de otro tipo de tratamientos. Por ello y solo en esos casos, no debe resultar preferible, sino obligatorio adoptar una evaluación de impacto.

Asimismo, resulta necesario que en el mismo artículo se establezcan otros supuestos de riesgo elevado y en los que, por ende, también corresponderá aplicar la evaluación en cuestión. Por ejemplo, la monitorización mediante el Internet de las Cosas, rastreo de contactos o la geolocalización son tratamientos que pueden entrar dentro de dicha categoría, pues son tratamientos sumamente

intrusivos por recopilar datos de manera continua y en tiempo real, involucrar tratamiento masivo y por el riesgo de comprometer la intimidad de la persona por el registro de su información y actividad en el domicilio (Polo Roca, 2020, p.151). Cabe señalar que las decisiones sin intervención humana también pueden entrar dentro de dicha categoría, ya que pueden condicionar la calidad de vida de vida de las personas al decidir sobre el acceso a servicios.

Ahora bien, otro punto cuestionable de la regulación es la falta de observancia del principio de predictibilidad, aquel que implica que el administrado tenga la certeza sobre lo que se espera de él para acreditar el cumplimiento de la normativa vigente (Guzmán Napurí, 2009, p.248). En lo que respecta al artículo 40 del Reglamento, indica que los responsables podrán realizar evaluaciones de impacto, pero sin establecer el contenido mínimo de dicho instrumento. Ello ocasionaría no solo que los responsables no adquieran conocimiento pleno sobre el contenido esperado en dichas evaluaciones, sino que además tampoco garantizar uniformidad de criterios por parte de la ANPDP para evaluar la idoneidad de las evaluaciones de impacto presentadas por los administrados, sea en el contexto de una fiscalización o de un procedimiento sancionador cuando el responsable la presenta como atenuante.

En este sentido, se recomienda incorporar en el Nuevo Reglamento contenido mínimo para realizar la evaluación de impacto. Dentro del posible contenido, pueden estipularse los ya contemplados en el RGPD de la Unión Europea, tales como la descripción de las operaciones, el análisis de proporcionalidad con respecto a la finalidad, la evaluación de riesgos y libertades y las medidas de mitigación previstas. Si los responsables del tratamiento incorporan dichos requisitos en sus evaluaciones, ello acreditará que no solo comprenden todos los tratamientos, sino que además serán capaces de diseñar medidas relacionadas con la magnitud y la probabilidad del riesgo.

Sin perjuicio de dicho contenido, resulta necesario que la ANPDP cumpla con emitir disposiciones complementarias para orientar a los responsables en la elaboración de dichos mecanismos, como está establecido en el 40.3 del Nuevo Reglamento. Los puntos sobre los que cabe realizar precisiones para garantizar el adecuado diseño de evaluaciones de impacto son los siguientes (AEPD, 2021):

- Parámetros para la evaluación de idoneidad, necesidad y proporcionalidad del tratamiento: para cada etapa del test, existen parámetros a observar. 1) idoneidad (umbral de efectividad del tratamiento y grado de satisfacción de los intereses del responsable), 2) necesidad (determinación de relevancia del tratamiento, limitación a la finalidad, existencia de otros medios con menor riesgo) y proporcionalidad en sentido estricto (identificación del grado de impacto en la privacidad, identificación de beneficios, balance costo-beneficio).

- Matriz impacto x probabilidad: debe especificar la magnitud (bajo, mediano, alto y muy alto), aquella que se medirá de acuerdo con determinados criterios, tales como reversibilidad de los efectos, pérdida

de confidencialidad, suplantación de identidad, afectación al ejercicio de derechos fundamentales. Asimismo, indica también el grado de probabilidad (improbable, baja, alta, muy alta), dependiendo de la frecuencia en la que se materializa el riesgo (nunca, en escasas oportunidades, durante el último año). Por medio de dicha matriz permitirá efectuar el análisis conjunto del impacto y probabilidad para determinar el nivel del riesgo.

- Catálogo de medidas para mitigación de riesgos del tratamiento: debe especificarse la naturaleza de las posibles medidas a aplicar. Pueden clasificarse de la siguiente manera: gobernanza (establecer políticas internas, designar al oficial de protección de datos, capacitaciones al personal), seguridad (control de accesos, cifrados, copias de seguridad) y de protección desde el diseño (depuración de datos innecesarios, anonimización, listas negras anónimas).

- Distinción entre riesgo inherente y residual: el riesgo inherente es aquel que se origina de la actividad de tratamiento antes de la implementación de medidas de mitigación, mientras el residual se trata del riesgo resultante después de la aplicación de medidas. A partir de la determinación de este último riesgo, el responsable podrá decidir si lo asume, si implementa medidas adicionales o si abandona el tratamiento.

Aparte de lo ya señalado, debe destacarse que, conforme al Nuevo Reglamento, no se contempla la posibilidad de solicitar opinión a los principales afectados sobre las particularidades del tratamiento antes de que se lleve a cabo. Ello sería útil, pues de esta forma el responsable podrá obtener una visión completa sobre la forma en la que se verán afectadas las personas cuya información se someta a tratamiento (Gadea Soler, 2020, p.61). Además de promover la participación de los afectados, sino además se atiende al principio de transparencia, puesto que ellos habrán tomado conocimiento del tratamiento incluso desde antes que comience a operar.

