# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

# FACULTAD DE DERECHO

Informe jurídico sobre la Resolución Directoral N.° 110-2024-JUS/DGTAIPD La necesidad de fortalecer el programa de prevención de riesgos que fortalece la protección de datos personales: estudio del caso BCP y el uso de biometría en el Libro de Reclamaciones Virtual

Trabajo de Suficiencia Profesional para optar el Título de Abogada que presenta:

Rocío Guadalupe Lázaro Alegre

ASESOR:

Edison Paul Tabra Ochoa

Lima, 2025

**Informe de Similitud**

Yo, TABRA OCHOA, EDISON PAUL, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo de Suficiencia Profesional titulado "Informe jurídico sobre la Resolución Directoral N.° 110-2024-JUS/DGTAIPD La necesidad de fortalecer el programa de prevención de riesgos que fortalece la protección de datos personales: estudio del caso BCP y el uso de biometría en el Libro de Reclamaciones Virtual", del autor(a) LAZARO ALEGRE, ROCIO GUADALUPE, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 27%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 10/01/2026.

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

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

Lima, 13 de enero del 2026

| | |
|---|---|
| TABRA OCHOA, EDISON PAUL | |
| DNI: 20112143 | Firma:  |
| ORCID: https://orcid.org/0000-0002-6126-841X | |

**RESUMEN**

La resolución analizada trata sobre el uso de verificación biométrica facial que el BCP aplicaba para que los usuarios pudieran presentar reclamos en el Libro de Reclamaciones Virtual. Aunque los bancos deben cumplir la Resolución 504-2021-SBS, que exige autenticación reforzada para operaciones financieras, la ANPD señaló que esa obligación no alcanza a la presentación de reclamos. El motivo es que este procedimiento no es una operación ni un servicio financiero que justifique controles tan intrusivos, salvo que se vea comprometida información patrimonial o la privacidad del usuario. Por eso, el uso de biometría fue considerado innecesario y desproporcionado; así como la falta de consentimiento válidos, constituyendo una infracción grave a la Ley 29733 y derivando en una multa de 63 UIT.

A partir de ello, el problema es determinar qué elementos deberían incluirse en un Programa de Prevención de Riesgos para evitar tratamientos excesivos o injustificados de datos sensibles. Por tanto, se concluye que el criterio de proporcionalidad debe incorporarse en la evaluación de riesgos para lo que se propone un Test de Proporcionalidad obligatorio antes de aplicar mecanismos biométricos o tratar datos sensibles, de modo que estas medidas solo se utilicen cuando realmente sean necesarias y no exista una alternativa menos intrusiva. Asimismo, de forma posterior debe realizarse una Evaluación de Impactos de Protección de Datos que permitirá que se determine qué riesgos pueden ser asumidos por las entidades financieras, si deben ser modificadas sus medidas o erradicados.

**Palabras clave**

Consentimiento, Proporcionalidad, Infracciones, Evaluación, Biometría

***ABSTRACT***

The analyzed resolution concerns the use of facial biometric verification that BCP required for users to submit complaints through the Virtual Complaints Book. Although banks must comply with Resolution 504-2021-SBS, which mandates reinforced authentication for financial operations, the ANPD stated that this obligation does not apply to the submission of complaints. This is because such a procedure is not a financial operation or service that would justify intrusive controls, unless the user's patrimonial information or privacy is at risk. For this reason, the use of biometrics was considered unnecessary and disproportionate, as well as lacking valid consent, constituting a serious violation of Law 29733 and resulting in a fine of 63 UIT.

Based on this, the issue is to determine which elements should be included in a Risk Prevention Program to avoid excessive or unjustified processing of sensitive data. Therefore, it is concluded that the proportionality criterion must be incorporated into the risk assessment, for which a mandatory Proportionality Test is proposed before implementing biometric mechanisms or processing sensitive data, ensuring that such measures are used only when truly necessary and when no less intrusive alternative exists. Additionally, a subsequent Data Protection Impact Assessment should be conducted to determine which risks can be assumed by financial institutions, and whether their measures must be modified or eliminated.

***Keywords***

Consent, Proportionality, Infractions, Data, Biometrics

## ÍNDICE

**PRINCIPALES DATOS DEL CASO**

| | |
|---|---|
| **N° EXPEDIENTE** | Resolución Directoral N.° 110-2024-JUS/DGTAIPD |
| ÁREA(S) DEL DERECHO SOBRE LAS CUALES VERSA EL CONTENIDO DEL PRESENTE CASO | Datos Personales, Compliance, Procedimiento Administrativo Sancionador |
| IDENTIFICACIÓN DE LAS RESOLUCIONES Y SENTENCIAS MÁS IMPORTANTES | Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP<br>Resolución 504-2021-SBS |
| DEMANDANTE/DENUNCIANTE | Demandante Anónima |
| DEMANDADO/DENUNCIADO | Banco de Crédito del Perú S.A. |
| INSTANCIA ADMINISTRATIVA O JURISDICCIONAL | Dirección de Protección de Datos Personales |
| TERCEROS | |
| OTROS | |

# I. INTRODUCCIÓN

## 1.1 Justificación de la elección de la resolución

Considero relevante la presente resolución debido a que el Banco de Crédito del Perú (BCP), al ser una entidad financiera, pertenece a un sector empresarial pionero en materia de compliance. Ello se remonta al origen del compliance, el cual se implementa en el sistema bancario a finales de la Primera Guerra Mundial, cuando el Comité de Supervisión Bancaria de Basilea (CSBB) impuso la necesidad de establecer estándares prudenciales para la supervisión del riesgo financiero. Como resultado, las entidades bancarias cuentan hoy con un marco regulatorio internacional y nacional sumamente amplio, del cual deben nutrirse para proveer garantías en el cumplimiento de las normas.

En este contexto, la infracción detectada por la Autoridad Nacional de Protección de Datos Personales (ANPDP), basada en el incumplimiento del artículo 132 del Reglamento de la Ley de Protección de Datos Personales (RLPDP), incentiva a reflexionar acerca de qué medidas de compliance debió implementar el BCP para prevenir la infracción cometida y, a su vez, qué acciones debe adoptar hacia adelante para evitar infracciones de la misma naturaleza.

Asimismo, esta resolución también deja en evidencia una tensión normativa entre: una norma sectorial que regula las funciones de los bancos, como lo es la Resolución 504-2021-SBS y la generalidad con que el RLPDP protege el derecho a la autodeterminación informativa. En tal sentido, surge una limitación para que las instituciones financieras desplieguen medidas de seguridad antifraude y contra la suplantación de identidad en determinadas materias como lo es la imposición de reclamos o quejas digitales. En consecuencia, los bancos enfrentan restricciones para implementar mecanismos de autenticación más robustos, pese a que ello contribuiría a un mejor control sobre los usuarios y a la prevención de riesgos.

Finalmente, es preciso mencionar que, la Constitución Política del Perú ampara la libertad de empresa mediante el artículo 59; por tanto, esta sanción impuesta por la ANPDP puede representar una acción que transgrede esta libertad que la carta magna le otorga a las empresas. Adicionalmente, la CSBB sostiene que la regulación prudencial busca reducir los riesgos que amenazan a las instituciones bancarias y al sistema financiero en su conjunto, además de garantizar que los supervisores, tales como la Superintendencia de Banca y Seguros AFP del Perú, puedan monitorear el cumplimiento normativo y evitar la asunción de riesgos excesivos.

En ese sentido, el presente trabajo busca analizar dos dimensiones del compliance: el compliance administrativo y el compliance bancario. El primero hace referencia a la protección de datos personales y las obligaciones que la ANPDP exige. En cambio, el compliance bancario está relacionado con las obligaciones que la SBS impone a los bancos. Por tanto, el problema central que guía esta investigación se basa en ¿Cuáles son los elementos en materia de protección de datos personales debería incluir el programa de prevención de riesgos a fin de evitar sanciones por incumplimiento a la normativa sectorial de la SBS y la Ley de Protección de Datos Personales y su Reglamento?

## 1.2 Presentación del caso y del análisis

Mediante la Resolución Directoral N.° 110-2024-JUS/DGTAIPD, la Autoridad Nacional de Protección de Datos Personales impuso al Banco de Crédito del Perú (BCP) una multa ascendente a 63 Unidades Impositivas Tributarias (UIT) por haber implementado la verificación biométrica facial para los usuarios que deseaban presentar reclamos o quejas digitales a través de su Libro de Reclamaciones Virtual. Al respecto, se entiende por datos biométricos como el proceso que permite identificar a una personalidad de acuerdo a la recolección características mediante el escaneo de rasgos físicos, específicamente faciales para efectos del presente caso.

En esa línea, la ANPDP concluyó que esta exigencia no se encontraba vinculada a la prestación o venta de un servicio financiero que justificara la aplicación de medidas de autenticación reforzadas, ya que se trataba únicamente de solicitudes de atención que no implicaban operaciones financieras ni transacciones patrimoniales al no ser estrictamente requerido para la finalidad de canalizar reclamos. Por lo que, determinó dos infracciones, (i) el uso de datos biométricos resultaba innecesario y desproporcionado, (ii) la recolección de los mismos no contaba con el consentimiento válido de los usuarios.

En consecuencia, determinó que dicha práctica constituía una vulneración a los principios de proporcionalidad y finalidad establecidos en la Ley de Protección de Datos Personales (LPDP) y en su Reglamento (RLPDP), imponiendo al BCP no solo la multa mencionada, sino también medidas correctivas orientadas a suprimir dicho mecanismo de validación.

Desde mi apreciación personal, considero que esta medida no resultó ser la más idónea; sin embargo, representa un precedente importante que permite analizar qué elementos deben incluir las entidades financieras en su Programa de Prevención de Riesgos que permitan mitigar los riesgos derivados de la recolección y tratamiento de datos personales. Ello porque dicha entidad cuenta con un programa interno de compliance bancario orientado al cumplimiento normativo, y adoptó como medida para interponer reclamos el uso de datos biométricos, en atención a lo dispuesto por la Resolución SBS N° 504-2021, que establece la obligación de implementar mecanismos de autenticación reforzada en los canales digitales de las entidades financieras.

En este sentido, la medida implementada por el BCP no consideró que se vulnerarían los datos sensibles de los usuarios, por el contrario, buscaba garantizar un estándar de seguridad frente a riesgos de fraude y suplantación de identidad. Por ello, la severidad de la sanción debió ser ponderada en función del marco regulatorio sectorial bajo el cual actuaba el banco.

De este análisis se desprende el problema principal en materia de compliance**:** ¿Cuáles son los elementos en materia de protección de datos personales debería incluir el programa de prevención de riesgos a fin de evitar sanciones por incumplimiento a la normativa sectorial de la SBS y la Ley de Protección de Datos Personales y su Reglamento?

Este problema principal se descompone en dos problemas secundarios**:** ¿Cómo debe implementarse el criterio de proporcionalidad en la evaluación de riesgos y la evaluación del impacto de protección de datos?; y ¿Qué buenas prácticas internacionales podrían servir de referencia para fortalecer la prevención de infracciones administrativas en el sistema financiero peruano?

El análisis se sustenta en diversos instrumentos normativos: la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento, que fijan el marco general de protección de la autodeterminación informativa; la Resolución SBS N.° 504-2021, que exige medidas reforzadas de seguridad en canales digitales del sistema financiero; la Resolución Directoral N.° 110-2024-JUS/DGTAIPD, que constituye el caso concreto objeto de estudio; el Código Penal, que contempla figuras vinculadas a la vulneración de datos personales; la Constitución Política del Perú que ampara el derecho a la privacidad; y la doctrina internacional del Comité de Supervisión Bancaria de Basilea, que establece principios prudenciales sobre gestión de riesgos en el sector bancario.

Asimismo, también se recurre a las normas de chile y Colombia. Por un lado, Chile cuenta con la Ley N.º 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Por otro lado, Colombia cuenta con la Ley Estatutaria 1581 de 2012, que dicta disposiciones generales para la protección de datos personales.

Desde el aspecto doctrinal, se cuenta con posiciones como la de Diego Kohn que señala que el compliance financiero surge como un mecanismo de autorregulación financiera para la gestión de riesgos, que

luego se expande a otras áreas a fin de contribuir con la buena gobernanza corporativa. Desde la óptica europea, Agustín Puente plantea que los principios de proporcionalidad y finalidad son ejes que sirven para limitar el manejo de datos personales, criterio que permite ser aplicado como parte del elemento que debe tomarse en cuenta como parte del programa de prevención de riesgos.

Por último, respecto a la jurisprudencia a tener en cuenta se tiene la Resolución Directoral N.º 240-2019-JUS/DGTAIPD-DF, que se basa en un procedimiento sancionador de la ANPDP a la Universidad Femenina del Sagrado Corazón por la recopilación de datos sensibles innecesarios. Así también, se cuenta con la Opinión Consultiva N°032-2021-JUS/DGTAIPD de la ANPDP, que permite considerar bajo qué criterios válidos la ANPDP aprueba la recolección de datos biométricos.

Como conclusión preliminar, se sostiene que los bancos deben implementar como elemento del programa, el criterio de proporcionalidad que debe incorporarse tanto en la evaluación de riesgos como en los controles operativos del programa. Para ello, se propone la implementación de un Test de Proporcionalidad obligatorio antes de aplicar mecanismos biométricos o tratar datos sensibles, Dichos modelos deben justificar el uso de medidas de autenticación robusta únicamente cuando sea estrictamente necesario, documentar de manera clara el sustento jurídico para el tratamiento de información sensible y ofrecer alternativas menos intrusivas a los usuarios. Solo de esta manera será posible garantizar un equilibrio entre seguridad digital y protección de datos personales, reforzar la confianza del consumidor y, al mismo tiempo, minimizar los riesgos de sanciones administrativas y de eventuales responsabilidades de índole penal.

## II. IDENTIFICACIÓN DE LOS HECHOS RELEVANTES

### 2.1 Antecedentes

El presente caso ocurre en el año 2024, cuando una clienta del BCP interpuso una denuncia ante la Autoridad Nacional de Protección de Datos Personales (ANPDP) debido a la exigencia de validación mediante datos biométricos para el registro de reclamos en el Libro de Reclamaciones digital del banco. A raíz de ello, el Comité de Protección de Datos Personales de la ANPDP inició una investigación y declaró fundada la denuncia, imponiendo al BCP una multa equivalente a 63 UIT, al considerar que el tratamiento de datos biométricos en este contexto resultaba excesivo y no guardaba proporcionalidad con la finalidad de atender reclamos, por no tratarse de una operación financiera. Así como tampoco existía consentimiento de parte de los titulares de los datos.

En su defensa, el BCP presentó un recurso de apelación alegando que esta medida respondía a las obligaciones impuesta por la SBS por medio de la Resolución N.° 504-2021-SBS; la cual establece la necesidad de implementar mecanismos robustos de autenticación en canales digitales para disminuir los riesgos de fraude y suplantación de identidad en operaciones financieras. Sin embargo, la Dirección de Protección de Datos Personales confirmó en segunda instancia la decisión inicial, ratificando la sanción.

Esta resolución representa un precedente de suma importancia en el ámbito de la protección de datos personales, pues refleja que existen tensiones entre una norma general como la LPDP, que tutela el derecho fundamental a la autodeterminación informativa bajo el principio de consentimiento, y la aplicación del criterio de proporcionalidad en el tratamiento de datos personales. Así como, una norma sectorial como la Resolución SBS N.° 504-202 que, bajo la regulación prudencial, exige a las entidades bancarias a elevar sus estándares de seguridad digital.

### 2.2 Hechos relevantes del caso

1. El 05 de agosto de 2021, la SBS emite la Resolución N° 504-2021-SBS, que obliga a las entidades financieras a implementar mecanismos robustos de autenticación en operaciones digitales para prevenir fraudes y suplantación de identidad.

2. Posteriormente, el BCP condicionó el acceso al Libro de Reclamaciones digital al uso obligatorio de reconocimiento biométrico facial, impidiendo al usuario presentar un reclamo si no aceptaba ese tratamiento de datos sensibles.

3. Con fecha 02 de agosto de 2023, una usuaria presentó denuncia contra el BCP ante la Dirección de Protección de Datos Personales por la exigencia de los datos biométricos faciales exigidos por el BCP para la interposición de reclamos digitales.

4. Con fecha 02 de octubre de 2023, por medio del Informe Técnico N° 107-2023-DFI-ORQR el analista de Fiscalización de la DFI informó acerca de una fiscalización realizada al BCP, concluyendo que: El BCP realiza el enrolamiento biométrico de usuarios que presentan un reclamo por primera vez usando la información y fotografía obtenida del servicio de consulta de datos del RENIEC. Para validaciones posteriores, el banco ya no usa RENIEC, sino su propia base de datos biométrica BIOM (ORACLE 19C), donde almacena imágenes encriptadas.

5. Con fecha 13 de octubre de 2023, la ANDP mediante la Dirección de Fiscalización e Instrucción resuelve iniciar procedimiento administrativo sancionador al BCP mediante Resolución Directoral N.° 232-2023-JUS/DGTAIPD-DFI, debido a las presuntas infracciones por realizar el tratamiento desproporcionado de los datos personales a quienes generan un reclamo y por almacenar los datos biométricos faciales sin obtener el consentimiento del titular.

6. El 01 de julio de 2024, por medio de la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP, la Dirección de Protección de Datos Personales (DPDP) notifica el 09 de julio del 2024, mediante Cédula de Notificación N.º 992-2024-JUS/DGTAIPD-DPDP al BCP, la siguiente resolución: sancionar con la multa ascendente a 27 UIT por haber efectuado el uso de datos sensibles de forma excesiva, no necesaria ni pertinente; asimismo, sancionar con una multa ascendente a 36 UIT por la falta de consentimiento de los titulares. Adicionalmente, como medidas correctivas se impuso la supresión de la información biométrica de la base de datos BIOM, cesar el almacenamiento de patrones biométricos y la remisión de documentos que sustenten su implementación.

7. Con fecha 30 de julio de 2024, BCP apeló la resolución previamente indicada, alegando pese a la sanción impuesta, la propia DPDP habría reconocido que en ciertos casos sí resulta proporcional y necesario validar la identidad mediante biometría para proteger la información patrimonial del usuario. El banco sostiene que este mecanismo es idóneo y se ajusta a lo exigido por la SBS, que requiere dos factores de autenticación y no ofrece alternativas menos intrusivas para clientes intermitentes. Asimismo, afirma que los clientes regulares pueden optar libremente por usar clave o biometría, por lo que la medida no sería desproporcionada. Además, cuestiona que la DPDP no haya ponderado adecuadamente los riesgos, no haya identificado opciones viables y haya realizado un análisis poco coherente respecto a la proporcionalidad y al almacenamiento de los datos. Finalmente, señala que no sería exigible el consentimiento; toda vez que, el almacenamiento no respondería a un interés comercial.