Por último, en lo referido a la evaluación de impacto, cabe señalar que tampoco existe la obligación de actualizar la evaluación de impacto en el transcurso del tratamiento. De hecho, la actualización de dicha evaluación deviene en necesaria, en tanto toda operación del tratamiento sea dinámica y se encuentre sujeta a cambios permanentes (Grupo de Trabajo del Artículo 19, 2017, p.16). Por ello, es recomendable añadir que las evaluaciones de manera continua conforme surjan nuevos riesgos en el tratamiento.

Ahora bien, en relación con los códigos de conducta, antes de la regulación establecida en el Nuevo Reglamento, se contemplaban en el artículo 31 de la LPDP como normas internas creadas de manera voluntaria por las propias entidades responsables del tratamiento de datos para asegurar la mejora en las condiciones de operación de los sistemas de procesamiento de datos. De esta forma, se reconoce que los códigos son instrumentos de autorregulación que permiten establecer directrices dentro de una entidad para garantizar el cumplimiento de la normativa vigente (Santamaría Ramos, 2020, p.159).

Lo novedoso del Nuevo Reglamento es que se indique en el artículo 59 que son mecanismos de responsabilidad proactiva por el hecho de que permitan demostrar el cumplimiento normativo. Dicho reconocimiento resulta pertinente para la aplicación del principio de responsabilidad proactiva, pues la elaboración de dichos códigos denota que la protección de privacidad de usuarios está integrada a los procesos internos de los entes responsables del tratamiento. Así, dichos códigos reflejan que la adecuada gestión de los datos está integrada en la organización de la empresa.

Asimismo, de lo previsto en el artículo previamente señalado, se resalta el hecho de que existan códigos sectoriales emitidos por organizaciones representativas de los mismos. Ello resulta positivo, en tanto fomenta la colaboración de entidades de un mismo sector para homogenizar la organización de las operaciones del tratamiento. Así, se garantiza que los códigos establezcan prácticas comunes asociadas al tratamiento de datos en un sector en específico.

Sin perjuicio de las virtudes ya señaladas sobre la regulación de los códigos de conducta, cabe señalar que dichos mecanismos no solo se deben aplicar en virtud del sector, sino además del tamaño de la empresa. Como se resaltó previamente en el presente trabajo, en el RGPD sí contempla en su artículo 40.1 que la aplicación de dichos códigos dependerá de las necesidades específicas de las pequeñas y medianas empresas. Estipular una disposición similar en la normativa peruana sería coherente con el principio de proporcionalidad, puesto que no solo dichas empresas poseen menores recursos, sino además por la considerable diferencia del nivel de riesgo de las operaciones en comparación a las grandes empresas.

Por otro lado, está el artículo 60 del Nuevo Reglamento, en el que se reconoce el contenido mínimo de dichos códigos, aquel que requiere la incorporación de los siguientes aspectos:

- La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo
- Las disposiciones para el cumplimiento de los principios de protección de datos personales a los tratamientos sometidos al código de conducta.
- El establecimiento de procedimientos que faciliten el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición de los afectados.
- La determinación de las transferencias nacionales e internacionales de datos personales que, en su caso, se prevean con indicación de las garantías que deban adoptarse
- Las acciones de fomento y difusión en materia de protección de datos personales dirigidas a quienes los traten.
- Mecanismos para asegurar la confidencialidad de los datos personales por parte de quienes los traten.

- Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código de conducta.
- Cláusulas para la obtención del consentimiento de los titulares de los datos personales al tratamiento o transferencia de sus datos personales.
- Cláusulas para informar a los titulares de los datos personales del tratamiento
- Formatos para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.
- En caso de que se realice el tratamiento de datos personales por encargo, se presenta formatos de cláusulas para la contratación del encargado del tratamiento, conforme lo establece la Ley y el presente Reglamento.

Como se advierte del contenido señalado, está enfocado tanto en delimitar las actividades de tratamiento de una empresa o grupo de empresas y de garantizar el cumplimiento normativo a partir de la observancia de obligaciones establecidas en ley. No obstante, el problema es que la formulación de dicho contenido todavía fomenta el cumplimiento meramente documental al limitarse a requerir cláusulas y formatos, lo que hace que el código se vuelva un mecanismo que se restrinja al cumplimiento formal. Por ello, se recomienda también incorporar pautas para la realización de evaluaciones de impacto, criterios para el análisis de riesgo y parámetros para control de decisiones automatizadas para incorporar el enfoque de riesgos y la privacidad en el diseño en la elaboración de dichos códigos.

Adicionalmente, cabe indicar que, a partir de dicho contenido, se prevé la existencia de supervisión de la aplicación del código, lo que permite a las entidades responsables del tratamiento designar a entes autónomos encargados para supervisarlos. Aún así, no se regula en el mismo artículo 60 ni en alguna otra disposición del Nuevo Reglamento que dichos entes deberán ser evaluados por la ANPDP para poder llevar a cabo dicha supervisión, así como tampoco establece que se aplicarán sanciones para aquellos entes autónomos supervisores que incumplan su labor de supervisar, tal como lo contempla el RGPD europeo en el artículo 41. Ello conllevaría a que los mecanismos de supervisión se queden en el papel, pero sin garantías de que se vayan a aplicar o a implementar de forma adecuada.

Cabe señalar que tampoco se determina la necesidad de establecer un régimen sancionador por inobservancia del código. Dicha omisión deviene aún más ineficiente la supervisión de dichos códigos, puesto que el órgano designado para la supervisión no solo debe limitarse a advertir a las empresas adheridas al código de conducta que lo acaten, sino además disuadir a las empresas a incurrir en infracciones al código, ello a partir de sanciones desde la amonestación hasta la pérdida de la condición de entidad adherida. Por ello, se requiere que dentro del contenido mismo del código se establezca un apartado de infracciones y sanciones por incumplimiento. De lo contrario, no habrá cumplimiento efectivo de dicho mecanismo.

Otro tema relevante sobre la regulación del código su configuración como atenuante en el artículo 125 del Nuevo Reglamento. El reconocimiento como causal atenuante funciona como incentivo para las entidades responsables del tratamiento, toda vez que garantiza una disminución en el monto de multa por infracciones a la normativa de protección de datos. Dicho reconocimiento se debe a que, al igual que en el caso de las evaluaciones de impacto, la implementación del código denota que el responsable adoptó los esfuerzos razonables para garantizar el cumplimiento normativo, pese a haber incurrido en infracción a la normativa vigente.

No obstante, la aplicación de dicho incentivo es suficiente para fomentar la elaboración de códigos. Por un lado, ante la existencia de flujos transfronterizos o transferencias internacionales, los códigos permitirán acreditar el ofrecimiento de garantías suficientes, en tanto se garantice un nivel adecuado de protección sin importar el territorio (Blasi Casagrán, 2020, p.16). En este sentido, si el importador extranjero se adhiere a un código, ello permitirá al exportador peruano demostrar que el nivel de protección se mantiene o es equivalente al de la normativa nacional. Por consiguiente, se recomienda estipular en el artículo 20 de "garantías para flujo transfronterizo" la utilización de los códigos en cuestión.

Por otro lado, es importante ligar la implementación de los códigos con repercusiones reputacionales. Ello se puede lograr con la promoción de sellos que acrediten el cumplimiento normativo. Mediante dichos sellos, se puede reconocer que el responsable ofrece garantías suficientes para el tratamiento de datos personales por acreditar la existencia y aplicación de códigos de conducta (Roig Batalla, 2017, p.11). Así, la entidad responsable no solo mejora su reputación en el mercado, sino que además genera confianza en los principales afectados por el tratamiento.

Finalmente, cabe señalar que aparte de la previsión de los dos mecanismos previstos en el Nuevo Reglamento, también resultaría pertinente incluir como tercer mecanismo de responsabilidad proactiva a las certificaciones de privacidad. Como se ha explicado previamente en el apartado de "mecanismos de autorregulación", la utilidad de dichas certificaciones deriva en evaluar y acreditar que el proceso, producto o servicio tecnológico ofrecido cumple con los parámetros necesarios para proteger la privacidad de sus usuarios. Así, se podrá corroborar qué empresas realizan un tratamiento idóneo de datos personales.

Actualmente, se han establecido figuras similares a la de la certificación. Como señala Zegarra Valdivia, la obligación de inscripción de bancos de datos de entidades públicas al Sistema de Gestión de Seguridad de la Información establecida en el Anexo C de la Directiva de Seguridad funciona de manera similar a la certificación, pues con dicha inscripción se garantiza el cumplimiento de las medidas de seguridad previstas (2019, p.202). No obstante, dicha aproximación no basta para establecer un marco de certificación en el país, siendo necesario no solo que se prevea

expresamente en el ordenamiento, sino además que se establezcan los criterios de designación de entidades certificadoras independientes, el proceso de obtención de la certificación y el plazo de duración de la misma.

## 5. Conclusiones

- El principio de responsabilidad proactiva se introdujo recientemente a partir del artículo IX del Título Preliminar del Decreto Supremo 016-2024-JUS, aquel que aprueba el Nuevo Reglamento de la Ley de Protección de Datos Personales. Sin embargo, dicha figura no es nueva o reciente, sino más bien producto de años de desarrollo normativo internacional.

- La primera aparición del principio tuvo lugar tras la promulgación por parte de las Directrices de la OCDE sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales de 1980. En dichas directrices, figuraba como "principio de responsabilidad", aquel por el que los responsables se prometían a cumplir la normativa interna en materia de datos personales. Posteriormente, dicho principio se trasladó a otros documentos internacionales como la Directiva 95/46/ec de la Unión Europea o la Ley de Protección de Información Personal y de Documentos Electrónicos canadiense.