8. Con fecha 27 de diciembre de 2024, la ANDP mediante la Dirección de Protección de Datos Personales emite pronunciamiento en segunda instancia resolviéndolo como Fundado en Parte, pues reformula la medida correctiva ordenando que el BCP debe eliminar los patrones biométricos faciales obtenidos a través del Libro de Reclamaciones Virtual; y, si técnicamente no es posible hacerlo de manera selectiva, deberá demostrar

dicha imposibilidad. En todo lo posterior ratifica la resolución en primera instancia.

## III. IDENTIFICACIÓN DE LOS PRINCIPALES PROBLEMAS JURÍDICOS

### 3.1 Problema principal

¿Cuáles son los elementos en materia de protección de datos personales debería incluir el programa de prevención de riesgos a fin de evitar sanciones por incumplimiento a la normativa sectorial de la SBS y la Ley de Protección de Datos Personales y su Reglamento?

### 3.2 Problemas secundarios

1. ¿Cómo debe implementarse el criterio de proporcionalidad en la evaluación de riesgos y la evaluación del impacto de protección de datos?

2. ¿Qué buenas prácticas internacionales (por ejemplo, de Chile, Colombia y España) podrían servir de referencia para fortalecer la prevención de infracciones administrativas en el sistema financiero peruano?

### 3.3 Problemas complementarios

¿Fue proporcional la multa de 63 UIT impuesta al BCP por la ANPDP, y, en tal sentido, dicha sanción resulta coherente con el objetivo de incentivar que las entidades financieras adopten y fortalezcan modelos de compliance administrativo que garanticen el cumplimiento de la normativa sobre protección de datos personales?

## IV. POSICIÓN DEL CANDIDATO/A

### 4.1 Respuestas preliminares a los problemas principal y secundarios

¿Cuáles son los elementos en materia de protección de datos personales debería incluir el programa de prevención de riesgos a fin de evitar sanciones por incumplimiento a la normativa sectorial de la SBS y la Ley de Protección de Datos Personales y su Reglamento?

Las entidades financieras deberían implementar elementos al Programa de Prevención de Riesgos que eviten infracciones e incumplimientos, los cuales deben implementar políticas de compliance para proteger la información personal de los individuos, en armonía tanto con la normativa sectorial como con la normativa general. En vista a ello, para el manejo de datos personales, debe efectuarse una Evaluación de Impacto de Privacidad que permite determinar cuáles son los principales riesgos y las posibles afectaciones que podrían sufrir estos datos producto de la gestión de dicha información.

Bajo esta evaluación se plantea ceñirse al criterio de proporcionalidad mediante un test de proporcionalidad interno sobre la necesidad de implementar medidas rígidas para que los usuarios accedan a los sistemas bancarios, tales como el libro de reclamaciones digital. Este test debe considerar las exigencias que la SBS impone a las entidades bancarias a fin de regularlos; asimismo, tomar en cuenta las indicaciones la LPDP para regular la protección de datos personales. A partir de ello, los bancos incurrirían en menores infracciones e implementarían las medidas menos lesivas y adecuadas que eviten que recaigan tanto en infracciones administrativas como posibles ilícitos penales.

En adición, tanto las entidades bancarias como cualquier otra entidad deben tratar los datos biométricos u otro tipo de datos personales mediante un consentimiento expreso, específico e informado a los usuarios, que contenga el detalle de la finalidad de su recopilación y tratamiento. De estar vulnerándose

algún derecho de privacidad de los usuarios, debería optarse por otros medios de autenticación menos intrusivos que permitan que no se materialicen los fraudes o suplantaciones de identidad.

1. ¿Cómo debe implementarse el criterio de proporcionalidad en la evaluación de riesgos y controles operativos del programa de prevención de riesgos?

El criterio de proporcionalidad debe incorporarse en el Programa de Prevención de Riesgos en dos niveles: (i) dentro de la evaluación de riesgos, como parámetro para identificar tratamientos innecesarios o excesivos de datos personales, sobre todo aquellos que contemplen información sensible como los biométricos; y (ii) dentro de los controles operativos, mediante la exigencia de un Test de Proporcionalidad previo a cualquier tratamiento de datos sensibles o a la implementación de mecanismos biométricos.

Este debe contener elementos que aseguren un tratamiento responsable, seguro y proporcional de esta información sensible, como los datos financieros y biométricos, de conformidad con el artículo 2.5 de la Ley N 29733. No basta con implementar medidas de ciberseguridad o autenticación reforzada por mandato de la SBS; los bancos deben ejecutar estas medidas con respeto a los principios de finalidad, consentimiento y proporcionalidad que exige la ANPDP.

2. ¿Qué buenas prácticas internacionales (por ejemplo, de Chile, Colombia y España) podrían servir de referencia para fortalecer la prevención de infracciones administrativas en el sistema financiero peruano?

Los programas implementados en Chile y Colombia para proteger los datos personales de los usuarios presentan una graduación de sanciones que incentivan a las personas jurídicas su cumplimiento, no solo desde la imposición de multas, sino también de medidas correctivas.

La graduación que implementa Chile en base a la Ley N° 21.719, se creó la agencia de Protección de Datos Personales, símil a la ANPDP. Dicha agencia implementa un sistema de infracciones modelado al sistema europeo. Esta ley clasifica las sanciones entre leves, graves y muy graves. Asimismo, prevé criterios de graduación como la reincidencia, el beneficio desplegado del tratamiento de datos, la cooperación que la persona jurídica preste y la exigencia de programas de cumplimiento. De forma adicional, plantean medidas correctivas que hacen más flexibles las sanciones que su agencia ordena.

Por otro lado, en Colombia la Superintendencia de Industria y Comercio que se posiciona como la autoridad en esta materia, cuenta con competencias tanto en supervisión como sanción. Esta aplica un régimen sancionador estricto en términos económicos, contemplando multas superiores a las peruanas. Sin embargo, considera y valora la cooperación, reincidencia, programas de cumplimiento, lo cual incentiva que las empresas implementen programas preventivos en sus sistemas.

En ese sentido, que ambas establezcan medidas correctivas que incentiven la implementación de sistemas de compliance en las instituciones financieras, vienen a ser prácticas internacionales que debe considerar la ANPDP. Por su parte, las entidades financieras deben tomar como principal medida de buena práctica de ambos países, el establecimiento de programas de compliance que coadyuven a proteger los datos personales de los usuarios y desmaterializar riesgos, tales como las infracciones administrativas.

### 4.2 Posición individual sobre el fallo de la resolución

Como apreciación personal, considero que debe valorarse que, el BCP actuó en un marco de compliance sectorial**,** respondiendo a la obligación impuesta por la Resolución SBS N.° 504-2021, que exige a las entidades bancarias que implementen mecanismos de autenticación reforzada en los servicios digitales. A ese entender, la medida de seguridad implementada por el banco, obedecía a la necesidad de alinearse a estándares prudenciales de seguridad exigidos por

la SBS, que buscan proteger tanto a las entidades financieras como a los usuarios frente a fraudes y suplantaciones de identidad.

Si bien es cierto, la LPDP protege la autodeterminación informativa y exige proporcionalidad en el uso de datos sensibles. En este caso, existió una dualidad normativa que no permitía al banco estimar medidas de acceso a sus sistemas (libro de reclamaciones digital), que no vulnere los datos biométricos de sus usuarios, el cual devengó en una multa de 27 UIT, siendo calificada la infracción como grave. En ese sentido, la Resolución Directoral N.º 232-2023-JUS/DGTAIPD-DFI, marca un precedente en el establecimiento de medidas de seguridad que no transgredan limitaciones al uso de los datos personales.

En conclusión, mi posición es que, si bien la Resolución no fue proporcional al modelo de compliance que ya había sido implementado por el BCP para el manejo de datos personales; las instituciones financieras deben contar con un marco de compliance que no solo se oriente a cumplir con las normas sectoriales, sino que deben considerar el cumplimento de la normativa vigente en esta materia, y otras que puedan provocar infracciones administrativas que generen daños económicos y reputacionales.

Por lo tanto, las entidades financieras deben reforzar sus Programas de Prevención de Riesgos mediante la implementación de elementos que consideren el criterio de proporcionalidad como parte de la evaluación de riesgos como en los controles operativos del programa. Por lo que, resulta importante realizar un Test de Proporcionalidad obligatorio antes de aplicar mecanismos biométricos o tratar datos sensibles, Ello garantiza y justifica el uso de medidas de autenticación robusta únicamente cuando sea estrictamente necesario.

A fin de fortalecer tal implementación, se proponen como guía los modelos extranjeros como el colombiano y chileno. Todo ello permite crear una mejor cultura de compliance en la que se prevé mitigar infracciones de este tipo por parte de las diferentes entidades financieras.

## V. ANÁLISIS DE LOS PROBLEMAS JURÍDICOS

1. ¿Cómo debe implementarse el criterio de proporcionalidad en la evaluación de riesgos y controles operativos del programa de prevención de riesgos?

El concepto de datos personales hace referencia a toda aquella información propia de una persona que permite identificarla; asimismo, los datos sensibles son aquellos que describen aspectos de salud, financieros, biométricos (Niño, 2022). En esa línea, los datos personales financieros conforme al artículo 2.5 de la Ley N° 29733, Ley de Protección de Datos Personales, se identifican como datos sensibles. En ese sentido su tratamiento se convierte más delicado y requiere de un mayor nivel de seguridad de parte de los encargados de los bancos de datos personales.

De esta manera, dichas entidades no solo acceden a información sensible financiera, sino también a información biométrica que permita mantener resguardada la información financiera así como el acceso a sus servicios mediante esta validación. Estas como intermediarias del sistema económico manejan un volumen extenso de información personal y financiera de usuarios (Abdo, 2024). Ante este manejo de información sensible masiva de parte de los bancos, la SBS mediante la Resolución N° 504-2021, los obliga a implementar mecanismos de autenticación reforzada en sus canales digitales, con el fin de mitigar fraudes ciberdigitales.

Por lo tanto, la implementación de modelos de cumplimiento constituye una herramienta esencial para prevenir infracciones administrativas derivadas del manejo inadecuado de dichos datos. Por tanto, las empresas deben tener en cuenta los riesgos de privacidad y cómo pueden afectar una protección adecuada de los datos personales de los usuarios (Sebastián y Vasquez, 2021, p. 44). De forma específica, en el sector financiero es necesario articular la incorporación de avances tecnológicos y el estricto cumplimiento de las normas vigentes relacionadas con la protección de datos personales, sobre todo en el contexto de la digitalización global (Dávalos y Mujica, 2022, p. 9).

Así pues, el caso del BCP frente a la ANPDP expone cómo incluso una entidad financiera con altos sistemas de seguridad de la información y cumplimiento sectorial, puede incurrir en infracciones al no lograr la armonización de las exigencias normativas impuestas por la SBS con las exigencias de la Ley N.º 29733 y su Reglamento, que para la presente Resolución objeto de análisis, el banco obtuvo como infracción una multa de 27 UIT debido a que la ANPDP consideró que el manejo de datos sensibles no superó el estándar de necesidad para este fin.

Este criterio de la finalidad del uso de datos biométricos, emana del numeral 30 de la Opinión Consultiva N°032-2021-JUS/DGTAIPD de la ANPDP, que establece que únicamente es posible utilizar sistemas de identificación biométrica para obtener el consentimiento de sus titulares, cuando el tratamiento guarde proporcionalidad con la finalidad perseguida. De esta manera, se entiende que la ANPDP busca que previo al uso de datos biométricos, los titulares de los bancos de datos analicen que su finalidad sea proporcional, de lo contrario, sería un tratamiento excesivo, como el considerado en el caso BCP.

En ese sentido, la experiencia doctrinal y jurisprudencial demuestra que el cumplimiento normativo en materia de datos personales debe concebirse como un mecanismo preventivo, más que como una respuesta sancionadora. De allí la necesidad de identificar cuáles son las medidas concretas de compliance que deben ser implementados por las instituciones bancarias para garantizar el tratamiento adecuado de los datos personales, tema que se desarrollará en los siguientes apartados.

### 1.1. La importancia de la gestión de riesgos en protección de datos personales

Las entidades financieras son aquellas que más requieren reafianzar y promocionar sus servicios; debido a que el volumen de empresas y oferta de productos genera mayor competencia, de forma indirecta, esto se refleja en la disminución de clientes, ingresos y potenciales negocios (Onetto, 2007, p. 6). En

tal sentido, se encuentran sometidas a mayores regulaciones, sobre todo las impuestas por la SBS. En tal sentido, los bancos son más propensos a seguir modelos de compliance en el proceso total de sus operaciones.

Debe entenderse al compliance como el deber de acatar las leyes, regulaciones, normas y códigos internos de la organización, así como los principios de buena gestión y los parámetros de ética requeridos (Rios, 2014, p. 5). Este no solo busca el cumplimiento, sino promueve que no se cometan ilícitos tales como el lavado de activos, multas, sanciones, entre otros. Se trata entonces de un mecanismo de regulación interna implementado por la compañía para preservar la imagen pública corporativa (p. 27).

Que el sistema de compliance resulte o no efectivo depende de qué tan actualizado se encuentre para evaluar los potenciales riesgos (Herrera y Rodriguez, 2023). En esa línea, se vincula el compliance con la gestión de riesgos, la cual se entiende como aquellas amenazas que provienen de fuentes tales como la inestabilidad financiera, las obligaciones legales, la aplicación tecnológica de insumos, las deficiencias en la gestión estratégica, los incidentes y los desastres naturales. Por lo que, la gestión de estos busca anticipar las amenazas y los efectos de su materialización; para lo cual establecen planes que los mitiguen (McGrath y Jonker, s/f).

Ahora bien, en el sector financiero, según Miller, la función de cumplimiento es aquella que busca ofrecer ayuda a los bancos para una adecuada gestión de los riesgos de cumplimiento, tanto en regulación como prevención de pérdidas financieras y de su reputación (2014). Con ello, permite que las instituciones financieras realicen un análisis para mitigar la materialización de los mismos y sus negativas consecuencias que no solo repercuten en su capital, sino también a nivel reputacional.

Dado que el término riesgos se entiende de forma general, la SBS realiza los clasifica en el artículo 23 de la Resolución SBS N° 271-2017. A efectos del análisis de la Resolución Directoral N.° 110-2024-JUS/DGTAIPD, objeto de estudio del presente trabajo, se destacan los siguientes:

1. Riesgo de reputación: Potenciales pérdidas generadas por un debilitamiento en la confianza generada hacia la institución cuando se ve comprometido el buen nombre y la integridad de la empresa. Este riesgo puede originarse como consecuencia de otros riesgos propias de las actividades de la organización.

2. Riesgo operacional: Potenciales pérdidas provocadas por el uso de procedimientos inidóneos, deficiencias de personal, fallas en los sistemas de TI o la concurrencia de sucesos externos. Comprende el riesgo legal, mas excluye al estratégico y al reputacional.

Ambas tipologías se relacionan con la gestión inadecuada de procesos, pues de las fallas operativas puede desprenderse un riesgo reputacional, dependiendo del impacto que estas generen en la imagen y confianza del banco en el mercado. Así ocurrió en el caso del BCP, en el que la infracción impuesta por la ANPDP derivó, por un lado, en una multa que afectó su capital interno y, por otro, en un daño reputacional acerca de la solidez de su sistema de compliance.

Es así que, se construye la organización y estructura de la función de compliance, la cual se articula en cuatro ámbitos esenciales: i) identificar y analizar las exigencias normativas para determinar su incidencia en la actividad empresarial; ii) elaborar y aplicar mecanismos de control y detección de conductas irregulares o infracciones; iii) verificar la observancia de dichas exigencias por los miembros de la organización y iv) capacitar, sensibilizar y asesorar a los individuos responsables para garantizar su cumplimiento (Dill, 2019). Estas fases propuestas por Dill constituyen las directrices que entidades financieras como el BCP deberían adoptar para asegurar una gestión integral del riesgo normativo, fortalecer la cultura organizacional de cumplimiento y garantizar la sostenibilidad de sus operaciones en un entorno regulatorio cada vez más exigente como lo es la protección de datos personales, que cada vez adquiere mayor rigidez normativa.

En las primeras fases de gestión de riesgos que propone Dill, el banco debe medir su riesgo de cumplimiento y calcular los costos necesarios para reducirlo

a un nivel aceptable. La clave está en que los gastos de control suelen ser mucho menores que las pérdidas derivadas de un eventual incumplimiento (Rodriguez, 2024, pp. 21). En ese sentido, gestionar riesgos no implica únicamente la prevención de resultados adversos, sino también que los favorables coadyuven a fortalecer el desempeño global y corroborar que un negocio es rentable (McGrath y Jonker, s/f). Para ello, debe entenderse que el cumplimiento no es solo un requisito legal, sino una inversión estratégica que protege la sostenibilidad y reputación del banco.

De forma adicional, todo lo previamente mencionado no termina de hacer efectivo el compliance, sin la participación de dos elementos: el Officer Compliance, quien es el encargado de supervisar que se implemente el programa preventivo; y el Programa de Cumplimiento, cuyo contenido debe incluir normativa la normativa vinculada a la prevención, un plan de seguimiento a los procesos de riesgo, así como la implementación de instrumentos preventivos requeridos por la SBS (Diaz y Goitia, 2025, pp. 26). Esto permite que la gestión de riesgos pueda ser implementados, supervisados y puestos en práctica, caso contrario, es ineficiente que las instituciones financieras realicen una gestión que solo quede en el papel.

Al respecto, la SBS (2019) indica que la implementación de sistemas de compliance aspira a transformarse en una actividad común y esencial para cualquier organización. Únicamente de ese modo podrá ser posible obtener una gestión eficiente de las empresas, donde se proteja la reputación institucional y, al mismo tiempo, se fomente una cultura ética, generando múltiples impactos positivos para la sociedad.

De este modo, el compliance en las entidades financieras se configura no solo como una exigencia regulatoria impuesta por la SBS, sino como un instrumento indispensable en la prevención de riesgos, la protección de datos personales y la preservación de la confianza de los usuarios, de modo que su adecuada implementación, a través de programas y oficiales de cumplimiento, garantiza una gestión eficiente de las potenciales amenazas y la sostenibilidad de la institución en un entorno regulatorio cada vez más exigente.

## 1.2. El Test de Proporcionalidad en la evaluación de riesgos

La evaluación de riesgos permite identificar cuáles son los riesgos a los cuales está expuesta una organización durante el flujo normal de sus operaciones. Para el presente se plantea de forma específica la evaluación enfocada en la protección de datos personales. Es así que, un manejo responsable de la información personal es clave para reducir riesgos legales, resguardar la imagen de la entidad y prevenir posibles pérdidas financieras (Pineda y Larrota, 2023, pp. 12). Se entiende entonces que, esta evaluación como parte del programa de prevención de riesgos, bajo su enfoque preventivo, puede implementar el criterio de proporcionalidad que permita evaluar la medida menos lesiva en el tratamiento de información personal y sensible de los usuarios, lo cual permitirá que la alta dirección tome decisiones adecuadas para evaluar el impacto de su protección.

Cabe destacar la existencia de determinadas resoluciones que reafianzan la necesidad del test de proporcionalidad como mecanismo preventivo. Así pues, la Resolución 065-2016-JUS/DGPDP sancionó a la Clínica Good Hope por solicitar datos sensibles sobre creencias religiosas que no eran necesarios para la prestación del servicio médico. Este precedente evidencia que la proporcionalidad exige limitar la recolección a lo estrictamente indispensable, evitando tratamientos excesivos de datos sensibles.

Asimismo, la Resolución Directoral N.º 240-2019-JUS/DGTAIPD-DF, se basa en un procedimiento sancionador de la ANPDP a la Universidad Femenina del Sagrado Corazón por recolectar y difundir imágenes sin un consentimiento válido. Esto evidencia que, en el tratamiento de datos sensibles, no basta con justificar su necesidad: la autoridad exige además un consentimiento específico, informado y debidamente acreditado. Este precedente refuerza la importancia de evaluar necesidad y validez del consentimiento como condiciones inseparables.

En ese sentido, de acuerdo con la Sentencia N° 0045-2004-AI, el test de proporcionalidad contiene tres elementos: la idoneidad es un análisis de la

relación del medio y fin, mediante el elemento de la necesidad se evalúa si existen otros medios alternativos menos gravosos, y mediante el elemento de la ponderación se realiza un análisis comparativo en el que cuanto mayor intensidad en la intervención o afectación del derecho hay, tanto mayor habrá de ser el grado de realización. Esto es importante debido a que, conforme a Hernández se deben considerar tales elementos de la siguiente manera:

- Idoneidad: se debe determinar si lo propuesto alcanza la eficacia necesaria para los fines que persigue (2025, pp. 100). Para el caso específico, el banco debe determinar si las medidas utilizadas para obtener datos sensibles cumple con el fin de prevenir usurpaciones de identidad o fraudes en las operaciones financieras, lo cual, conforme a los descargos realizados por BCP en la Resolución Directoral N° 110-2024-JUS/DGTAIPD; permitiría contar con certeza de quién interpone un reclamo digital, pues la validación mediante biometría facial cuenta con patrones que garantizan la autenticidad de las personas.

- Necesidad: verificar si la finalidad que se persigue se puede conseguir de una forma menos lesiva, este elemento aplicado en datos personales consigue alcanzar el objetivo de la transparencia de la información (2025, p. 101). Así pues, la Dirección de Protección de Datos Personales en esta Resolución comenta que el BCP debió haber considerado medidas menos lesivas.

  Esto evidencia que el banco no implementó este criterio de forma preventiva a la recolección de datos biométricos faciales, pues si bien existen reclamos vinculados a operaciones financieras, también existen reclamos que no lo vinculan. Por lo que, como primer error, la aplicación generalizada de este requisito no superaría el elemento de la necesidad. Así también, existirían medios menos lesivos de comprobación, tales como el envío de un código único mediante mensaje SMS para confirmar la imposición de un reclamo.

- Proporcionalidad: para evaluar una medida vinculada al tratamiento de datos, debe analizarse la magnitud del riesgo para los derechos y la privacidad. También se requiere verificar que sea adecuada y proporcional. El juicio final consiste en ponderar si los beneficios sociales superan las afectaciones a otros derechos, de manera y objetiva (2025, p. 101).

  Aplicado al caso objeto de análisis, el banco debe validar si contar con la autenticación de datos biométricos faciales supera la afectación al artículo 2.6 de la Constitución Política del Perú: “Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias”. Este derecho no es absoluto, pues en determinados supuestos no sería vulnerado (Miranda, 2021, p. 8). Por lo que, debería justificarse que la vulneración de este derecho satisface un interés mayor.

  En ese sentido, considerando que, en el elemento de la necesidad, se verifica que existirían medidas menos lesivas, entonces la recolección de datos biométricos no supera la afectación de la intimidad personal.

A ese entender, en el uso de datos biométricos, como parte del análisis de la proporcionalidad que se propone, las entidades financieras deben considerar que, la normativa peruana mantiene coherencia la legislación empleada a nivel internacional, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea que, de igual forma, considera la especial necesidad de su protección (Champi y otros, 2025, p. 16). De acuerdo a lo mencionado en párrafos previos, los datos sensibles son mayormente protegidos debido a que su uso vulnera el derecho a la intimidad.

En adición, la ANPDP, en su Opinión Consultiva N.º 36-2020-JUS/DGTAIPD, establece en el numeral 35, con base en los artículos 9 y 16 de la LPDP, que los encargados de manejar datos personales tienen la obligación de adoptar medidas legales, técnicas y organizativas que aseguren su protección integral, evitando riesgos como el acceso indebido, la alteración o la pérdida de información Estas disposiciones refuerzan el enfoque preventivo del

cumplimiento normativo en este ámbito, cuyo propósito es garantizar que la protección de la información no se limite a un cumplimiento formal, sino que se integre de manera efectiva en los lineamientos internos de las instuticiones financieras.

### 1.3. Evaluación de Impacto en la recolección de datos sensibles

Posterior a que se haya realizado el test de proporcionalidad, y se haya determinado viable implementar nuevas medidas para el tratamiento de datos sensibles, debe realizarse una Evaluación de Impacto en Protección de Datos (EIPD) que determine el grado de afectación a los titulares de los datos. Es preciso resaltar que, esta medida se encuentra plasmada en el artículo 40 del Reglamento de la Ley N° 29733; sin embargo, es de forma facultativa, mas no obligatoria. Por lo que, se propone que esta forme parte del programa de prevención de riesgos de una forma obligatoria.

Conceptualmente, la evaluación de impacto es un mecanismo preventivo para analizar los posibles riesgos asociados a un tratamiento antes de ejecutarlo. Permite identificar amenazas a la privacidad, valorar su gravedad y definir medidas para evitar, reducir o gestionar dichos riesgos cuando se implementen nuevos procesos, servicios o tecnologías (Gadea, 2020, pp. 50). En ese sentido, esta evaluación permite validar que el impacto del tratamiento de datos sensibles sea el menor y permite que la alta dirección decida sobre ello.

Los pasos con los que debe contar la evaluación, conforme a lo sugerido por Rodríguez se basan en: analizar su necesidad, debe justificarse por qué se va a realizar la evaluación; detallar el periodo de duración de los datos; efectuar un análisis de la necesidad y proporcionalidad del manejo; gestión de riesgos; plan de acción que es el que contendrá las medidas que mitigarán la materialización de riesgos; supervisar y revisar la implantación, debe haber un seguimiento que garantice el cumplimiento normativo (2020, pp. 45-46). De estas fases, algunas se tienen recubiertas por el elemento descrito en el punto anterior, como la evaluación de necesidad y proporcionalidad, y los instrumentos de gestión de riesgos.

Es importante definir un responsable del tratamiento de la EIPD, que debe apoyarse de un encargado, y un delegado de la protección de datos que va a asesorar al responsable del desarrollo de la EIPD. (Montesinos, 2022, pp. 36). De esta manera, la EIPD se desarrolla con roles definidos y supervisión especializada, asegurando rigor técnico y cumplimiento normativo en todo el proceso.

Respecto al encargado de proteger la información, esta responsabilidad puede recaer sobre el Oficial de Datos Personales que se plantea en el Reglamento de la Ley N° 29733, quien conforme al numeral 17 del artículo III es el encargado de la supervisión, asesoramiento e incorporación del cumplimiento normativo sobre la protección de datos personales. De forma complementaria, el artículo 38 designa un perfil en el que este debe contar con cualidades que acrediten que tiene conocimiento y práctica en materia de datos personales. En tal sentido, este resulta ser una figura importante y necesaria que garantice la eficacia del desarrollo de la EIPD.

Ahora bien, considerando la NTP ISO 31000, una vez que se han identificado los riesgos, el tratamiento de estos implica la selección e implementación de opciones que los modifiquen. Así, se configura un proceso cíclico en el que se define el tratamiento aplicable, se determina si el nivel de riesgo residual es tolerable y, de no serlo, se generan nuevas medidas, evaluando continuamente su eficacia. En consecuencia, el riesgo puede evitarse, aceptarse, eliminarse o modificarse en su probabilidad y consecuencias (2016, p. 30). De esta manera, permite gestionar los riesgos del tratamiento de datos sensibles mediante un proceso estructurado, verificable y orientado a la mejora continua.

De la NTP-ISO/IEC 27005:2018 se extraen elementos esenciales para sustentar la EIPD, como la identificación de activos, amenazas y vulnerabilidades; el análisis del impacto sobre la reserva, integridad y accesibililidad; la definición de criterios de riesgo y niveles aceptables; la selección de opciones de tratamiento y la necesidad de un ciclo continuo de revisión y documentación del proceso. Estos componentes complementan el enfoque del Test de Proporcionalidad y

permiten integrar la EIPD como un control técnico y operativo dentro del Programa de Prevención de Riesgos.

Considerando que, una vez que se haya implementado una medida, como parte de la EIPD, debe haber un seguimiento a que exista cumplimiento normativo; por lo que las normas ISO/IEC 27701: 2019 brinda los lineamientos para administrar y gestionar adecuadamente los datos, así como salvaguardar la privacidad de la información que permite identificar a las personas (GlobalSuite, 2023). Es decir, perfecciona la gestión de datos, y garantiza a las entidades la salvaguarda de la privacidad de los datos.

La aplicación de esta normativa posibilita que las entidades acrediten su compromiso con la protección de los datos personales, al adoptar controles especializados y actualizar de forma permanente sus prácticas en materia de privacidad (International Organization for Standardization, 2019). Esto se garantiza mediante la identificación y gestión de riesgos, y la identificación del impacto de su exposición.

En conjunto, estos estándares permiten que la Evaluación de Impacto en Protección de Datos se incorpore como un procedimiento sólido, verificable y alineado con prácticas internacionales. Su integración en el Programa de Prevención de Riesgos no solo ordena el tratamiento de datos sensibles bajo criterios técnicos y normativos, sino que establece una organización definida para la toma de decisiones y el seguimiento continuo de las medidas implementadas, asegurando que cualquier tratamiento futuro se gestione con un nivel adecuado de diligencia y coherencia interna.

2. ¿Qué buenas prácticas internacionales (por ejemplo, de Chile, Colombia y España) podrían servir de referencia para fortalecer la prevención de infracciones administrativas en el sistema financiero peruano?

La evolución en la protección de datos personales en Latinoamérica se ha producido debido a un incremento sustancial en el flujo de datos entre los distintos países de la región, producto de la integración a nivel económico y

social, así como un aumento en los intercambios con agentes públicos y privados (Milanes, 2017, p.16). Debido a ello, los países buscan perfeccionar su marco normativo en materia de protección de datos personales con el fin de proteger la privacidad de la información personal. Actualmente los datos de las personas son recolectados, almacenados y tratados en cada operación diaria (p. 17).

Es así que la legislación peruana en protección de datos personales forma parte de un ecosistema regional y global en el que los países, sobre todo, latinoamericanos enfrentan desafíos similares derivados de la globalización y su rápido avance en el ámbito de recolección permanente de información. En el sector financiero, estos sistemas se encuentran cada vez más digitalizados, tal es así que su evolución proviene desde el reconocimiento del derecho a la privacidad por el artículo 12 de la Declaración Universal de Derechos Humanos hasta consolidarse como un eje fundamental en el marco jurídico digital contemporáneo (Solove, 2019).

En el contexto latinoamericano, la mayoría de países reconocen el derecho a la protección de datos personales en sus respectivas constituciones, aunque con enfoques y alcances distintos. Entre ellos se encuentran Argentina, Brasil, Colombia, México, Perú y Venezuela.

Así, resulta necesario poder realizar una evaluación comparativa del estado regional de la cuestión, donde se tenga presente cómo van evolucionando los sistemas Peruano, Chileno y Colombiano en materia de datos personales, los cuales comparten una arquitectura legal basada en principios europeos, derechos ARCO, deberes de seguridad, supervisión administrativa, consentimiento como base general y un régimen sancionador para proteger los datos personales.

Es en base a que estos tres países rigen su normativa en principios europeos, que cogen el modelo español para su implementación. Por lo que, debe realizarse un breve análisis de este sistema, que permita reflexionar acerca de las necesidades regionales y deficiencias que perfeccionen la normativa nacional

en materia de datos personales, e incentiven a las empresas a contar con un modelo de prevención acorde a los lineamientos normativos.

Por ejemplo, en Chile, la Comisión para el Mercado Financiero ha adoptado marcos de gestión de riesgos basados en estándares internacionales que integran la seguridad informática con la protección de datos (CMF, 2023). Asimismo, en Colombia, la Superintendencia Financiera exige evaluaciones de impacto en privacidad como condición previa para el despliegue de tecnologías de autenticación reforzada (SFC, 2022). Finalmente, en España, la coordinación entre el Banco de España y la Agencia Española de Protección de Datos ha permitido desarrollar parámetros vinculantes para garantizar la proporcionalidad tecnológica en el sector bancario (AEPD, 2020).

Estas experiencias permiten observar que la integración entre protección de datos y supervisión bancaria no es una tendencia aislada, sino un estándar regulatorio emergente. En esa línea, el análisis de estos modelos comparados permitirá identificar buenas prácticas que podrían servir de referencia para crear un módulo de compliance en protección de datos dentro de las entidades financieras peruanas

### 2.1. La protección de datos personales en el sistema normativo peruano

El derecho a la protección de datos personales obtiene reconocimiento constitucional en base al inciso 6 del artículo 2, que señala lo siguiente: “A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”. Asimismo, también se encuentra previsto como uno de los derechos tutelados por el proceso constitucional Habeas Data, regulado por el artículo 200.3,

Asimismo, la Ley N° 29733 Ley de Protección de Datos Personales busca salvaguardar el derecho fundamental a la protección de datos de las personas y regula la gestión legítima de su información personal por medio de la Autoridad Nacional de Protección de Datos Personales y el Reglamento de la referida ley.

Así pues, en el aspecto sancionador, para garantizar la tutela de los bienes jurídicos relacionados con el interés general, nuestro sistema jurídico otorga a la Administración Pública diversas facultades propias del derecho público, a través de las cuales se hace efectivo el ejercicio del poder de imperio del Estado (Gomez y otros, pp. 33). Esta potestad sancionadora le es otorgada a la ANPDP.

La Ley N° 29778, Ley de Protección de Datos Personales, en su artículo 38 establece cuáles son las infracciones al incumplimiento de sus disposiciones, o las de su Reglamento, y las clasifica en leves, graves y muy graves. Las infracciones leves implican una multa desde 1 hasta 5 UIT, y corresponden a faltas de comunicación oportuna sobre el tratamiento de esta información o la falta de inscripción del banco de datos personales ante las autoridades correspondientes. Las graves se castigan con multas entre más de 5 y 50 UIT, y ocurren cuando se recopilan datos sin consentimiento, no se garantizan los derechos ARCO o faltan medidas de seguridad adecuadas. Finalmente, las muy graves implican multas de más de 50 hasta 100 UIT y se configuran al transferir datos sin autorización, tratarlos de manera indebida o actuar con negligencia en su gestión (Champi y otros, 2025, p. 17).

Asimismo, existe una serie de principios que rigen el tratamiento de datos personales, dentro de las cuales se destacan de la Ley N° 29733: el de legalidad, que exige que se efectúe con todas las garantías de la ley y sin recurrir a medios ilícitos o engañosos; el de consentimiento, que requiere que el titular haya autorizado el manejo de sus datos de manera previa, expresa e informada; el de finalidad, que limita el uso de los datos únicamente a propósitos lícitos, específicos y previamente informados; y el de proporcionalidad que sostiene que la necesidad de que la recopilación de estos datos para alcanzar un fin en específico. Estos principios buscan evitar la utilización inadecuada de los datos, garantizando que su manejo sea legal, con consentimiento del titular y para fines legítimos y seguros (Champi y otros, 2025, p. 17).

Tratándose de casos en los que las infracciones son derivadas del uso de tecnologías, el uso de esta conlleva a modelos de procesamiento de datos innovadores, variados e intensivos, que debe adecuarse a la legislación sobre

protección de datos y con respeto a la dignidad de los titulares de la información que es objeto de tratamiento (Zamudio, 2024, pp. 329). Parte de este tratamiento implica el consentimiento de los titulares, el cual debe ser avisado, informado, expreso e inequívoco. (Defensa Popular, 2019). Como señala Auccatoma (2023), esta autorización se puede brindar verbalmente o de forma escrita. No obstante, resulta imperativo contar con la formalidad cuando se tratan datos sensibles (p. 20).

Los casos en los que no se requiere del consentimiento del titular, los establece la Ley N° 29733, que se da cuando son adquiridos por entidades estatales para cumplir sus funciones, provienen de fuentes accesibles al público, resultan necesarios para ejecutar contratos, atender emergencias médicas o fines de salud bajo secreto profesional, o pertenecen a miembros de organizaciones sin fines de lucro. De tal forma, se plantea como uno de los fundamentales requisitos para la recolección y tratamiento de datos personales, una autorización previa de su titular.

En ese sentido, los titulares de bancos de datos personales tienen la obligación de proteger dicha información, a fin de resguardar el derecho de los titulares y prevenir las infracciones que pudieran derivarse de su vulneración, que tiene como consecuencia la imposición de multa y otras sanciones. Por lo tanto, en base al principio de seguridad, estos titulares deben internalizar los mecanismos a nivel técnico, legal y organizacional para asegurar cumplir con los estándares de reserva, integridad y accesibilidad y, con ello, evitar la pérdida, manipulación o desviación de la información, realizada con o sin intención, así como cualquier manejo de estos datos que se efectúe al margen de la ley (Alvarado, 2016, p. 28).