- En cuanto al desarrollo moderno de dicho principio, cabe señalar dos hitos relevantes: 1) la creación en 1995 del concepto de privacidad desde el diseño a partir del trabajo "Privacy Enhancing Technologies" y 2) la emisión de las Normas Internacionales de Madrid del año 2009. A partir de dichas normas, se establecen las dos obligaciones características del principio: 1) adopción de medidas que garanticen el cumplimiento y 2) demostración del cumplimiento. Como resultado, el Reglamento General de Protección de Datos europeo del año 2016 adoptó la configuración del principio en virtud de esas dos obligaciones, además de reconocer expresamente el concepto de privacidad desde el diseño.

- A partir del Nuevo Reglamento peruano y por inspiración del modelo europeo, se incorporó ese principio con las mismas obligaciones para los responsables. Sin perjuicio de ello, en el RGPD se regula dicho principio de manera más flexible preventiva, en tanto señale que su aplicación dependa de las condiciones del tratamiento y enfatice en el enfoque de riesgos como parte del principio. Asimismo, el RGPD desarrolla aspectos no desarrollados en el Nuevo Reglamento peruano como la proporcionalidad en la exigencia de medidas de cumplimiento, así como la obligación de continua actualización de aquellas.

- En lo referido al principio de licitud establecido en el RGPD, no solo se prevé que exista conformidad del tratamiento con lo establecido en la normativa como el principio de legalidad del artículo 4 de la LPDP peruana, sino que además se centra en la legitimidad de este al establecer en el artículo diversas bases por las que se justifica el tratamiento. Ello influye en la aplicación del principio de responsabilidad proactiva, puesto

que el responsable no solo se limitará a escoger una base, sino además debe justificar su elección y demostrar que ha llevado a cabo el tratamiento a partir de ella mediante registros de actividad, así como acreditar que cumplió con informar previamente a los titulares de los datos que dicha base se empleará para dicho tratamiento.

- En cuanto a la aplicación del principio de responsabilidad proactiva sobre terceros, se constata que, en contraste con la legislación peruana, el RGPD europeo sí especifica que el principio de responsabilidad proactiva no solo se debe aplicar respecto al tratamiento que los responsables realicen de manera directa, sino además de aquel realizado por los encargados mediante supervisiones constantes a los mismos; así como conservar los modelos de contrato o documentar la comunicación de instrucciones detalladas.

- Otro aspecto relevante de la regulación de la RGPD y que tampoco se halla presente en el Nuevo Reglamento es el concepto de privacidad desde el diseño. Dicho concepto permite incrustar la privacidad desde la arquitectura de equipos, productos o dispositivos en los que se realice el tratamiento de datos personales. Para alcanzar dicho propósito, se emplean técnicas de anonimización, seudonimización, minimización de datos y de configuración predeterminada de interfaz.

- Con relación a los mecanismos de responsabilidad proactiva reconocidos por la Unión Europea, se contemplan cuatro: a) la evaluación de impacto, b) los códigos de conducta, c) certificaciones y d) registros. A partir de las evaluaciones, el responsable identifica los riesgos existentes y determina las medidas de mitigación de riesgos. En el caso de los códigos de conducta, se trata de normas internas dentro de una misma entidad o grupo de entidades que permite acreditar el cumplimiento normativo. Por parte de las certificaciones, contribuyen a verificar si los productos o servicios brindados se ciñen a la normativa de protección de datos personales. Y los registros permiten la gestión de los datos al detallar qué operaciones se realizan con los datos y qué medidas son empleadas para mitigar los riesgos que puedan ocasionar dichas operaciones.

- Respecto a la aplicación del principio de responsabilidad proactiva en el entorno nacional, se desprenden cinco desafíos: a) El carácter abierto del concepto de responsabilidad proactiva, b) la inversión de la carga de la prueba y presunción de licitud detrás de la obligación de demostración del cumplimiento, c) la transición de un modelo de gestión a un modelo de responsabilidad, d) la necesidad de incorporar responsabilidad proactiva en la supervisión del tratamiento de terceros y el deber de colaboración de dichos terceros, e) la implementación de los mecanismos de autorregulación en el entorno nacional.

- El carácter abierto del principio de responsabilidad proactiva radica en no especificar cuáles medidas de cumplimiento deben implementarse. Y aunque en efecto dicha situación colisiona con la seguridad jurídica, debe considerarse que la indeterminación garantiza una flexibilidad que permite la adaptación a las nuevas tecnologías, fomentar en los responsables del tratamiento proponer medidas de acuerdo con el contexto del tratamiento y velar porque la protección de los datos se adecúe a la realidad de cada empresa o titular que realice actividades de tratamiento.

- Respecto a la inversión de la carga de la prueba, se evidencia en el principio cuando el artículo IX exige que el responsable pueda demostrar que ha cumplido con la norma. Ante dicha situación, existe el riesgo de vulnerar el principio de presunción de licitud establecido en el TUO de la LPAG, en tanto se deba partir de una presunción de cumplimiento y no requerir al administrado acreditarlo. Para evitar dicha contingencia, la ANPDP debe valerse de los principios de impulso de oficio y verdad material para recopilar las pruebas necesarias para determinar que el responsable ha incurrido en incumplimiento a la normativa de protección de datos personales.

- El ordenamiento peruano no garantizará la aplicación del principio de responsabilidad proactiva sin la transición del modelo de gestión al de responsabilidad. Para ello, requerirá que se fomente una cultura de cumplimiento normativo en la que los responsables del tratamiento reemplacen la aplicación mecánica y formal de la ley por un enfoque de prevención de riesgos y de privacidad desde el diseño. De esta forma, se exige que los responsables no se limiten a cumplir las obligaciones legales a manera de checklist, sino que adopten medidas de cumplimiento que se adapten a las nuevas tecnologías.

- Con relación al tema del control de los responsables sobre el tratamiento de terceros, se contempla que los responsables, al tener el poder de decisión sobre el tratamiento, deben no solo para asegurar que el tratamiento que realicen directamente se ciña al de la normativa, sino además en relación de los encargados y subcontratados a su cargo. Sin embargo, no se establece explícitamente en la regulación del principio que deba garantizarse el cumplimiento de la normativa en el tratamiento de terceros, lo que conlleva a que el responsable no aplique las medidas de supervisión para evitar que sus subordinados incurran en infracciones.

- Para finalizar, cabe constatar que el Nuevo Reglamento ha reconocido expresamente a las evaluaciones de impacto y a los códigos de conducta como mecanismos de responsabilidad proactiva. Dichos mecanismos no solo velan por la previsión de riesgos, sino además son medios probatorios para demostrar el cumplimiento. Sin embargo, cabe realizar algunas recomendaciones en cuanto a la regulación de los mismos.

Mientras que para la evaluación de impacto se requiera establecer su obligatoriedad para tratamientos de alto riesgo, detallar el contenido mínimo de dicha evaluación y estipular la obligación de actualizarlas de manera constante, se necesita que los códigos no se limiten a contener documentos formales de cumplimiento (cláusulas, formatos) y reforzar la supervisión de su aplicación a partir de órganos independientes.

## 6. Bibliografía

### Fuentes doctrinarias


- Alhadeff, J., Van Alsenoy, B. and Dumortier, J. (2012). The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. En: Postigo, H. et al. Managing Privacy Through Accountability. Basingstoke: Palgrave Macmillan, 2012.
- Alvarado, F.J. (2016). La gestión de la seguridad de la información en el régimen peruano de protección de datos personales. Revista Foro Jurídico, N° 15, 2016, p. 26 – 41.
- Baca Merino, R. (2020). Alcances de la presunción de licitud en el procedimiento administrativo sancionador. Derecho & Sociedad, 1(54), 267–276.
- Bacaria, J. (2018). Legitimación y base legal para el tratamiento. Especial referencia al consentimiento. Economist & Jurist. 01 de febrero del 2018.
- Barrio Andrés, M. (2024). Los principios generales del Reglamento General de Protección de Datos Personales. Actualidad Jurídica Iberoamericana, N° 20, febrero 2024, p. 1322 – 1341.
- Blasi Casagrán, C. (2020). Transferencias internacionales de datos personales. Universidad Oberta de Catalunya. 2020.
- Cano Galán, Y. (2020). La seudonimización y la anonimización de datos personales en las sentencias del orden jurisdiccional, Nº 119, 2020, págs. 31-56.
- Cañavete Mejías, María Ángeles (2021). El principio de responsabilidad proactiva en el Reglamento General de Protección de Datos. Trabajo de Máster: Universidad Internacional de la Rioja. 21 de julio de 2021.
- Cassagne, J.C. (2009). La discrecionalidad administrativa. Foro Jurídico, (09), 82–91.
- Carbajo Cobos, J.J. (2020). Conceptos jurídicos indeterminados y Derecho Canónico. Revista Española de Derecho Canónico: Universidad Pontificia de Salamanca. Vol 77, Núm. 189. Segundo semestre 2020.
- Cavoukian, A. y Borking, J. (1995). Privacy-Enhancing Techonologies: The Path to Anonymity. Editorial Registratiekamer. Enero de 1995.
- Cavoukian, A. (2009). Privacy By Design: 7 Foundational Principles, Implementation and Mapping of Fair Information Practices.
- Cavoukian, A. (2012). Operalizing privacy by design: A guide to implementing strong privacy practices. Diciembre de 2012.
- Chávez Bravo, V. (2025). El “nuevo” principio de responsabilidad proactiva y una de sus principales herramientas: La Evaluación de

Impacto en la Protección de Datos Personales. Enfoque Derecho, 2 de mayo de 2025: https://enfoquederecho.com/el-nuevo-principio-de-responsabilidad-proactiva-y-una-de-sus-principales-herramientas-la-evaluacion-de-impacto-en-la-proteccion-de-datos-personales/