En esa línea, la gestión propicia del riesgo de cumplimiento en materia de protección de datos se configura como un instrumento estratégico para garantizar la sostenibilidad institucional y la legitimidad frente a un entorno regulatorio cada vez más estricto.

### 2.2. La protección de datos personales en el sistema normativo chileno

La ley que aborda la materia de los datos personales en Chile es la ley N° 19.628, su aprobación marcó un momento decisivo en la evolución normativa latinoamericana, al convertir a Chile en el primer país de la región en abordar legislativamente la protección de datos personales. Sin embargo, progresivamente, tanto la doctrina como la jurisprudencia han puesto de relieve que, pese a su carácter pionero, la norma adolecía de múltiples vacíos y limitaciones que dificultaron su aplicación práctica y evidenciaron la necesidad de una regulación más robusta y actualizada (Quezada, 2019, pp. 28)

Así pues, los diferentes proyectos de ley que se propusieron con el fin de modificar la norma chilena dan evidencia de la negativa que recibía esta norma, en base a que se percibía esta como incompleta o una que realmente no velaba por la protección de los datos personales (Jervis, 2006, pp. 32). Por todo esto, el modelo normativo ha buscado perfeccionarse conforme a los nuevos contextos que han puesto en exposición de vulneración el derecho a la privacidad de los chilenos.

En esa línea, el sistema chileno se encuentra en constante revolución hacia la digitalización de la información; es así que, surgen beneficios en transformación tecnológica; así como posibles vulneraciones al tratamiento de la información. En respuesta a estas nuevas exigencias, la protección de los datos personales aparece como un derecho humano reciente e independiente, desarrollado precisamente frente al avance de las tecnologías modernas (Contreras, 2020).

En suma a esta necesidad de mejorar el tratamiento de datos personales, mediante una encuesta realizada el año 2022 por parte del Servicio Nacional del Consumidor, existe un porcentaje muy reducido de la población (4,1%) que manifiesta leer con frecuencia las políticas de privacidad de las plataformas digitales a las que ingresa. Este hecho, genera lo que se conoce como “paradoja de la privacidad”, especialmente si consideramos que, en esta misma encuesta, el 72% de los ciudadanos expresa su preocupación porque sus datos estén siendo recabados en Internet (Pinto, 2024, pp. 8).

Es claro que, el sistema chileno muestra una clara preocupación por conocer la percepción ciudadana de la situación de la protección de los datos personales, para establecer exigencias claras y precisas. Así pues, la ley que actualmente rige los datos personales es la ley N° 19.628 sobre Protección de la Vida Privada, la cual se complementa con la Ley N° 21.180 sobre Transformación Digital del Estado, que aumenta la tendencia a digitalizar los procesos administrativos, lo que eleva el riesgo de vulneraciones de derechos digitales Jara-Fuentealba & Jorquera-Cruz, 2021).

El modelo normativo chileno se alinea con los criterios del Reglamento General de Protección de Datos de la Unión Europea, considerado hoy el principal referente global en materia de resguardo de los derechos de las personas y de su información personal (Gobierno de Chile, 2024). Como se ha mencionado antes, las normas latinoamericanas en materia de datos personales se orientan del modelo europeo para realizar sus modificaciones normativas.

Es así que, existe una posición doctrinaria mayoritaria que sostiene que, en esta materia, las sanciones administrativas no buscan castigar, sino asegurar que los responsables cumplan los deberes legales y garanticen la privacidad y los derechos de los titulares. Se configuran, así, como herramientas para proteger el interés público asociado al tratamiento adecuado de la información personal. (Harris y otros, 2022, p.3). Se entiende que la validez de las sanciones administrativas, diferenciadas de las penales se basa en que, si bien ambos contienen un carácter sancionador, en términos administrativos las autoridades repelen el incumplimiento mediante este tipo de sanciones que no se catalogan como delitos.

En ese sentido, este tipo de sanciones se rige del principio de proporcionalidad que califica la gravedad del incumplimiento, la capacidad económica del infractor y las atenuantes que concurran en favor del infractor (p. 8). Es así que, en materia jurisprudencial, la Rol Nº 13.077-2022 indica que su principal objetivo no es exigir a cabalidad el cumplimiento de toda la normativa, evitar que se incurra en conductas revestidas por una gravedad considerable.

Así pues, en base a todos los criterios antes señalados, la nueva ley chilena N° 21.180, presenta una relación de conductas e infracciones: leves, graves y gravísimas, a las que atribuye multas de hasta 5.000 UTM, 10.000 UTM y 20.000 UTM, respectivamente. Esto permitirá que la Comisión Europea lo catalogue como un Estado en un nivel adecuado de protección de datos personales (Gobierno de Chile, 2024). Lo cual permite que Chile como país tenga mayor aceptación para el flujo transfronterizo de información, que producto de la globalización, se ha vuelto importante mantener un buen nivel en esta materia, pues fortalece las relaciones comerciales y garantiza los derechos humanos sobre privacidad.

### 2.3. La protección de datos personales en el sistema normativo colombiano

La regulación de los datos personales en Colombia surge como parte del Plan Nacional de Desarrollo 2010-2014, establecido mediante la Ley N° 1450 del 2011, que plantea como objetivo ingresar a la Organización para la Cooperación y el Desarrollo Económico (OCDE), hecho que le generaría una mejoría en su posicionamiento internacional. Así pues, el Ministerio de Tecnologías de la Información, la Comisión de Regulación de Telecomunicaciones y la Superintendencia de Industria y Comercio regularon la protección de datos personales conforme a los requisitos de la OCDE (Cabezas 2023, p. 3). Se tiene como incentivo para regular la materia, con el fin de promover el crecimiento económico, pues formar parte de esta organización permite que otros países califiquen de forma positiva a aquellos países miembros.

Para entender la importancia de los datos personales a nivel internacional, se deriva del flujo transfronterizo de estos, pues el aumento de frecuencia en la circulación de esta clase de información a nivel global ha generado la creación de reglas que buscan preservar los esfuerzos nacionales de protección de estos datos cuando se realicen transferencias entre países (Remolina, 2010, p. 496). Así pues, los países deben asegurar estándares adecuados de protección de esta información y ser catalogados como “buenos hospedadores de la información”, que permita que los datos de un país receptor tenga el mismo nivel de protección que el país receptor, lo cual afianza y expande las relaciones

comerciales, sobre todo con países europeos, que procuran mantener relaciones comerciales con países que contengan regulación en la materia.

La doctrina colombiana plantea que existe complejidad en el manejo de datos personales, pues Cabezas señala que el acceso automatizado a la información implica una responsabilidad elevada, que exige asegurar tanto los derechos de los titulares como el respeto de los principios que orientan la protección de datos como finalidad, libertad y seguridad, lo que requiere un tratamiento adecuado de dichos datos (2023, pp. 2). Resulta relevante tal propósito, siendo el que guía que no solo se busque regular el tratamiento de datos personales, sino que este sea adecuado.

Ahora bien, la Ley Orgánica de Protección de Datos Personales, Ley N° 1581, presenta de forma directa y sintetizada los artículos, acciones a cumplir y sanciones a aplicar, dejando de lado la ambigüedad. Esta misma ley se complementa con el Decreto Legislativo 1377, el cual cuenta con la multas y cuantías de estas, que pueden llegar a ser equivalentes a 2000 salarios mensuales legales (Sanlate y otros, 2013). Estas se gradúan en base a criterios tales como: la dimensión del daño; el beneficio económico que recibe el infractor; la reincidencia, la resistencia, negativa u obstrucción a la apertura de las investigaciones de la Superintendencia de Industria y Comercio (SIC); la renuencia o desacato de las disposiciones de la Superintendencia; el reconocimiento de la infracción (Escuela de Privacidad, 2021).

Son diferentes los criterios que van a definir tanto las infracciones en multas como en el flujo de la empresa, pues no solo se afecta el capital empresarial, sino también el giro del negocio y la confianza que tengan los inversionistas sobre las empresas sancionadas.

Colombia presenta un caso similar al analizado en el presente trabajo, respecto al uso de datos biométricos. El 09 de mayo del presente año, Mercado Libre Colombia fue multada con más de 214 millones de pesos colombianos debido a la exigencia del uso de datos biométricas para el acceso a la plataforma. Al respecto la Superintendencia resalta que la solicitud de este tipo de datos solo

se da en determinados casos permitidos por ley (Cruz, 2025). Como primer punto a resaltar, la regulación colombiana contiene de forma específica en sus leyes, las situaciones en las que las entidades públicas o privadas pueden acceder a datos sensibles.

Continuando, la SIC ordenó la censura de la medida adoptada por la empresa, así como también resalta que los datos personales recolectados deben respetar la finalidad de su propósito y deben ser recogidos conforme el cliente apruebe la medida y esté completamente informado sobre el uso y el tipo de información que se solicita (Cruz, 2025). Es decir, busca que exista un uso proporcional en el uso de datos sensibles, que exista consentimiento libre y expreso, y no subordinación a este mediante el acceso a plataformas web.

Posterior a esta sanción, la Dirección de Investigaciones de Protección de Datos Personales de la SIC orientó a Mercado Libre acerca de la adopción de mecanismos menos intrusivos que no transgredan los derechos de los titulares de los datos personales (Cruz, 2025). Esto demuestra que la entidad encargada de sancionar, en su interés de tutelar la protección de datos, busca mitigar la reincidencia mediante la orientación de medidas menos lesivas.

### 2.4. El modelo español en protección de datos personales

Tal como se ha referenciado en subcapítulos previos, el sistema latinoamericano se centra en el modelo europeo para regular la protección de datos personales. En tal sentido, de forma breve resulta necesario especificar cómo es este modelo, el cual se orienta del Reglamento General de Protección de Datos Personales que guía a toda la Unión Europea, que establece que cada estado miembro cuente con autoridades sancionadoras que controlen la aplicación y cumplimiento del Reglamento (Melis, 2020).

Es preciso mencionar que, si bien España se orienta del Reglamento que se rige en todo Europa, también cuenta con la Ley Orgánica de Protección de Datos Personales. Esta última también resulta aplicable a todo individuo cuyos datos sean tratados, sin importar su nacionalidad, asegurando que tanto residentes

como no residentes reciban las mismas garantías y derechos (Emancipatic, 2023).

En esa línea, la Ley Orgánica tiene por finalidad salvaguardar los derechos fundamentales y las libertades de las personas físicas con relación al uso de su información personal, poniendo especial atención en la defensa de su honor y en la preservación de su vida privada y familiar.

Así pues, este Reglamento crea nuevos derechos: transparencia de la información, derecho de supresión o “derecho al olvido”, limitación del tratamiento, y derecho a la portabilidad (Legal Veritas S/F). Entonces, este reglamento crea nuevos derechos de forma adicional a los derechos ARCO regulados por el sistema latinoamericano, sin dejar de contemplarlos en su marco regulatorio.

Las multas que establece el Reglamento parten desde los 90 euros hasta los 20 millones de euros o 4% de la facturación global de la empresa. Siendo los criterios para la graduación de las infracciones los enlistados a continuación: la infracción cometida; el volumen del negocio del infractor; la intencionalidad; el nivel de responsabilidad; la existencia o ausencia de un factor reincidente; la tipología de los datos personales y el grado de exposición; si el caso es objeto de conocimiento de la autoridad de control; la adhesión a los códigos de conducta y otros factores que incluyen el grado de beneficio (Melis, 2020). Son algunos de estos criterios los que también son considerados por los modelos peruano, colombiano y chileno para la graduación de la infracción.

En síntesis, el modelo europeo se ha consolidado como el referente central para la construcción de los sistemas latinoamericanos de protección de datos personales, no solo por su amplitud regulatoria, sino también por su enfoque en derechos fundamentales y por la precisión con la que define su régimen sancionador. La experiencia española evidencia cómo un país puede complementar el marco europeo con una normativa interna robusta que refuerce garantías y adapte principios comunes a su propia realidad jurídica. Esta articulación entre estándares supranacionales y legislación interna ha servido

como guía para países como Perú, Colombia y Chile, que han incorporado criterios similares en sus procesos sancionadores y en el reconocimiento de nuevos derechos. Con ello, la región avanza hacia marcos más coherentes, protectores y alineados con las exigencias globales en materia de privacidad y tratamiento responsable de la información personal.

## VI. CONCLUSIONES Y/O RECOMENDACIONES

Se cuentan con dos conclusiones a los problemas jurídicos desarrollados en el análisis; así como una conclusión general. Como primera conclusión, la implementación de los elementos: Criterio de Proporcionalidad en la Evaluación de Riesgos y Evaluación de Impacto de Protección de Datos como parte del Programa de Prevención de Riesgos de las entidades financieras, va a permitir que de forma preventiva a la implementación de medidas que versen sobre el tratamiento de datos sensibles, se realice una evaluación minuciosa tanto de la proporcionalidad en el sentido de elegir la medida menos lesiva luego de realizar el test de proporcionalidad; así como la decisión sobre el impacto del riesgo que genere. Con ello se reducirían las posibilidades de recaer en infracciones tales como la presentada en la resolución analizada en el presente informe.

Como segunda conclusión, el análisis comparado de Brasil, Colombia y España permite advertir que las buenas prácticas internacionales tienen tres elementos comunes que resultan directamente trasladables al sistema financiero peruano: del modelo colombiano se extrae la necesidad de implementar mecanismos de evaluación previa del impacto del tratamiento de datos personales; del modelo chileno, la adopción de marcos de gestión de riesgos normativos integrados a la supervisión financiera; y del modelo europeo se contiene la exigencia de criterios normativos claros para ponderar proporcionalidad y finalidad frente a mecanismos de autenticación reforzada.

Como conclusión general, las entidades financieras que por su naturaleza manejan volúmenes extensos de datos personales y sensibles de un gran sector poblacional, deben considerar que para poder mejorar la implementación de medidas, estas deben contar con un sustento legal por detrás, uno que se adhiera al cumplimiento normativo constante, pues la normativa que busca regular el tratamiento de datos personales están expuestas a constantes modificaciones, sobre las cuales, debe existir constante atención con el fin de validar que las medidas que usan los bancos, cumplen tanto por lo dispuesto por la norma sectorial de la SBS, como las normas en protección de datos.

En ese sentido, la Resolución Directoral N° 110-2024-JUS/DGTAIPD permite conocer que las entidades financieras pese a contar con modelos de compliance que fortalecen sus sistemas con el fin de mitigar riesgos, aún presentan deficiencias en la incorporación de herramientas para la recolección de datos, pues en el supuesto que el BCP hubiese considerado los elementos que se han propuesto en el desarrollo del presente trabajo; así como los modelos Brasileño, Colombiano y Español, hubiesen reafianzado sus procesos y ampliado la gama de opciones a considerar para mantener el acceso a sus sistemas de forma robustecida tal como lo plantea la Resolución N° 504-2021-SBS sin transgredir la Ley N° 29733 ni su Reglamento.

## BIBLIOGRAFÍA


Abdo León, L. B. (2024). *Responsabilidad bancaria: manejo de datos personales y la violación a la privacidad del deudor* (Bachelor's thesis, Universidad del Azuay).

Auccatoma Gozme, E. (2023). Análisis del Impacto de la Ley de Protección de Datos Personales del consumidor peruano en empresas comerciales".

Autoridad Nacional de Protección de Datos Personales (ANPDP). (s. f.). *Institucional*. Recuperado de https://www.gob.pe/institucion/anpd/institucional

Autoridad Nacional de Protección de Datos Personales (ANPDP). (2021). Opinión Consultiva N.° 032-2021-JUS/DGTAIPD: Sobre los datos biométricos y su empleo en la identificación de personas, el tratamiento de datos personales, la obtención del consentimiento, la conservación de documentos digitales, la atención de derechos ARCO y registro de bancos de datos. https://www.gob.pe/institucion/anpd/informes-publicaciones/2082384-oc-n-032-2021-jus-dgtaipd-sobre-los-datos-biometricos-y-su-empleo-en-la-identificacion-de-personas-el-tratamiento-de-datos-personales-la-obtencion-del-consentimiento-la-conservacion-de-documentos-digitales-la-atencion-de-derechos-ar

Alvarado, F. J. (2016). La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales. *Foro Jurídico*, (15), 26-41.

Arcos-Argudo, M., Matute-Pinos, K., & Fernández-Mora, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. Revista Ibérica de Sistemas e Tecnologias de Informação, (E60), 100-114.

Artavia Murillo vs. Costa Rica (Fecundación In Vitro). Excepciones preliminares, fondo, reparaciones y costas. Serie C N° 257 (Corte IDH, 28 de noviembre de 2012).

Ayadi, R., Naceur, SB, Casu, B. y Quinn, B. (2016). ¿Importa el cumplimiento de Basilea para el rendimiento bancario?. Journal of Financial Stability , 23 , 15-32.

Bermeo-Pérez, S. K., Ureta-Arreaga, L. A., & Yamba-Yugsi, M. (2024). Gestión de protección de datos personales en el sector financiero popular y solidario. MQRInvestigar, 8(3), 3624-3638.

Cabezas Azuero, J. S. (2023). Tratamiento de datos personales y compliance en Colombia. Revista de la Facultad de Derecho y Ciencias Políticas, 53(138), pp. 1-25. doi: https://doi.org/10.18566/rfdcp.v53n138.a2

Concepción, R. (s. f.). *La relación entre el derecho administrativo y el derecho financiero*. Scribd. Recuperado de https://es.scribd.com/document/769731998/La-relacion-entre-el-derecho-administrativo-y-el-derecho-financiero

Contraloría Ciudadana. (2020, 15 de enero). El origen del compliance. https://www.contraloriaciudadana.org.mx/es/comunicacion/el-origen-del-compliance.html

Champi Zavaleta, L. A., Del Aguila Rodriguez, B. X., Garcia Martinez, A. F., & Meneses Oriundo, Y. L. (2025). Análisis de la eficacia normativa de la Ley de Protección de Datos Personales en el sector empresarial financiero: Propuesta de mejora del marco normativo para el fortalecimiento de la Ciberseguridad Corporativa.

Crovi, D. (2005). La sociedad de la información: una mirada desde la comunicación. Revista Ciencia, 56(oct-nov.), 23-37.

Cruz Marroquín, M. J. (2025, 9 de mayo). SIC anuncia millonaria sanción a Mercado Libre por exigir datos biométricos para el acceso a la plataforma. El Tiempo. https://www.eltiempo.com/economia/empresas/sic-anuncia-millonaria-sancion-a-mercado-libre-por-exigir-datos-biometricos-para-el-acceso-a-la-plataforma-3452096

Davalos Guillen, A. J., & Mujica Sanchez, M. L. (2024). Ciberseguridad y vulneración de datos personales en entidades financieras, Lima 2022.

Defensoría del pueblo. (2019). Manual de Protección de datos personales. Defensoría del Pueblo, Lima. Obtenido de https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-deProtecci%C3%B3n-de-Datos-Personales.pdf

De La Haza Barrantes, A. (2016). No se lo digas a nadie, pero tengo un banco de datos de clientes sensibles, la gestión de la protección de datos personales en el sistema financiero para la prevención del lavado de activos. *Revista Actualidad Mercantil*, (04), 74-93.

Diaz Pari, A. C. C., & Goitia Cardenas, S. E. (2025). Los delitos informáticos y el compliance en las entidades financieras en Lima Metropolitana, 2024.

Diaz Romero, B. (2024). La transformación digital del Estado y el derecho a la protección de datos personales. Gobierno Y administración pública, (7), 15-27. https://doi.org/10.29393/GP7-2DEDR10002

Dill, A. (2019). Bank Regulation, Risk Management, and Compliance : Theory, Practice, and Key Problem Areas (Edition 1) (1st ed.). Routledge. Disponible en: https://doi.org/10.4324/9780429351167

Eguiguren, Francisco. (2015) “El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú.” THĒMIS-Revista de Derecho, no. 67.

Emancipatic. (s. f.). Protección de datos personales: Todo lo que necesitas saber. Recuperado de https://www.emancipatic.org/proteccion-de-datos-personales/

EscueladePrivacidad.co. (2021, 22 de abril). Sanciones por incumplimiento del régimen de protección de datos personales: modelo europeo y Colombia. Recuperado de https://escueladeprivacidad.co/2021/04/22/sanciones-por-incumplimiento-del-regimen-de-proteccion-de-datos-personales-modelo-europeo-y-colombia/#:~:text=En%20el%20caso%20colombiano%2C%20las,sanci%C3%B3n%20a%20que%20hubiere%20lugar

Gobierno de Chile. (27 de agosto de 2024). Ley de protección de datos personales: aprobación eleva estándar de derechos. Recuperado de https://www.gob.cl/noticias/ley-proteccion-datos-personales-aprobacion-eleva-estandar-derechos/

Gordon, P. L., Varela, J. C., & Sanlate, G. (2013, 29 de julio). Colombia adopta normas sobre la protección de datos personales: Aplicación y sanciones en caso de incumplimiento. Littler. https://www.littler.com/news-analysis/asap/colombia-adopta-normas-sobre-la-proteccion-de-datos-personales#:~:text=Aplicaci%C3%B3n%20y%20sanciones%20en%20caso,establecidas%20en%20las%20normas%20estudiadas

GlobalSuite Solutions. (s. f.). New ISO/IEC 27701:2019 [Artículo web]. Recuperado de https://www.globalsuitesolutions.com/es/iso-iec-27701-2019/

Harris Moya, P., Wilkins Binder, J., Williams Obreque, G. & Bermúdez Soto, R. (2022, noviembre). Sanciones administrativas en materia de protección de datos personales (Asesoría Técnica Parlamentaria Nº SUP 136.728). Biblioteca del Congreso Nacional de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio%2F10221%2F33803%2F1%2FBCN_Sanciones_Administrativas__2022.pdf

Herrera, E.; Barrera, K. & Rodríguez, I. (2023). Responsabilidad penal de las personas jurídicas en Perú: una reevaluación del aforismo societas delinquere nec punire potest a partir de una perspectiva anticonceptualista. Revista Direito GV, 19(23), 1-26. http://surl.li/wqbchc

Instituto Nacional de Calidad. (2016). *NTP ISO 31000:2016. Gestión del riesgo – Directrices*. INACAL.

Instituto Nacional de Calidad. (2018). *NTP-ISO/IEC 27005:2018. Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información*. INACAL.

Jervis Ortiz, P. (2006). La regulación del mercado de datos personales en Chile.

Lapeyre Valderrama, C. E., & Anicama Seminario, J. C. (2023) Propuesta de un plan para la implementación de un sistema de gestión de la seguridad de la información, basado en la ISO/IEC 27001 para una empresa corredora de seguros.

Legal Veritas. (2021, 15 de septiembre). Nuevo Reglamento General de Protección de Datos, principales dudas y cuestiones. https://www.legalveritas.es/nuevo-reglamento-general-proteccion-datos-dudas-cuestiones/

López, J. M. H. (2025). Protección de datos, intimidad y acceso a la información pública. Ponderación y proporcionalidad. *Revista Canaria de Administración Pública*, (5), 73-105.

Melis, I. (2020, 11 de febrero). Aplicando el RGPD: quién, cuánto, cómo, a quién y qué se sanciona. KPMG Tendencias. https://www.tendencias.kpmg.es/2020/02/rgpd-aplicacion-sanciones/#:~:text=%C2%BFC%C3%B3mo?:%20Criterios%20de%20graduaci%C3%B3n,como%20beneficios%20obtenidos%2C%20p%C3%A9rdidas%20evitadas%E2%80%A6

McGrath, A., & Jonker, A. (s. f.). ¿Qué es la gestión de riesgos? IBM Think. Recuperado de https://www.ibm.com/mx-es/think/topics/risk-management

Miller, G. P. (2014). The Role of Risk Management and Compliance in Banking Integration.
New York: New York University Law and Economics Working Papers.

Ministerio de Justicia y Derechos Humanos. (2016). *Resolución Directoral N.º 065-2016-JUS/DGPDP, que sanciona a la Clínica Good Hope por tratamiento indebido de datos sensibles*. Dirección General de Protección de Datos Personales, Perú.

Ministerio de Justicia y Derechos Humanos. (2022). *Resolución Directoral N.º 013-2022-JUS/DGTAIPD, que confirma sanción a la Universidad Femenina del Sagrado Corazón por difusión no autorizada de imágenes personales*. Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, Perú.

Miranda Gonçalves, R. (2021). Consideraciones sobre el principio de proporcionalidad en los derechos fundamentales: mención especial a la videovigilancia masiva. *Revista de Direito da Faculdade Guanambi*.

Montesinos Rodrigo, L. (2022). *Guía para la realización del Privacy Impact Assestment (PIA, Evaluación de Impacto en la Protección de Datos Personales) para encargados y responsables de tratamiento de datos* (Doctoral dissertation, Universitat Politècnica de València).

Onetto, M. H. L. Open Banking: Desafíos de las Entidades Financieras a la protección de Datos Personales.

Pinto Iribarren, CJ (2024). Agencia de protección de datos personales: oportunidades y desafíos respecto a las recomendaciones OCDE.

Pineda Cano, L., & Larrota Lazo, L. M. (2023). Componentes Clave en Aseguramiento, Análisis de Riesgos y Evaluación de la Gestión en la Protección de los Datos Personales.

Protección de datos y seguridad de la información. (2023). *Revista Canaria De Administración Pública*, *1*, 285-311.

Quezada Santana, J. F. (2019). Análisis de uso de datos personales por instituciones bancarias y financieras.

Remolina-Angarita, N. (2010). ¿ Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. International Law, (16), 489-523.

Ríos, M. A. (2014). La función de Compliance y su importancia dentro de las instituciones financieras. UCEMA. Recuperado de: https://ucema.edu.ar/posgrado-download/tesinas2014/Tesina_MAF_UCEMA_Rios.pdf

Rodríguez Ferrer, M. (2020). *Guía para la evaluación de impacto requerida en el Reglamento Europeo de Protección de Datos* (Doctoral dissertation, Universitat Politècnica de València).

Rodríguez Luján, A. A. (2024). Aplicación del Soft Law en la implementación del Sistema de Gestión de Compliance de una entidad bancaria.

Rotondo Tornaría, F. (2021). Derecho Administrativo, big data y protección de datos personales. *Revista De Derecho Administrativo*, (20), 194–211. Recuperado a partir de https://revistas.pucp.edu.pe/index.php/derechoadministrativo/article/view/25208

Sebastián, M. A., & Vázquez, N. E. (2021). *Modelo de prevención para el tratamiento de datos personales* (Doctoral dissertation, Universidad Nacional de La Plata).

Soler, E. G. (2020). Análisis de riesgos y evaluación de impacto relativa a la protección de datos: su aplicación a las sociedades cooperativas. *Boletín de la Asociación Internacional de Derecho Cooperativo*, (56), 47-72.

Superintendencia de Banca, Seguros y AFP (SBS). (2019, noviembre). *Buenas prácticas para implementar el Compliance* [Boletín N.º 42]. Boletín SBS. Recuperado de https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/90

Superintendencia de Banca, Seguros y AFP (SBS). (2017, 18 de enero). *Reglamento de gobierno corporativo y de la gestión integral de riesgos* (Resolución SBS N.° 272-2017). https://www.sbs.gob.pe/Portals/0/jer/Auto_Nuevas_Empresas/Normas_Comunes/5.%20Reg.%20de%20Gobierno%20Corporativo_Res.%20SBS%20N%C2%B0%20272-2017.pdf

Superintendencia de Banca, Seguros y AFP (SBS). (s. f.). *La SBS y sus mandatos*. Recuperado de https://www.sbs.gob.pe/la-sbs-y-sus-mandatos

Zamudio Salinas, L. (2024). Perú: retos del derecho fundamental a la protección de datos personales. *Revista Peruana De Derecho Constitucional*, (15), 327–343. Recuperado a partir de https://revista.tc.gob.pe/index.php/revista/article/view/406

**ANEXOS**

# *Resolución Directoral N.º 110-2024-JUS/DGTAIPD*

Lima, 27 de diciembre de 2024

**EXPEDIENTE N.º** : 122-2023-JUS/DGTAIPD-PAS
**ADMINISTRADA** : **BANCO DE CRÉDITO DEL PERÚ S.A.**
**DENUNCIANTE** : [redacted]
**MATERIAS** : Principio de proporcionalidad y consentimiento en el tratamiento de datos personales

**VISTOS:**

El documento de fecha 30 de julio de 2024 (Registro N.º 000369052-2024MSC) que contiene el recurso de apelación presentado por el Banco de Crédito del Perú S.A. contra la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP, de fecha 01 de julio de 2024; y, los demás actuados obrantes en el Expediente N.º 122-2023-JUS/DGTAIPD-PAS.

**CONSIDERANDO:**

## I. ANTECEDENTES

1. El 02 de agosto de 2022[1], la señora [redacted] (en adelante, la denunciante) presentó denuncia contra el Banco de Crédito del Perú (en adelante, la administrada), donde reportó que la entidad estaba realizando el tratamiento de sus datos personales (estado civil, CUI, sexo, fecha de nacimiento, fotografía, ubigeo, fecha de inscripción, emisión y caducidad) que no son necesarios para cumplir con la finalidad de presentar un reclamo virtual, lo cual contraviene la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP).

2. Con Carta N.º 490-2022-JUS/DGTAIPD-DFI de 25 de octubre de 2022[2], la Dirección de Fiscalización e Instrucción (en adelante DFI) requirió a la administrada la siguiente información:

   - Detalle qué finalidad tiene el recopilar y almacenar la toma de fotografía del documento de identidad y la validación de biometría facial para las personas que presentan un reclamo, asimismo, si ello obedece a exigencias legales de la normativa del sector en el que desarrolla sus operaciones.

[1] Obrante en folios 1 al 51
[2] Obrante en folios 149 al 152.

- Detalle a qué banco de datos personales corresponden los datos personales que se recopilan y almacenan para presentar un reclamo ante su entidad.
- Detalle el procedimiento utilizado para la validación de biometría facial que realiza al momento de presentar un reclamo, para ello, debe incluir información sobre la tecnología que utiliza y el flujo que tiene la información a través de sus sistemas.
- Detalle las medidas de seguridad que han implementado en el procedimiento para presentar un reclamo ante su entidad.

3. Mediante Carta N.º 599-2022-JUS/DGTAIPD-DFI de 07 de diciembre de 2022[3], la DFI requirió a la administrada la siguiente información:

   - Señale, acredite y justifique el procedimiento que ha implementado para la interposición de reclamos de los clientes y no clientes del Banco, respecto al tratamiento de los datos personales.
   - Precise cuál es la relevancia de los datos personales requeridos para ingresar reclamos.

4. Con escrito presentado el 29 de diciembre de 2022 (Código de Registro N.°000511686-2022MSC[4]), la administrada dio respuesta al requerimiento de la DFI; informó que el requerimiento realizado con Carta N.º 490-2022-JUS/DGTAIPD-DFI ha sido atendido con escrito presentado el 14 de noviembre de 2022 (Registro N.°000450331-2022MSC[5]) y; además, solicitó el encausamiento de los expedientes 186-2022-DFI y 291-2022-DFI en un único expediente toda vez que, versan sobre la misma denuncia.

5. Mediante Proveído de 17 de febrero de 2023[6], la DFI dispuso la acumulación de los expedientes de fiscalización Nos. 186-2022-DFI y 291-2022-DFI, que versan sobre las denuncias presentadas por la denunciante.

6. A través del Informe de Fiscalización N.º 068-2023-JUS/DGTAIPD-DFI-EMZA de 7 de marzo de 2023[7], el analista legal de Fiscalización de la DFI informó sobre la fiscalización realizada a la administrada concluyendo lo siguiente:

   > *"BANCO DE CRÉDITO DEL PERÚ con RUC N.º 20100047218, estaría recopilando datos sensibles (imagen facial para validación biométrica), y los datos personales contenidos en las imágenes del documento de identidad de quienes formulan un reclamo ante su entidad, que no son necesarios, pertinentes y adecuados para la finalidad determinada, conforme a lo señalado en el numeral 3 del artículo 28 de la LPDP. Hecho que constituiría una presunta infracción, según lo regulado en el literal d), numeral 2, artículo 132 del RLPDP, esto es, "Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos.", dicha infracción es grave conforme al citado artículo."*

[3] Obrante en folios 52 al 56.
[4] Obrante en los folios 62 al 77.
[5] Obrante en los folios 154 al 161
[6] Obrante en los folios 78 al 81.
[7] Obrante en los folios 162 al 177.

7. Dicho informe fue notificado a la administrada con la Cédula de Notificación N.º 216-2023-JUS/DGTAIPD-DFI, el 8 de marzo de 2023[8]

8. El 21 de agosto de 2023, personal de la DFI ingresó al sitio web de la administrada, a fin de verificar la forma cómo se valida la identidad de los reclamantes[9].

9. Con Orden de Visita N.º 106-2023-JUS/DGTAIPD-DFI de 26 de setiembre de 2023[10], se ordenó realizar una visita de inspección complementaria a la administrada con la finalidad de verificar el procedimiento utilizado para la validación facial (verificación biométrica) implementado para la atención de sus clientes y usuarios de sus servicios en general que incluye el Libro de reclamaciones virtual.

10. La primera visita de fiscalización a la administrada se realizó el 26 de setiembre de 2023[11], anotándose en el acta de fiscalización la solicitud de reprogramación de la visita, debido a que el personal responsable del tratamiento de la base de datos "Biometría" estaba trabajando de manera remota.

11. El 27 de septiembre de 2023 se realizó la segunda visita de fiscalización a la administrada[12], consignándose en el acto de fiscalización respectiva.

12. Con Informe Técnico N° 107-2023-DFI-ORQR de 02 de octubre de 2023[13], el analista de fiscalización informó las siguientes conclusiones:

> *"**Primera.-** Se verificó que el BANCO DE CRÉDITO DEL PERÚ, hace uso del servicio de biometría facial, con la finalidad de validar la identidad de las personas que requieren presentar un reclamo virtual*
> ***Segunda.-** Se verificó que para el caso de personas que van a registrar un reclamo por primera vez y no han sido sometidas a una verificación biométrica facial previamente por el banco, se procede a su enrolamiento haciendo uso del servicio de consulta de datos provisto por el RENIEC, de donde se obtiene la ficha que incluye la fotografía que luego será empleada para el análisis biométrico.*
> ***Tercera.-** Se verificó que cuando una persona y/o cliente enrolado realiza una transacción, operación o reclamo que requiera una validación biométrica facial por segunda vez, es decir si con anterioridad el banco ya ha realizado una validación biométrica facial, en las consultas ya no es necesario el uso del servicio de consulta de datos provisto por el RENIEC, toda vez que las consultas son realizadas a la base de datos propia del banco a la cual han denominado base de datos BIOM (ORACLE 19C), donde se almacenan las imágenes de las personas y/o imágenes del documento de identidad de las mismas debidamente encriptadas.*
> ***Cuarta.-** BANCO DE CRÉDITO DEL PERÚ, ha evidenciado generar y mantener registros de evidencias producto de la interacción lógica, referentes al inicio de sesión, cierre de sesión y acciones relevantes de las actividades realizadas por los operadores de su base de datos "BIOM" y/o gestor de base de datos ORACLE 19C, cumpliendo lo establecido en el numeral 2 del artículo 39° del Reglamento de la LPDP.*
> ***Quinta.-** BANCO DE CRÉDITO DEL PERÚ ha evidenciado garantizar el respaldo de la información correspondiente a su base de datos "BIOM", a través de la generación de copias seguras y continuas, por lo cual cumple con lo establecido el segundo párrafo del artículo 40o del Reglamento de la LPDP."*

[8] Obrante en el folio 178.
[9] Obrante en folios 192 al 198.
[10] Obrante en folios 199 al 202.
[11] Obrante en folios 203 al 205.
[12] Obrante en los folios 206 al 216.
[13] Obrante en los folios 217 al 222.

13. Con Resolución Directoral N.º 232-2023-JUS/DGTAIPD-DFI de 13 de octubre de 2023[14], notificada a través de la Cédula de Notificación N.º 928-2023-JUS/DGTAIPD-DFI[15], la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por las siguientes presuntas infracciones:

> ***Hecho imputado N° 1:*** *Haber realizado el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, al recopilar la fotografía del Documento Nacional de Identidad - DNI y la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica (dato sensible). Datos personales que no son necesarios pertinentes ni adecuados para cumplir con la finalidad de identificar al reclamante. Incumpliendo la obligación establecida en los artículos 7 y numeral 3 del artículo 28 de la LPDP, lo que configuraría la infracción grave tipificada en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP.*
> ***Hecho imputado N° 2:*** *Haber realizado el tratamiento de los datos personales sensibles de los usuarios y clientes, al almacenar el dato biométrico referido a la imagen facial, en una base de datos propia, sin obtener válidamente el consentimiento del titular de los datos personales, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento, lo que configuraría la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP .*

14. Mediante escrito presentado el 08 de noviembre de 2023[16] (000521071-2023MSC), la administrada presentó sus descargos al procedimiento administrativo sancionador, a fin de que sean analizados por la autoridad instructora.