- Consuegra Caicedo, L. et al. (2023). Algoritmos de inteligencia artificial basada en perfiles socio conductuales para la segmentación inteligente de clientes: estudio de caso. Ingeniería y competitividad: revista científica y tecnológica, vol 25, n°3, 2023.
- De Hert, P. (2012). Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights La. En: Postigo, H. et al. Managing Privacy Through Accountability. Basingstoke: Palgrave Macmillan. 2012.
- De Miguel Asensio, P.A. (2024). Minimización, licitud del tratamiento, categorías especiales y vías de tutela: novedades en materia de datos personales. Revista La Ley Unión Europea, n.130, noviembre 2024, pp.1-19.
- Díaz Romeral, A. (2016). “Los códigos de conducta en el Reglamento General de Protección de Datos”, Reglamento de Protección de Datos. Hacia un nuevo modelo de privacidad, Reus S. A.
- Durán Cardo, B. (2016). La figura del responsable en el derecho a la protección de datos personales. Editorial Wolters Kluwer. Primera Edición-Octubre 2016, pp. 179-259.
- 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, 2022, p.67-90.
- Esteva Garvayo, M.D.M (2020). Análisis a la luz del Dictamen del GT29. Trabajo de Máster: Universidad Internacional de la Rioja. 14 de octubre de 2020.
- Esteve Pardo, J. (2003). De la policía administrativa a la gestión de riesgos. Revista Española de Derecho Administrativo, N°119, 2003.
- Gamero Casado, E. y Berning Prieto, A.D. (2025). Evaluaciones de impacto y herramientas para su cumplimiento normativo en la implantación de algoritmos y tecnologías de IA. En Cerrillo y Martínez, A. y Velasco Rico, C., La regulación de la inteligencia artificial en España: una propuesta normativa para su uso en las administraciones, 2025.
- Gadea Soler, E. (2020). Análisis de riesgos y evaluación de impacto relativa a la protección de datos: su aplicación para sociedades corporativas. Boletín De La Asociación Internacional De Derecho Cooperativo, n.º 56 (abril), 47-72.
- Gastañaudi Ramírez, A. (2024). Patrones oscuros, datos personales y sombras legales: entendiendo a los patrones oscuros desde la normativa peruana sobre la protección de datos personales. Vol 2, decimo séptima edición.

- Gil Miñano, R. (2020). La ciberseguridad como solución de la privacidad: Especial incidencia en la privacidad en el diseño. Trabajo de Máster: Universidad Internacional de la Rioja. 02 de febrero de 2020.
- González, P.A. (2017). Responsabilidad proactiva en el tratamiento masivo de datos. Revista Dilemata, n°24, 2017.
- Goñi Stein, J. (2018). La autorregulación y los códigos de conducta en las redes sociales. En A.Batuecas y J.P.Aparicio (coordinador). Algunos desafíos en la protección de datos personales. Granada: Comares.
- Guzmán Napurí, C. (2009). "Los principios generales del Derecho Administrativo", Ius et Veritas N° 38.
- Guzmán Napurí, C. (2013). Manual del Procedimiento Administrativo General. Primera Edición-Junio 2013, pp. 63-95.
- Helguero Sainz, J. (2010). "Objeto y naturaleza de los códigos tipo", en Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, Thomson-Reuters, Cívitas, Pamplona, 2010.
- Jiménez Asensio, R. (2019). El nuevo marco normativo de protección de datos personales: su aplicación a las entidades locales. Anuario Aragonés del Gobierno Local 2019. N°10, pp.321-365.
- Martínez Martínez, R. (2018). Transformación digital y diseño orientado a la privacidad en la universidad. Ruidera: Revista de Unidades de Información, n. 13, 1er semestre 2018.
- Morón Urbina, J.C. (2023). Comentarios a la ley del procedimiento administrativo general. 17ª Edición-Julio 2023.
- Lifante Vidal, I. (2020). Sobre los conceptos indeterminados. Las pautas de "conducta y diligencia" en el Derecho. III Coloquio entre civilistas y filósofos del Derecho». Reus, 2020, pp.565-582.
- López Calvo, J. Una obra que acomete un exhaustivo, necesario y plural análisis del complejo marco establecido por el Reglamento y la Ley. En J. López (coordinador), La adaptación tras el nuevo marco de protección de datos tras el RGPD y la LPODGDD. Madrid, Wolker Kluwer.
- Maccasi Zavala, J.P. y Salazar Ortiz, E.E. (2020). Aspectos esenciales de la prueba en el procedimiento administrativo sancionador peruano: derecho a la prueba, carga y estándar de la prueba. Derecho & Sociedad, 1(54), p.337–356.
- Magide Herrero, M. y González Prada Arriarán, C. (2020). La prueba en el Derecho administrativo sancionador en Perú y en España. Derecho & Sociedad, 1(54), 323–336.
- Mato Pacín, M.N. (2020). Privacidad y consentimiento en el entorno digital: aproximación desde la perspectiva de la Unión Europea. Revista Electronica Direito e Sociedade. Canoas, v. 8, n. 3, 2020.
- Mato Pacín, M.N. (2024). Aspectos jurídicos del diseño de las interfaces digitales. En especial, los patrones oscuros. Agencia Estatal Boletín Oficial del Estado. Madrid, 2024.
- Martín Faba, J.M. (2024). Novedades en materia de indemnización y protección de datos personales. Revista CESCO de Derecho de Consumo. N°49,2024.