15. Con Informe N.º 008-2023-JUS/DGTAIPD-DFI de 23 de enero de 2024[17], la DFI emite Informe Final de Instrucción en donde se recomendó lo siguiente:

> *"1) Se recomienda imponer sanción administrativa de multa ascendente a veintisiete (27.00) U.I.T. al BANCO DE CRÉDITO DEL PERÚ S.A., por el cargo acotado en el Hecho Imputado N.° 01, por infracción grave tipificada en el literal d, numeral 2, del artículo 132° del RLPDP: "Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos".*
> *2) Se recomienda imponer sanción administrativa de multa ascendente a cuarenta y cinco (45.00) U.I.T. al BANCO DE CRÉDITO DEL PERÚ S.A., por el cargo acotado en el Hecho Imputado N.° 02, por infracción grave tipificada en el literal g, numeral 2, del artículo 132° del RLPDP: "Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley N.° 29733 y su Reglamento"*
> *3) Habiendo tomado conocimiento de la conducta de la administrada en relación a la posible afectación de los derechos del consumidor de los servicios financieros, se dispone, el envío de la copia de la denuncia presentada, al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, a fin de que actúe de acuerdo a sus competencias."*

16. Mediante Resolución Directoral N.º 018-2024-JUS/DGTAIPD-DFI de 23 de enero de 2024[18], la DFI dio por concluidas las actuaciones instructivas del procedimiento

[14] Obrante en los folios 223 al 255.
[15] Obrante en los folios 256 al 263.
[16] Obrante en los folios 265 al 281.
[17] Obrante en los folios 282 al 343.
[18] Obrante en los folios 344 al 348.

administrativo sancionador, disponiendo la remisión de los actuados a la DPDP, para su resolución en primera instancia. El Informe Final de Instrucción y la Resolución Directoral, fueron notificados a la administrada mediante Cédula de Notificación ° 069-2024-JUS/DGTAIPD-DFI[19].

17. Por escrito de 01 de febrero de 2024 (registro 000055458-2024MSC)[20], la administrada presentó su absolución al Informe Final de Instrucción.

18. El 27 de febrero de 2024, se llevó a cabo el informe oral solicitado por la administrada[21].

19. Con Carta N° 309-2024-JUS/DGTAIPD-DPDP[22] y N° 310-2024-JUS/DGTAIPD-DPDP[23], ambas, del 27 de febrero de 2024[24], la DPDP solicitó a la administrada remitir Documentos (contratos, convenios y/o adendas) suscritos con el Registro Nacional de Identificación y Estado Civil – RENIEC, en mérito de los cuales este último brinda los servicios de consulta de datos y provee las fichas que contienen las imágenes de rostros de los reclamantes, que son cotejadas con las imágenes de estos (tomadas desde su Libro de Reclamaciones Virtual).

20. A través del escrito presentado el 13 de marzo de 2024 (registro 000113250-2024MSC)[25], la administrada presenta información requerida a través de las cartas citadas de manera precedente.

21. A través de Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024[26], notificada a la administrada el 09 de julio de 2024 mediante Cédula de Notificación N.º 992-2024-JUS/DGTAIPD-DPDP[27], la DPDP resolvió lo siguiente:

> "**SE RESUELVE:**
> **Artículo 1**.- Sancionar al Banco de Crédito del Perú con la multa ascendente a veintisiete Unidades Impositivas Tributarias (27 UIT) por haber efectuado el tratamiento de datos sensibles (datos biométricos) que resultan excesivos, no necesario, adecuados ni pertinentes para el uso de su libro de reclamaciones virtual, en incumplimiento de lo dispuesto en los artículos 7 y numeral 3 del artículo 28 de la LPDP, configurando la infracción grave tipificada en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP.
>
> **Artículo 2**.- Sancionar al Banco de Crédito del Perú con la multa ascendente a treinta y seis Unidades Impositivas Tributarias (36 UIT) por haber efectuado el tratamiento de datos sensibles (datos biométricos) de los usuarios de su libro de reclamaciones virtual, sin su consentimiento válido contrariando lo dispuesto en el numeral 13.5 y 13.6 del artículo 13 de la LPDP y el artículo 12 del Reglamento de la LPDP; infracción grave tipificada en el literal b) del inciso 2 del artículo 132 del Reglamento de la LPDP.

---

19 Obrante en el folio 349.
20 Obrante en los folios 353 al 381.
21 Obrante en el folio 396.
22 Obrante en el folio 397
23 Obrante en el folio 403
24 Se advierte un error material de ambos documentos fechados el 27 de febrero de 2022.
25 Obrante en los folios 409 al 428.
26 Obrante en los folios 429 al 474
27 Obrante en los folios 486 a 487.

**Artículo 3.-** Imponer como medidas correctivas al Banco de Crédito del Perú las siguientes:

• Suprimir los patrones biométricos faciales almacenados en la base de datos "BIOM".

• Cesar el almacenamiento de patrones biométricos obtenidos desde la imagen facial de los usuarios de su libro de reclamaciones virtual, así como el uso de estos para la validación de las identidades de estos.

• Remitir documentación sustentatoria de la implementación de ambas medidas correctivas.

(…)"

22. Con escrito presentado el 30 de julio de 2024 (Código de Registro 000369052-2024MSC) la administrada presentó recurso de apelación contra la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP, argumentando lo siguiente:

**Respecto al Hecho imputado 1:**

i. Que la denunciante no cuestionaría que sus datos hayan sido utilizados con fines comerciales o de monetización, sino que su objeción se centraría en el uso de sus datos, en calidad de "cliente intermitente", como medida de seguridad en el libro de reclamaciones virtual.

ii. Que, a pesar de imponer la sanción, en el fondo la DPDP les habría dado la razón cuando concluyó que en ciertos escenarios es proporcional y necesario validar la identidad del usuario a través de su biometría, justificando esta medida por los niveles de seguridad requeridos para proteger los intereses patrimoniales del usuario.

iii. Que, la DPDP reconocería que el uso de la biometría para la verificación de identidad en el sistema financiero es justificado en el caso de clientes intermitentes cuando sus reclamos están relacionados con temas patrimoniales; sin embargo, la DPDP cometería el error al afirmar que este método de identificación solo estaría legitimado en casos excepcionales y no debería aplicarse en todos los casos, como en aquellos donde los clientes regulares optan por validar su identidad mediante biometría facial o en clientes intermitentes cuyos reclamos no parecen estar vinculados a temas patrimoniales.

iv. Que, los servicios brindados por el BCP estarían íntimamente relacionados con aspectos patrimoniales, por lo que, bastaría con que se trate de información financiera sensible y por lo tanto tendrían que tomar especiales medidas para cuidar de ello, no solamente cuando afectan directamente el secreto bancario. Asimismo, indica que no tendría sentido excluir a los clientes regulares de la necesidad de una adecuada verificación de identidad mediante biometría facial, especialmente considerando el aumento de delitos financieros y la facilidad con que se podría suplantar la identidad de los usuarios debido a la sofisticación tecnológica.

v. Que el BCP estaría en una mejor posición para identificar riesgos y problemas de seguridad en el sistema financiero, por lo que puede tomar las medidas necesarias para enfrentarlos, teniendo en consideración que su decisión se

encontraría protegida bajo la libertad de autoorganización (libertad de empresa); por lo cual, sería crucial que la Autoridad de Datos otorgue discrecionalidad a las entidades reguladas que implementan medidas de seguridad adecuadas a su sector para resguardar la seguridad de los usuarios.

vi. Que la Superintendencia de Banca y Seguros (SBS), a través de la Resolución 504-2021, exigiría a las empresas del sistema financiero verificar la identidad del usuario en el acceso a los servicios que provea y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad. Asimismo, exigiría la utilización de dos factores de autenticación; es decir, serían dos factores biométricos o de dos factores de categorías diferentes.

vii. Que, la apelante señala que la autenticación biométrica sería el medio idóneo elegido por ella para garantizar la seguridad de sus usuarios; sin embargo, para la DPDP la utilización del factor biométrico en la utilización del libro de reclamaciones virtual sería intrusivo y desproporcional, a pesar que la SBS permitiría la utilización de este mecanismo de autenticación.

viii. Que la DPDP, tampoco habría realizado mayor análisis de qué otros factores de autenticación podrían ser utilizados y cómo ello garantiza la seguridad del usuario; es decir, no existiría una ponderación de factores cuando la DPDP señala que, para el caso de clientes intermitentes podría satisfacerse simplemente con la consignación del número de DNI, el cual sería un dato elemental y de muy fácil conocimiento, por lo que no cumpliría con la exigencia de la SBS. Además, la Dirección sugirió de manera genérica que existen otros datos para validar la identidad, pero no presentó alternativas concretas ni consideró la obligación regulatoria de utilizar dos factores de autenticación.

ix. Que, la DPDP señalaría que realizaría un examen de proporcionalidad para verificar si la validación de identidad mediante biometría era adecuada; sin embargo, no habría demostrado la existencia de alternativas menos gravosas, porque no existiría para el caso de clientes intermitentes, donde no contarían con mayor información previa.

x. Que, la regulación sectorial autorizaría a la administrada a gestionar sus riesgos de la manera más adecuada, dentro de las opciones reconocidas, como la validación a través de la biometría facial y la constatación del DNI con lo registrado en la base de datos del RENIEC, y posteriormente con la base de datos que ha recopilado, no existiría otro medio de validación de identidad a distancia por factibilidad por seguridad, pues es el mismo mecanismo que utiliza el RENIEC para solicitudes de duplicado de DNI; y, debe considerarse los riesgos advertidos por la SBS en el documento adjunto como Anexo 5-A.

xi. Que en el caso de clientes regulares, no se podría considerar desproporcional la decisión libre de un usuario para validar su identidad, ya que los clientes tienen la opción de elegir entre dos alternativas: la cuenta y clave, o la biometría facial. Asimismo, la DPDP cometió un error al suponer que la tarjeta y clave constituyen dos factores de autenticación suficientes, y que por ello no es necesario el uso de la biometría cuando en realidad solo constituiría un único factor de autenticación.

xii. Que, en otros aspectos, en el caso de los clientes que han contratado productos con el BCP existiría dos "opciones" entre las que estos escogen luego de identificarse con su DNI: (i) introducir el número de su tarjeta y la clave de ésta; o, (ii) la biometría facial, siendo ellos quienes se someterían voluntariamente a cualquiera de los dos mecanismos, por lo que no se podría considerarse desproporcional, aspecto que ha sido implementado en el 2021 y no ha sido cuestionado por la autoridad.

xiii. Que, existiría un interés legítimo en el tratamiento de datos personales de clientes que han contratado un producto BCP, pues con la implementación de la validación biométrica, BCP busca (i) proteger la seguridad de sus usuarios; y, (ii) ejecutar la relación contractual con estos (en el marco del servicio prestado a través del LVR); por lo tanto, constituiría un tratamiento lícito.

xiv. Que, la DPDP habría analizado incorrectamente la actividad de almacenamiento en el Hecho Imputado I, debido a que en su resolución señala que el hecho imputado se limitaría a la recopilación para fines de validación de identidad; mientras que, el Hecho imputado II se evaluaría si se requiere consentimiento para almacenar dichos datos en su base de datos, pero de la revisión de los fundamentos 123, 125, 131 y 133 se mezclarían ambos conceptos, lo que ha afectado la claridad y precisión del análisis, no siendo coherente que la DPDP se pronuncie sobre una supuesta desproporcionalidad en el almacenamiento de los datos personales.

xv. Que un adecuado análisis de proporcionalidad demostraría que el uso de biometría facial como mecanismo de validación de identidad es idóneo, adecuado y necesario; y, que incluso si existiese algún grado de afectación a la privacidad del usuario por el uso de su biometría, resultaría plenamente razonable y justificado hacerlo en las circunstancias que se utiliza un medio digital y en atención a que los riesgos que obligan a realizar una fehaciente y segura validación de identidad, que de otro modo no sería factible.

**Respecto al Hecho imputado 2**

xvi. Que, la DPDP no tomaría en cuenta que el almacenamiento de datos biométricos no respondería a un interés comercial de la administrada (perfilamiento, envío de publicidad), sino que se realiza únicamente para fines de posteriores validaciones de identidad como parte de la debida ejecución de una relación contractual. Por lo que estarían exceptuados de obtener consentimiento por ser necesario para la ejecución contractual.

xvii. Que, no sería exigible el consentimiento por ser necesario para la ejecución contractual, pues cuando un cliente presenta un reclamo a la administrada, necesariamente habría tenido una interacción comercial con ella y la información que se solicita en el marco de la presentación de un reclamo para validar su identidad se recopilaría como consecuencia del vínculo entre el cliente y el banco, como sería el caso de la denunciante.

xviii. Que, tampoco sería exigible consentimiento para la protección de intereses legítimos del titular de los datos personales, toda vez que el tratamiento se realizaría con la finalidad de resguardar su seguridad y evitar que su información

se comparta con terceros no autorizados que puedan sacar un provecho ilícito, y no reportaría ningún beneficio comercial al BCP.

xix. Que, almacenaría estos datos biométricos faciales de los usuarios y datos biométricos que evidencia la aprobación de una operación a nombre del usuario, de manera encriptada y segura, de tal modo que la información de sus usuarios estaría debidamente protegida y no sería posible que algún tercero pueda "ver" los datos ni "operar" con ellos, pues estarían ante una serie de números y letras que no tienen mayor valor individual; es decir, no podría identificar a una persona.

xx. Que, la evaluación de la DPDP se centraría el almacenamiento de datos biométricos faciales, pero no debería extenderse al almacenamiento de valores biométricos con fines de evidencia (cuando la operación autorizada mediante validación biométrica requiere que se almacene un registro de uso de biometría que sirva como sustento de que fue precisamente el cliente quien aprobó la operación), aspecto sobre el cual se debe pronunciarse el revisor.

**Respecto a las medidas correctivas**

xxi. Que, en la Resolución Impugnada solo se dedicaría un párrafo a motivar la decisión de la DPDP en imponer medidas correctivas, en el cual se hace una referencia a la supuesta necesidad de aplicar una medida correctiva al término del análisis del Hecho Imputado 1 (proporcionalidad de validar identidad a través de biometría), a pesar de que la medida correctiva versaría esencialmente sobre el cese de almacenamiento y supresión de lo almacenado (Hecho Imputado 2).

xxii. Que, no se realizaría un análisis sobre cómo estas medidas son efectivas, si son las más idóneas, ni se habría evaluado otras alternativas; tampoco se acreditaría su adecuación y proporcionalidad; asimismo, durante el procedimiento se habría evaluado el mecanismo de validación de identidad de los usuarios del LRV y el almacenamiento de estos valores biométricos en la base de datos "BIOM", sin embargo, al ordenar que se supriman todos los valores biométricos faciales de la base de datos excedería el alcance de este procedimiento, dado que es una base de datos general.

xxiii. Que, los datos biométricos almacenados en esta base de datos no serían únicamente aquellos usados para fines de validación biométrica, sino también los que se guardan a modo de evidencia de la aprobación de operaciones; por lo que, se les estaría obligando también a eliminar información que constituye nuestra única evidencia ante un eventual reclamo de usuarios que aprobaron operaciones a través de su biometría.

xxiv. Que, si se confirma la orden de suprimir los valores biométricos faciales obtenidos a través del LRV para fines de validación de identidad, debería dejarse en claro que ello de ninguna manera alcanza a los valores almacenados con finalidad de sustento o evidencia.

xxv. Que, la medida de cese de todo uso de biometría para validación de los usuarios en el LRV no tendría motivación y excede su alcance, más aún que la propia

DPDP reconoció que existirían ciertos supuestos en los que la validación sí es necesaria y proporcional.

**Respecto a la graduación de la multa**

xxvi. Que respecto al Hecho Imputado No. 1, la Dirección habría establecido un monto base incorrecto, que debería ser de 5 UIT y no 22.5 UIT; por lo que, se aumentaría ilegalmente 17.5 UIT sin ninguna justificación legítima. Agrega que, aplicando la metodología utilizada, el monto base de 22.5 UIT se establecería incorrectamente en función de la variable relativa 3, pero en ninguna circunstancia se acreditaría la existencia de un daño. Señala que, si se quiere aplicar un monto base superior a 5 UIT, este debería ser máximo de 7.5 UIT.

xxvii. Que respecto que el Hecho imputado No. 2 ocurriría lo mismo señalado en el párrafo precedente, pues se habría aumentado ilegalmente a 25 UIT. Agrega que debería partir del mínimo y realizar el análisis de los factores de la infracción a partir de ahí.

xxviii. Que no se habría considerado como factores atenuantes la falta de perjuicio económico causado, que no es reincidente y que no existió intencionalidad al cometer la conducta infractora, tampoco sería posible sostener que exista un beneficio ilícito, lo cual debe ser tomado en cuenta por la autoridad al momento de determinar la multa.

xxix. Que, en ambos casos se concluyó que ambas conductas infractoras generaron un riesgo o daño a una persona y aplicó una agravante del 20% sobre la multa base; sin embargo, no se acreditaría riesgo o daño en ningún extremo de la resolución impugnada, y el argumento al aplicar la agravante sería idéntico en ambas imputaciones. Por otra parte, no resultaría válido que la sola conducta constituya la infracción y el hecho agravante. La Dirección concluyó que se habría generado un riesgo o daño.

xxx. Que, no se habría ponderado que la DPDP habría reconocido que existen supuestos válidos de recopilación de datos biométricos faciales con fines de validación de identidad; que existen fines legítimos para este mecanismo de validación de identidad, es decir, no existe un beneficio ilícito; y, que no puede existir desproporcionalidad porque existiría un mecanismo de identidad optativo para la mayoría de casos, por lo que la multa debería ser menor.