- Miralles López, R. (2019). Transferencias internacionales, códigos de conducta y certificaciones de cumplimiento. Universitat Oberta de Catalunya. Septiembre de 2019.
- Ornelas Núñez, L.G. (2013). La autorregulación en materia de datos personales: la vía hacia una protección global. Universidad de los Andes: Revista de Derecho, Comunicaciones y Nuevas Tecnologías. N°9, junio de 2013.
- Pavón Durán, R.I. (2024). Protección de datos en el ámbito notarial. Normativa y buenas prácticas. Editorial del Ecuador. 27 de diciembre de 2024.
- Pons Buigues, N. (2017). La protección de datos de carácter personal: principios legales y sistemas de gestión. Trabajo Final de Grado en Gestión y Administración Pública: Universidad de Valencia. 05 de septiembre de 2017.
- Piñar Mañas, J. et al. (2016). Reglamento general de protección de datos. 1era edición. Reus, 2016.
- Piñar Mañas, J.L. (coordinador) (2019). Memento Práctico: Protección de Datos Personales. Editorial Francis Lefebvre,13. Primera edición, 14 de mayo de 2019, pp.145-289.
- Polo Roca, A. (2020). Geolocalización, motores de búsqueda y cookies. Revista Jurídica de Castilla y León, N°52, pgs.141-184.
- Polo Roca, A. (2021). Datos, datos, datos: El dato personal, el dato no personal, el dato compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre el dato. Estudios de Deusto: revista de Derecho Público, vol.69, n°1, 2021.
- Puyol Montero, J. (2016). Los Principios del Derecho a la Protección de Datos. En Piñar Mañas, José Luis (director). Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Privacidad. Madrid: Editorial Reus, S.A.
- Puyol, Javier. 2018. El modelo de evaluación de riesgos en la protección de datos EIPD / PIA's. Valencia: Tirant lo Blanch, 2018.
- Quiroga León, J.A. (2021). Ciberseguridad y protección de datos personales en el Perú. Revista Advocatus, N°39, pp.15-21.
- Ramos Contreras, P.T. (2025). Replanteando el consentimiento: mecanismos de protección de los datos personales en el contexto del Big Data y las nuevas tecnologías en el marco legal peruano. Tesis para obtener el título de abogada. Pontificia Universidad Católica del Perú. 10 de septiembre de 2025.
- Real Pérez, A. (2012). Códigos de conducta y actividad económica: una perspectiva jurídica. Editorial Marcial Pons, Ediciones Jurídicas y Sociales SA.
- Rodríguez Arana, J. (2007). Principio de seguridad jurídica y técnica normativa. Círculo de Derecho Administrativo. Revista De Derecho Administrativo, (3), 251–268.
- Roig Batalla, A. (2017). Las obligaciones de los responsables y de los encargados del tratamiento. Universidad Oberta de Catalunya. 2017.

- Santamaría Ramos, F. J. (2020). El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano. Derecho PUCP, (85), 139–174.
- Sanz Marco, L. (2018). «Medidas Organizativas para la implantación del marco legal de protección de datos personales. El Registro de Actividades de Tratamiento».
- Serrano Pérez, M. M. (2021). Algunos elementos de los códigos de conducta. Asuntos Constitucionales: Universidad Castilla La Mancha. N°0,2021, pp. 151-168.
- Durán Troncoso, A. (2021). Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. 1era edición. Aranzadi, 2021.
- Vásquez Rodríguez, R. (2022). La Responsabilidad Proactiva en la Normativa Peruana de Protección de Datos Personales. Yachaq: Revista De Derecho, (13), p.25–37.
- Viguri Cordero, J. (2018). La Certificación en el Nuevo Reglamento Europeo de Protección de Datos y Anteproyecto de Ley Orgánica de Protección de Datos. Universidad Carlos III de Madrid, N°11, 2018.
- Villegas Vega, P. (2022). La actividad de fiscalización y derechos de los administrados: Las actas de inspección. IUS ET VERITAS, (65), 166–175.
- Zamudio Salinas, M.D.L. (2022). Reflexiones sobre la observancia del derecho fundamental a la protección de datos personales en los actos regulados por el Código Civil. Ius et Praxis, Revista de la Facultad de Derecho N° 55, diciembre 2022.
- Zegarra Valdivia, D.H. (2006). Control judicial de la discrecionalidad administrativa: Viejo problema y nuevo excursus (sus alcances en la Doctrina Española). Revista De Derecho Administrativo, (1), 33–62.
- Zegarra Valdivia, D.H. (2016). La utilización de conceptos jurídicos indeterminados en la tipificación de infracciones administrativas: breve aproximación a su estudio. En VII Congreso Nacional de Derecho Administrativo. (pp. 697 - 711). LIMA. EBC Ediciones-Thomson Reuters.
- Zegarra Valdivia, D.H. (2019). La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos a un uso responsable de la información. En D. H. Zegarra Valdivia (coordinador), La proyección del Derecho Administrativo peruano. Estudios por el Centenario de la Facultad de Derecho de la PUCP, páginas. 67-101. Editorial Palestra, páginas 165-211.


**Fuentes normativas y jurisprudencia**


- Agencia Española de Protección de Datos Personales (2009). Normas Internacionales sobre Protección de Datos Personales y Privacidad: Resolución de Madrid. 5 de noviembre de 2009.

- Consejo de Europa (1981). Convenio 108: para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. 28 de enero de 1981.
- Congreso de la República del Perú (2011). Ley 29733: Ley de Protección de Datos Personales. 3 de julio de 2011.
- Ministerio de Justicia y Derechos Humanos. (2019). Decreto Supremo 004-2019-JUS. Texto Único Ordenado de la Ley 27444. 25 de enero de 2019.
- Ministerio de Justicia y Derechos Humanos (2024). Decreto Supremo 016-2024-JUS: Decreto Supremo que aprueba el Reglamento de la Ley 29733, Ley de Protección de Datos Personales.
- Organización para la Cooperación y Desarrollo Económico (1980). Directrices que de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales. 23 de septiembre de 1980.
- Parlamento de Canadá (2001). The Personal Information Protection and Electronic Documents Act (PIPEDA). 13 de abril de 2000.
- Parlamento Europeo (1995). Directiva 95/46/EC, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. 24 de octubre de 1995.
- Parlamento Europeo (2016). Reglamento UE 2016/679, 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 y por el que se deroga la Directiva 95/46/CE. 27 de abril de 2016.
- Tribunal de Justicia Europeo. (2021). Sentencia 17.6.2021, asunto C-597/19. 17 de junio de 2021.
- Tribunal de Justicia Europeo. (2023). Sentencia 4.7.2023, asunto C-252/21. 04 de julio de 2023.


**Otros documentos**


- Agencia Española de Protección de Datos. (2018). Guía del Reglamento de Protección de Datos para Responsables de Tratamiento. Agosto 2018.
- Agencia Española de Protección de Datos. (2019). Guía de Privacidad desde el Diseño. Octubre 2019.
- Agencia Española de Protección de Datos. (2021). Gestión del riesgo y evaluación de impacto en el tratamiento de datos personales. Junio 2021.
- Autoridad Nacional de Protección de Datos Personales. (2021). Informe 069-2021-JUS/DGTAIPD-DFI. 31 de mayo de 2021.
- Autoridad Nacional de Protección de Datos Personales. (2021). Resolución Directoral 3439-2021-JUS/DGTAIPD-DPDP. 07 de diciembre de 2021.
- Autoridad Nacional de Protección de Datos Personales. (2022). Resolución 655-2022-JUS/DGTAIPD-DPDP. 14 de febrero de 2022.
- Autoridad Nacional de Protección de Datos Personales. (2025). Resolución Directoral 1254-2025-JUS/DGTAIPD-DPDP. 21 de abril de 2025.

- Comité Europeo de Protección de Datos Personales. (2019). Directrices 4/2019 relativas al artículo 25: Protección de datos desde el diseño y por defecto. 13 de noviembre de 2020.
- Comité Europeo de Protección de Datos Personales. (2020). Directrices 5/2020 sobre el consentimiento en el Reglamento (UE) 2016/679. 4 de mayo de 2020.
- Comité Europeo de Protección de Datos Personales. (2020). Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD. 2 de septiembre de 2020.
- Comité Europeo de Protección de Datos Personales. (2024). Dictamen 22/2024 dictamen sobre determinadas obligaciones derivadas de la dependencia del (de los) encargado(s) y subencargado(s) del tratamiento. 07 de octubre de 2024.
- Comunidad de Madrid. (2023). Recomendaciones sobre la anonimización y seudonimización de datos personales.
- Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. (2022). Opinión Consultiva 01-2022/DGTAIPD. 13 de enero de 2022.
- Grupo de Trabajo del Artículo 29 (2009). El futuro de la privacidad: Contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico del derecho fundamental a la protección de los datos personales. Bruselas, Bélgica, 2009.
- Grupo de Trabajo del Artículo 29 (2010). Dictamen 3/2010 sobre el principio de responsabilidad. 13 de julio de 2010.
- Grupo de Trabajo del Artículo 29 (2014). Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de datos en virtud del artículo 7 de la Directiva 95/46/CE. 09 de abril de 2014.
- Grupo de Trabajo del Artículo 29 (2017). Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento “entraña probablemente un alto riesgo” a efectos del Reglamento UE 2016/679. 4 de abril de 2017.
- Grupo de Trabajo del Artículo 29 (2017). Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. 28 de noviembre de 2017.
- Ministerio de Justicia y Derechos Humanos. (2013). Directiva de Seguridad. Primera edición, noviembre de 2013.
- Ministerio de Justicia y Derechos Humanos. (2024). Exposición de Motivos del Reglamento de la Ley de Protección de Datos Personales. 30 de noviembre de 2024.
- Organización para la Cooperación y el Desarrollo Económico. (2023). Memorando Explicativo de los Principios de la OCDE. Edición N°360. Octubre 2023.
- Tribunal Constitucional. Sentencia 00156-2012-PHC/TC. 8 de abril de 2012.