**Respecto al principio de legalidad y tipicidad**

xxxi. Que, la DPDP pretendería sancionar bajo infracciones tipificadas en un reglamento, lo cual contravendría los principios de legalidad y tipicidad y no correspondería imponer sanción.

xxxii. Que, bajo el principio de tipicidad y legalidad del procedimiento administrativo sancionador establecidos en el artículo 248 del TUO de la LPAG, así como lo establecido por el Tribunal Constitucional en la STC 20-2015-AI, no sería posible delegar la tipificación de las infracciones a las normas infra legales.

xxxiii. Que, no se podría crear infracciones a partir de reglamentos, puesto que estos solo podrían especificar o graduar infracciones que estén con anterioridad previstas en una Ley. Además, el Tribunal Constitucional en el Expediente N.º 1182-2005-PA/TC señalaría que la tipificación reglamentaria sin un debido sustento legal es contraria a nuestro ordenamiento.

xxxiv. Indica que estaría prohibido la creación de infracciones a partir de reglamentos ni siquiera por "reenvío" de una Ley. La posibilidad de que una ley "delegue" la tipificación a un reglamento no sería válida. Asimismo, manifiesta que las infracciones deberían ser establecidas exclusivamente mediante normas con rango de ley, sin que quepan excepciones, conforme a lo que habría establecido el Tribunal Constitucional en su sentencia recaída el 10 de noviembre de 2015.

23. A través de la N.º 148-2024-JUS/DGTAIPD de 12 agosto de 2024, se programó informe oral solicitado por la administrada.

24. El 21 de agosto de 2024 (Registro N.º 000412529-2024MSC) la administrada solicitó la reprogramación del informe oral, así como su realización de manera presencial.

25. A través de la N.º 150-2024-JUS/DGTAIPD de 22 agosto de 2024, se atendió la solicitud de la administrada y se reprogramó el informe oral, el mismo que se realizó el 3 de setiembre de 2024 en las instalaciones de esta Dirección General.

26. Con escrito del 12 de setiembre de 2024 (Registro N.º 000455794-2024MSC) la administrada presentó argumentos complementarios a su recurso de apelación, remitió copia de la presentación utilizada en el informe oral, así como copia simple de documentos elaborados por la consultora *Gartner* sobre los riesgos y necesidades en materia de identificación de personas de manera segura en entornos digitales.

27. El 24 de octubre de 2024 (Registro N.º 000535732-2024MSC) la administrada presentó un informe legal elaborado por la consultora *IA Law Digital Lawyers* sobre la captación de datos biométricos para la validación de la identidad de los usuarios en el sistema financiero.

## II. COMPETENCIA

28. Según lo establecido en el inciso 20 artículo 33 de la LPDP, la Autoridad Nacional de Protección de Datos Personales es la encargada de iniciar fiscalizaciones de oficio o por denuncia por presuntos actos contrarios a lo establecido en la Ley y en su reglamento, y de aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.

29. Conforme lo dispuesto en el artículo 70 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N.º 013-2017-JUS, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales ejerce la Autoridad Nacional de Protección de Datos Personales

30. Asimismo, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales es el órgano encargado de resolver en segunda y última instancia administrativa los procedimientos iniciados por la Dirección de

Protección de Datos Personales, conforme con lo establecido por el literal l) del artículo 71 del ROF del Ministerio de Justicia y Derechos Humanos.

## III. ADMISIBILIDAD

31. El recurso de apelación ha sido presentado dentro de los quince (15) días hábiles de notificada la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP del 01 de julio de 2024 y cumple con los requisitos previstos en los artículos 218[28] y 220[29] del Texto Único Ordenando de la Ley N.º 27444, Ley del Procedimiento Administrativo General (en adelante, TUO de la LPAG), razón por la cual es admitido a trámite.

**CUESTIÓN PREVIA: Si las infracciones imputadas contravienen los principios de legalidad y tipicidad**

32. La administrada, en el recurso de apelación, señala que la DPDP pretendería sancionar bajo infracciones tipificadas en un reglamento, lo cual contravendría los principios de legalidad y tipicidad y no correspondería imponer una sanción.

33. Agrega, entre otros, que los reglamentos no podrían establecer conductas prohibidas ni siquiera por reenvío de una Ley. La posibilidad de que una ley delegue la tipificación a un reglamento no sería válida. Las tipificaciones deberían ser establecidas exclusivamente mediante normas con rango de ley, sin admitir excepciones, conforme a lo que se habría establecido en la sentencia del Tribunal Constitucional recaída el 10 de noviembre de 2015, así como otras resoluciones citadas en su recurso de apelación.

34. En conclusión, la administrada cuestiona que ha sido sancionada por conductas tipificadas en el reglamento de la LPDP, lo cual, a su consideración, sería ilegal; pues no se contaría con sustento normativo debido a que la LPDP no habría determinado las conductas sancionables que han sido imputadas.

35. Sobre el particular, la DPDP en la tercera cuestión previa de la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024, señaló los siguiente:

> ***"Tercera cuestión previa: Sobre la supuesta contravención a los principios de legalidad y tipicidad de la potestad sancionadora de la administración***
>
> *55. Entonces, a diferencia de las normas del sistema nacional de control (la LOCGR), la normativa de protección de datos personales no cuenta con una norma de nivel*

---

28 **Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N.° 004-2019-JUS**
***(...) "Artículo 218. Recursos administrativos***
*218.1 Los recursos administrativos son:*
*a) Recurso de reconsideración*
*b) Recurso de apelación*
*Solo en caso que por ley o decreto legislativo se establezca expresamente, cabe la interposición del recurso administrativo de revisión.*
*218.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días."*

29 **Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N.° 004-2019-JUS**
***(...) "Artículo 220.- Recurso de apelación***
*El recurso de apelación se interpondrá cuando la impugnación se sustente en diferente interpretación de las pruebas producidas o cuando se trate de cuestiones de puro derecho, debiendo dirigirse a la misma autoridad que expidió el acto que se impugna para que eleve lo actuado al superior jerárquico."*

*constitucional que ciña su estructura ni su contenido; solo obedece al objetivo de garantizar una el derecho fundamental a la protección de datos personales, teniendo la libertad de desarrollar a través de la LPDP y su reglamento, las obligaciones y las infracciones que derivan de su incumplimiento.*
*(…)*
*58. Respecto de la especialización de la materia, es necesario resaltar también que la LPDP, así como su normativa complementaria (el Reglamento de la LPDP) tiene como objeto es el de garantizar un derecho fundamental, que es el de la protección de los datos personales, contenido en el numeral 6 del artículo 2 de la Constitución Política del Perú.*
*59. Para alcanzar tal finalidad, la LPDP contiene una lista enumerativa de principios rectores, los cuales constituyen pautas que los responsables del tratamiento de datos personales deben seguir para llevarlo a cabo y para garantizar el ejercicio de los derechos que dicha ley premune a las personas naturales, como titulares de los datos personales.*
*60. A fin de garantizar la observancia de tales principios y derechos, se establece en la normativa de protección de datos personales, obligaciones específicas que deben ser cumplidas por los responsables del tratamiento, siendo que en caso de su incumplimiento, se incurre en alguna de las infracciones, las que son conductas específicas contenidas en el artículo 132 del Reglamento de la LPDP.*
*61. Ahora bien, la sentencia de la Sala Civil Permanente recaída en la Apelación N° 5440-2019, señalada por la administrada, establece que deben entenderse complementariamente los mencionados principios, en mérito de lo cual se acoge una reserva de ley para determinar las conductas sancionables administrativamente, que deberán estar tipificadas de manera clara, específica, precisa e inequívoca.*
*(…)*
*63. Entonces, la sentencia reseñada admite a la excepción de la reserva de ley que en su momento, el Tribunal Constitucional acogió, permitiendo que mediante reglamento se desarrollen las conductas sancionables, sin crear nuevos supuestos infractores ni extralimitarse de lo que las normas legales impongan.*
*64. Se aprecia en el caso de la LPDP, que cumple con el requisito de reserva de ley para atribuir el ejercicio de potestad sancionadora (y sus funciones, como la fiscalización, instrucción e imposición de sanciones) y de imponer sanciones ante el incumplimiento de sus disposiciones, a la Autoridad Nacional de Protección de Datos Personales, en observancia del principio de legalidad, al aplicarse lo establecido en sus artículos 32, 33 y 39:*
*(…)*
*65. En lo concerniente al establecimiento de un supuesto de ilicitud (contrarios a la normativa) y a la tipificación de conductas específicas que encarnen tal ilicitud (infracciones), se debe analizar las normas del Título VII de dicha ley: (…)*
*66. De lo transcrito, se aprecia que la LPDP, en su artículo 37 establece una situación sancionable general: La comisión de actos contrarios a la LPDP y su reglamento; dejando la tipificación exhaustiva y específica al reglamento, como dispone el artículo 38 de dicha ley, que clasifica a las infracciones según su gravedad.*
*67. En tales artículos, la LPDP equipara el bien jurídico a proteger (preservar el derecho fundamental del numeral 6 del artículo 2 de la Constitución Política del Perú) con el cumplimiento del íntegro de sus disposiciones, siendo las situaciones contrarias a dicha ley y su reglamento, una conducta infractora sancionable, cuyos caracteres se especifican en su reglamento, al identificar tales conductas de forma exhaustiva, sin "crear" supuestos jurídicos que carezcan de base en la LPDP.*
*68. Dicha tipificación, que especifica los hechos que configuran la conducta general de incumplimiento, se desarrolla en el artículo 132 del Reglamento de la LPDP, sirviéndose de lo establecido en el artículo 38 de dicha ley.*
*69. Con ello, se configura la observancia de los principios de legalidad y tipicidad de la potestad sancionadora administrativa del artículo 248 de la LPAG, al ceñirse la normativa de protección de datos personales a la excepción establecida, así como estableciendo claramente las competencias para el ejercicio de dicha potestad.*

> *70. Se debe remarcar que la tipificación reglamentaria no constituye una reiteración o añadidura al sentido del artículo 37 de la LPDP, como puede suceder, por ejemplo, si se incluyen algún supuesto que consista exclusivamente en el incumplimiento de normas relativas a otros derechos fundamentales que no desarrolla esta ley; tampoco desnaturalizan el objeto de dicho artículo, que es preservar el cumplimiento de las disposiciones de dicha ley y su reglamento.*
> *71. En consecuencia, esta Dirección aprecia que la tipificación del artículo 132 del Reglamento de la LPDP se está aplicando con la especificidad suficiente para otorgar certeza sobre cada hecho ilícito, en observancia los principios mencionados del artículo 248 de la LPAG, por lo que cualquier acto administrativo que se emita respecto de ella estará premunido de validez."*

36. Así entonces, la DPDP concluye que, y, en virtud a la especialidad de la materia, la ley habilita expresamente a la tipificación de las infracciones a través del Reglamento; y, los hechos imputados cumplen con la especificidad suficiente para otorgar certeza sobre el hecho ilícito, siendo conforme con los principios de legalidad y tipicidad establecidos en el artículo 248 del TUO de la LPAG.

37. Precisamente, este Despacho advierte que, los principios de legalidad y tipicidad se encuentran previstos en los numerales 1 y 4 del artículo 248 del TUO de la LPAG, dispositivo que señala lo siguiente:

> ***"Artículo 248.- Principios de la potestad sancionadora administrativa***
> *La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:*
> ***1. Legalidad. -** Sólo por norma con rango de ley cabe atribuir a las entidades la potestad sancionadora y la consiguiente previsión de las consecuencias administrativas que a título de sanción son posibles de aplicar a un administrado, las que en ningún caso habilitarán a disponer la privación de libertad.*
> *(…)*
> ***4. Tipicidad. -** Solo constituyen conductas sancionables administrativamente las infracciones previstas expresamente en normas con rango de ley mediante su tipificación como tales, sin admitir interpretación extensiva o analogía. Las disposiciones reglamentarias de desarrollo pueden especificar o graduar aquellas dirigidas a identificar las conductas o determinar sanciones, sin constituir nuevas conductas sancionables a las previstas legalmente, **salvo los casos en que la ley o Decreto Legislativo permita tipificar infracciones por norma reglamentaria**.*
> *A través de la tipificación de infracciones no se puede imponer a los administrados el cumplimiento de obligaciones que no estén previstas previamente en una norma legal o reglamentaria, según corresponda.*
> *En la configuración de los regímenes sancionadores se evita la tipificación de infracciones con idéntico supuesto de hecho e idéntico fundamento respecto de aquellos delitos o faltas ya establecidos en las leyes penales o respecto de aquellas infracciones ya tipificadas en otras normas administrativas sancionadoras.*
> *(…)."*

38. Así entonces, el principio de legalidad refiere al instrumento normativo en el que debe reconocerse la potestad sancionadora y las consecuencias administrativas que a título de sanción son pasibles de aplicar en caso se determine la responsabilidad del administrado.

39. A mayor abundamiento, en la Casación N.º 1914-2017 CUSCO, la Sala de Derecho Constitucional y Social Permanente de la Corte Suprema de Justicia de la República, desarrolló el principio de legalidad, indicando:

> *"(…) 8.2. Dentro de este panorama es válido afirmar que la aplicación del principio de legalidad a los hechos involucrados en el presente caso exige que el operador judicial determine si la autoridad de salud y demás organismos y entes involucrados se encuentran facultados legalmente para ejercer función sancionadora administrativa o no, conforme lo prescrito por el numeral 1 del artículo 230 de la Ley N. ° 27444 (…)". En ese propósito, es preciso señalar en primer orden que el ejercicio de la potestad sancionadora de la Administración Pública, entendida como la atribución que el ordenamiento jurídico le reconoce para imponer, con independencia de los demás poderes del Estado, sanciones – sanciones consistentes generalmente en la privación de un bien o un derecho o la imposición de una obligación de pago como la multa– con el propósito de reprimir la infracción de las normas que contribuyen al correcto funcionamiento de la actividad administrativa, ha sido sometido por el legislador a una serie de principios sustentados en las garantías ínsitas en el Estado de Derecho, entre los que se encuentra el denominado principio de tipicidad."*

40. Por lo tanto, corresponde determinar si la Autoridad Nacional de Protección de Datos Personales (en adelante, la **ANPD**) se encuentra facultada legalmente para ejercer la función sancionadora de acuerdo con la normativa que la regula.

41. Al respecto, corresponde remitirnos a la LPDP, modificada por el Decreto Legislativo N.º 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses, específicamente a la Cuarta Disposición Complementaria Modificatoria que prevé lo referente al artículo 38 de la LPDP[30], dispositivo que establece la clasificación de las infracciones leves, graves y muy graves, las cuales son tipificadas vía reglamentaria.

42. Asimismo, se debe tener en cuenta que los artículos 32 y 33 de la LPDP[31] reconocen la potestad sancionadora de la ANPD y la facultad de imponer medidas correctivas y cautelares. Así también, el artículo 39 del mismo cuerpo legal, prevé lo referente a las sanciones a aplicar en relación con la gravedad de las conductas infractoras, de acuerdo con el siguiente texto:

> ***"(…) Artículo 39. Sanciones administrativas***

---

30 **Ley N.° 29733, Ley de Protección de Datos Personales**
*(…)*
*"**Artículo 38.- Tipificación de infracciones***
*Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N.º 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de ministros. (…)".*

31 **Ley N.° 29733, Ley de Protección de Datos Personales**
*(…)*
*"**Artículo 32.- Órgano competente y régimen jurídico***
*Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces. (…)"*
***"Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales***
*La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:*
*(…)*
*20. Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento."*

> *En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:*
> *1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).*
> *2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).*
> *3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).*
> *(…)*
> *La Autoridad Nacional de Protección de Datos Personales determina la infracción cometida y el monto de la multa imponible mediante resolución debidamente motivada. Para la graduación del monto de las multas, se toman en cuenta los criterios establecidos en el artículo 230, numeral 3), de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. (…)"*

43. En ese sentido, se aprecia que la potestad sancionadora de la ANPD, la clasificación de infracciones y la previsión de las consecuencias administrativas que a título de sanción se aplicó a la administrada (multa), se encuentran previstas en la LPDP; por lo que no se advierte vulneración del principio de legalidad establecido en el numeral 1 del artículo 248 del TUO de la LPAG.

44. Ahora bien, en cuanto al principio de tipicidad, si bien por regla general la infracción debe encontrarse debidamente tipificada en una norma con rango legal (principio de reserva de ley absoluta), nuestro ordenamiento jurídico reconoce la posibilidad de tipificar infracciones a través de norma reglamentaria siempre que exista una autorización por ley o decreto legislativo (reserva de ley relativa) conforme a lo establecido en el numeral 4 del artículo 248 del TUO de la LPAG, citado anteriormente[32].

45. Precisamente, este último supuesto, conocido como la colaboración reglamentaria por habilitación legal, ha sido desarrollado por María Lourdes Ramírez Torrado[33], quien señala en cuanto a dicha colaboración:

> *"(…) la colaboración entre la ley y el reglamento para la conformación del binomio infracción/sanción y el respeto de la reserva de ley en la actividad sancionadora administrativa se traduce en la posibilidad de que las disposiciones administrativas contemplen los supuestos típicos, o infracciones administrativas, con sus correspondientes sanciones; siempre que se respeten las previsiones de lo contemplado en la ley".*

46. Asimismo, el concepto de remisión normativa ha sido desarrollado doctrinalmente en los siguientes términos[34]:

> *"(…) la STS de 26 de diciembre de 1984 (Ar. 6729; Hierro): Entre las técnicas de habilitación figura con características propias que la diferencian sustantivamente de las demás, la denominada remisión normativa, por medio de la cual la ley remite al*

---

[32] En esa misma línea el artículo 24 del Reglamento de la Ley Marco para la Producción y Sistematización Legislativa (DS 007-2022-JUS) reconoce que las disposiciones sancionadoras constituyen la regulación del procedimiento administrativo sancionador y los reglamentos puede **contener la tipificación de infracciones si así fuese lo autorizado por la ley o decreto legislativo que dicho reglamento complementa**.

[33] RAMÍREZ TORRADO, María Lourdes. *"La Reserva de Ley en materia sancionadora colombiana".* Recuperado en: https://dialnet.unirioja.es/descarga/articulo/3192131.pdf

[34] Nieto, A. (2005). [Fragmento]. En Derecho administrativo sancionador (pp.222-253) (592p.) (5a ed). Madrid: Tecnos.

> *reglamento la ordenación -bien sea en términos de homologación con lo que ha venido a conceptuarse marco sistemático de ordenación y dentro de los límites inferidos o deducidos de los principios inspiradores y rectores de la ley- de alguno de los elementos de regulación legal, ora por vía de desarrollo y ejecución ora por medio de la ordenación secundaria de determinados particulares. (…)"*

47. Así entonces, por el principio de tipicidad, las disposiciones reglamentarias de desarrollo solamente pueden "especificar o graduar" aquellas normas dirigidas a identificar las conductas (infracciones) o determinar sanciones, sin constituir nuevas conductas sancionables a las previstas legalmente, *salvo los casos en que la "ley o Decreto Legislativo" permita tipificar infracciones por norma reglamentaria*, supuesto último que sí se advierte en la normativa que regula la protección de datos personales, específicamente el artículo 38 de la LPDP.

48. Para este Despacho, el artículo 38 de la LPDP cumple con este último supuesto, toda vez que, expresamente permite la tipificación de sus infracciones al Reglamento de la LPDP, en cumplimiento con los supuestos de colaboración reglamentaria en materia de Derecho Administrativo Sancionador que exige el cumplimiento de dos requisitos derivados de la reserva legal: (i) la habilitación previa que abre paso a la intervención reglamentaria en general y, (ii) la remisión, que incluye el establecimiento de unas condiciones o directrices esenciales que sirvan de pauta al reglamento posterior remitido[35].

49. Asimismo, se cumple con ambos requisitos señalados de manera precedente, toda vez que la habilitación previa se encuentra establecida en el artículo 38 de la LPDP; y, establece condiciones esenciales que sirven de pauta para la tipificación de las infracciones en su Reglamento al clasificar la gravedad de las infracciones (leves, graves y muy graves), establecer las sanciones que se imponen a los administrados respecto a cada tipo de infracción, y limitar la tipificación de infracciones a la comisión de actos que afecten el derecho fundamental a la autodeterminación informativa por vulneración de la LPDP y su reglamento.

50. Cabe precisar que, la figura de la reserva relativa para la tipificación de infracciones administrativas no solo es reconocida por nuestra normativa y la doctrina especializada, sino también ha sido objeto de pronunciamientos por parte de tribunales y jueces.

51. Así, el Tribunal Constitucional en la Sentencia de 10 de noviembre de 2015 (Pleno Jurisdiccional) recaída en los Expedientes N.º 0014-2014-P1/TC, 0016-2014-PI/TC, 0019-2014-P1/TC y 0007-2015-PI/TC, desarrolla los siguientes aspectos referidos al principio de legalidad y reserva de ley relativa:

> *"(…) 180. En esta materia aplica entonces aquella reserva de ley relativa. Por ende, no resulta inconstitucional que se derive al reglamento la tipificación de las infracciones, en tanto se ha fijado en la ley las conductas sancionables y la escala y los tipos de sanción. 181. Por último, cabe añadir que, si se regula una actividad con miras a garantizar la calidad del servicio público, resulta necesario dotar al organismo supervisor de las herramientas necesarias para corregir las infracciones que se adviertan en su ámbito específico.*

[35] Nieto, A. (2005). [Fragmento]. En Derecho administrativo sancionador (pp.248) (592p.) (5a ed). Madrid: Tecnos.

> *182. De otro lado, y como es obvio, las resoluciones de sanción deberán estar debidamente motivadas, y la sanción que se imponga debe resultar proporcional a la naturaleza y gravedad de la infracción en que haya incurrido la universidad. (…)".*

52. En consecuencia, en virtud del principio de reserva de ley relativa en el procedimiento administrativo sancionador, resulta válido que la LPDP derive a su Reglamento la tipificación de infracciones, criterio que puede ser reafirmado por lo resuelto por el Tribunal Constitucional a través de la Sentencia 201/2022 del 15 de junio de 2022, recaída en el Expediente N.º 0002-2021-PI/TC.

53. En la citada sentencia, el Tribunal Constitucional realiza un análisis de constitucionalidad del primer párrafo del inciso 4 del artículo 248 del TUO de la Ley 27444[36], reconociendo que en el ámbito del derecho administrativo sancionador, los reglamentos pueden especificar o graduar las infracciones debidamente tipificadas en la ley; y, precisa que, en casos de remisión legal expresa, es posible tipificar infracciones a través de normas reglamentarias[37]; además, reconoce la colaboración reglamentaria para tal fin, como se advierte en el siguiente fundamento:

> *20. "En el ámbito administrativo, tal precisión de lo considerado como antijurídico no está sujeta a una reserva de ley absoluta, sino que puede ser complementada a través de los reglamentos respectivos. La ausencia de una reserva de ley absoluta en esta materia, como indica Alejandro Nieto (Derecho administrativo sancionador, Editorial Tecnos, Madrid 1994, pág. 260), "provoca, no la sustitución de la ley por el reglamento, sino la colaboración del reglamento en las tareas reguladoras, donde actúa con subordinación a la ley y como mero complemento de ella" (cfr. Sentencia 02050-2002-AA/TC, fundamento 9)*
> *(…)*
> *La delegación legislativa en la Administración generalmente se produce porque se requiere regular aspectos técnicos muy específicos, pero jamás para que sea aquella quien cree los tipos ilícitos administrativos. Es por ello que, a fin de respetar los derechos de los administrados, el Tribunal considera que en la ley de remisión debe fijarse lo esencial de la conducta constitutiva del ilícito, así como contener los parámetros que impidan un ejercicio discrecional de la potestad reglamentaria atribuida a la Administración.*
>
> Subrayado nuestro

54. Por lo expuesto, se debe descartar lo señalado por la administrada en su recurso de apelación respecto a que nuestro ordenamiento jurídico no permitiría la tipificación de infracciones vía reglamentaria, ni siquiera por "reenvío de la ley", toda vez que tanto el inciso 4 del artículo 248 del TUO de la Ley 27444 sí permite la delegación de la tipificación de infracciones a través del Reglamento en el marco del procedimiento administrativo sancionador, siempre que exista una habilitación legal expresa establecida en ley o decreto legislativo.

55. Por otra parte, este Despacho no puede dejar de lado también lo señalado por el Tribunal Constitucional en la sentencia del 25 de abril de 2018 (Pleno Jurisdiccional)

---

[36] Pleno Sentencia del Tribunal Constitucional del 15 de junio de 2022 (Caso del cuestionamiento de los procesos de decisión en el ámbito de la administración pública - análisis de constitucionalidad del inciso 4 del artículo 248 del TUO de la Ley 27444) disponible en el siguiente enlace: https://www.tc.gob.pe/jurisprudencia/2022/00002-2021-AI.pdf

[37] Fundamento 16 del Pleno Sentencia del Tribunal Constitucional del 15 de junio de 2022.

recaída en el Expediente N.º 0020-2015-PI/TC (Caso Potestad Sancionadora de la Contraloría General de la República[38]), que en el fundamento 46 señala lo siguiente:

> *"(…) 46. Por tanto, al desarrollar normas con rango de ley, los reglamentos no pueden desnaturalizarlas creando infracciones sin una debida base legal. Admitir lo contrario implicaría aceptar una desviación de la potestad reglamentaria y vaciar de contenido los principios de legalidad y tipicidad que guardan una estrecha relación con el derecho fundamental al debido proceso."*
>
> (Subrayado agregado)

56. En ese contexto, se desprende claramente que la prohibición no se encuentra en la tipificación de infracciones a través de norma reglamentaria, sino que, lo que está proscrito es la desviación de la potestad reglamentaria que puede vaciar de contenido los principios de legalidad y tipicidad como, por ejemplo, cuando se tipifica infracciones sin habilitación legal expresa, cuando se tipifique incumplimientos de normas relativas a otros derechos fundamentales que no desarrolla la LPDP, cuando las sanciones para una determinada infracción sean distintas a la establecida en la Ley, o cuando las conductas prohibidas no cuenten con una adecuada base legal que delimite las características esenciales de la conducta prohibida.

57. Así, en la sentencia del Tribunal Constitucional 0020-2015-PI/TC, se ha señalado que las conductas prohibidas por un reglamento deben tener un adecuado sustento legal, lo cual es acorde a lo señalado anteriormente en un pronunciamiento anterior en el 1182-2005-PA/TC, pero no exige, como erróneamente interpreta la administrada que la conducta antijurídica se encuentre expresamente regulada en una norma con rango de ley:

> *"(…) 22. Para el Tribunal Constitucional esta disposición legal no admite una interpretación que permita la desnaturalización de los principios de legalidad y tipicidad. Resulta admisible que, en ocasiones, los reglamentos especifiquen o gradúen infracciones previstas de manera expresa en la ley. Sin embargo, nada justifica que establezcan conductas prohibidas sin adecuada base legal, o que, al desarrollar disposiciones legales generales o imprecisas, los reglamentos terminen creando infracciones nuevas subrepticiamente (cfr. Sentencia 00020- 2015-AI/TC, fundamento 44)*
>
> *23. En efecto, el artículo 248.4 del TUO de la LPAG, si bien reconoce como regla general la reserva de ley en materia de calificación de conductas pasibles de ser sancionadas administrativamente, admite también la posibilidad que la ley habilite la tipificación por vía reglamentaria. Sin embargo, entiende el Tribunal Constitucional que esta remisión de la ley al reglamento debe especificar las características esenciales de la conducta antijurídica, ya que bajo ninguna circunstancia puede ser una remisión en blanco."*
>
> (Subrayado agregado)

58. A mayor abundamiento, el Tribunal Constitucional a través de la Sentencia 201/2022 del 15 de junio de 2022 (fundamento 29) aclara que en el caso de la Potestad Sancionadora de la Contraloría General de la República *no se pronunció sobre el inciso 4 del artículo 248 del TUO de la LPAG, ni tampoco afirmó que la delegación*

[38] Sentencia del Tribunal Constitucional del 25 de abril de 2018 (Caso Potestad Sancionadora de la Contraloría General de la República) disponible en el siguiente enlace: https://tc.gob.pe/jurisprudencia/2019/00020-2015-AI.pdf

*de la competencia normativa para establecer infracciones y sanciones mediante normas infralegales vulnera el principio de tipicidad, sino que este principio resultó trasgredido por una inadecuada delimitación de la conducta prohibida en la norma que fue objeto de cuestionamiento.*

59. Así entonces, el Tribunal Constitucional, máximo intérprete de nuestra Constitución, de la cual se desprenden los principios de legalidad y tipicidad, han confirmado la posibilidad de tipificar infracciones a través de una norma reglamentaria para el ejercicio de la potestad sancionadora, siempre que se cuente con una adecuada base legal, una habilitación legal expresa y parámetros que impidan un ejercicio discrecional de la potestad reglamentaria.

60. Por lo tanto, este Despacho comparte el criterio establecido por la DPDP al señalar que la LPDP en su artículo *37* establece una situación sancionable general: La comisión de actos contrarios a la LPDP y su reglamento; dejando la tipificación exhaustiva y específica al reglamento, por la especialidad técnica de la materia, tal como dispone el artículo 38 de dicha ley, que clasifica a las infracciones según su gravedad, sin "crear" supuestos jurídicos que carezcan de base en la LPDP, cumpliéndose adecuadamente con el principio de tipicidad al existir una reserva legal relativa expresamente habilitada por ley.

61. Por otra parte, para determinar si la infracción imputada a la administrada, tiene una adecuada base legal, se debe evaluar si esta se está aplicando con la especificidad suficiente para otorgar certeza sobre el hecho ilícito, en observancia del principio de tipicidad.

62. Precisamente, el principio de tipicidad alude al grado de predeterminación normativa de las conductas típicas proscribiendo supuestos de interpretación extensiva o analógica, de tal forma que impone al legislador que las prohibiciones que definen sanciones estén redactadas con un nivel de precisión suficiente que permita a cualquier ciudadano comprender sin dificultad lo que se está proscribiendo, bajo amenaza de sanción en una determinada disposición legal[39].

63. A mayor abundamiento, Morón Urbina[40] indica lo siguiente:

> *"(…) La determinación de si una norma sancionadora describe con cierto grado de certeza la conducta sancionable, es un asunto que debe ser resuelto de manera casuística, puesto que el mandato de tipificación que se deriva de este principio no sólo se impone al legislador cuando redacta el ilícito, sino también a la autoridad administrativa cuando instruye un procedimiento sancionador y debe realizar la subsunción de una conducta en el tipo legal de la infracción."*
> (Subrayado agregado)

64. Así entonces, el principio de tipicidad no sólo se impone al legislador cuando redacta la infracción, sino también a la autoridad administrativa cuando instruye el procedimiento administrativo sancionador y, en dicho contexto, realiza la subsunción de una conducta en el tipo legal de la infracción, de tal manera que el hecho imputado

---

39 STC Expediente N.º 2192-2004-AA/TC.

40 Juan Carlos MORÓN URBINA, *"Comentarios a la Ley del Procedimiento Administrativo General"*, Tomo II, Gaceta Jurídica, Lima, 2018, pp. 769.

corresponda con aquel descrito en el tipo infractor, el cual debe ser comunicado en la resolución de imputación de cargos[41].

65. Teniendo en cuenta que, para que se produzca una legítima reserva de ley, corresponde la verificación de que la conducta sancionable (obligaciones) se encuentre especificada y correctamente determinadas en la LPDP, son dos cuestiones las que habrá que tener en cuenta en lo que respecta al estricto respeto al principio de tipificación: (i) un primer nivel referido a que la norma describa los elementos esenciales del hecho que califica como infracción sancionable, con un nivel de precisión suficiente que permita comprender sin dificultad lo que se está proscribiendo; y, (ii) un segundo nivel referido a la fase de aplicación de la norma, donde se exige que el hecho concreto imputado por el autor corresponda exactamente con el descrito en la norma[42].

66. Por tanto, recae sobre este despacho el deber de evaluar la concurrencia de los elementos que configuran el tipo legal de la infracción que ha sido imputado a la administrada. De la revisión de las normas se observa que el tipo infractor se constituye en dos elementos: (i) norma sustantiva, que es la que contiene las obligaciones de todos aquellos que realizan tratamiento de datos personales cuyo incumplimiento se les imputa; y, (ii) la norma tipificadora, que es la que califica el incumplimiento como infracción.

67. En este sentido, corresponde analizar si el tipo infractor contenido en el literal d) del numeral 2 del artículo 132 de dicho reglamento: "*"Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos*", se subsume dentro del tipo infractor imputado a la administrada*",* cuenta con un adecuado sustento legal; y, si el hecho verificado en la fiscalización, esto es: "*realizar el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, al recopilar la fotografía del Documento Nacional de Identidad - DNI y la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica (dato sensible). Datos personales que no son necesarios pertinentes ni adecuados para cumplir con la finalidad de identificar al reclamante. Incumpliendo la obligación establecida en los artículos 7 y numeral 3 del artículo 28 de la LPDP*", se subsume dentro del tipo infractor imputado a la administrada.

68. Lo mismo en el caso de la infracción contenida en el literal b) del inciso 2 del artículo 132 de dicho reglamento: *"Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular",* cuenta con un adecuado sustento legal; y, si el hecho verificado en la fiscalización, esto es: *"Realizar el tratamiento de los datos personales sensibles de los usuarios y clientes, al almacenar el dato biométrico referido a la imagen facial, en una base de datos propia, sin obtener válidamente el consentimiento del titular de los datos personales, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento"*, se subsume dentro del tipo infractor imputado a la administrada.

---

41 Juan Carlos MORÓN URBINA, *"Comentarios a la Ley de Procedimiento administrativo General",* Tomo II, Gaceta Jurídica, Lima, 2018, p. 413.

42 José GARBERÍ LLOBREGAT, *El procedimiento administrativo sancionador,* Tirant Le Branch, Madrid, 1998, p. 114.

**Primer Nivel del Principio de Tipicidad**

**Sobre el hecho infractor: "Realizar el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, al recopilar la fotografía del Documento Nacional de Identidad - DNI y la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica (dato sensible). Datos personales que no son necesarios pertinentes ni adecuados para cumplir con la finalidad de identificar al reclamante. Incumpliendo la obligación establecida en los artículos 7 y numeral 3 del artículo 28 de la LPDP"**

69. El artículo 3 de la LPDP, al establecer el ámbito de aplicación de la ley, establece que son objeto de especial protección los datos sensibles[43].

70. Asimismo, el artículo 7 de la LPDP reconoce al principio de proporcionalidad como un principio rector en el tratamiento de datos personales:

> ***Artículo 7. Principio de proporcionalidad***
> *Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados*."

71. Por su parte el artículo 28 de la LPDP establece las obligaciones del titular y el encargado del tratamiento señalando lo siguiente:

> ***"Artículo 28. Obligaciones***
> *El titular y el encargado de tratamiento de datos personales, según sea el caso, tienen las siguientes obligaciones:*
> *3. Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido."*

72. Ahora bien, resulta conveniente mencionar que el artículo 12 de la LPDP[44] establece el valor de los principios que deben tener en cuenta los titulares y encargados del tratamiento de datos personales, quienes deben ajustar sus actuaciones a los principios rectores contenidos en la LPDP.

73. Estas disposiciones normativas constituyen las normas sustantivas estipuladas en la LPDP; complementariamente el artículo 8 del Reglamento de la LPDP contiene la obligación referida al principio de finalidad en el tratamiento de datos personales de carácter sensible, disponiendo lo siguiente:

---

43 **Ley N.° 29733, Ley de Protección de Datos Personales**
*"**Artículo 3.- Ámbito de aplicación***
*Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N.º 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de ministros. (…)".*

44 **Ley N.° 29733, Ley de Protección de Datos Personales**
*"**Artículo 3.- Ámbito de aplicación***
*La actuación de los titulares y encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.*
*Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia**".***
*(…)".*

> ***"Artículo 8.- Principio de finalidad.***
> *(…)*
> *Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales."*

74. En este orden de ideas, el artículo 38 de la LPDP clasifica las infracciones en leves, graves o muy graves y el artículo 39 de la LPDP establece los márgenes de cuantía de las posibles sanciones, con lo que queda claro que los incumplimientos de las normas sustantivas contenidas en la LPDP pueden dar origen a multa.

75. Por específica remisión legal en colaboración reglamentaria **la norma sustantiva** (artículos 7 y 28 de la LPDP complementada por el artículo 8 del reglamento de la LPDP) **pasible de sanción** (artículos 38 y 39 de la LPDP) se encuentra **tipificada** en el artículo 132, numeral 2, literal d del reglamento de la LPDP que establece lo siguiente:

> "*(…)* ***Artículo 132.- Infracciones***
> ***2.Son infracciones graves:***
> *d) Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos."*

76. En efecto, cualquier administrado puede inferir del propio texto legal –con un grado de certeza suficiente– la acción prohibida: "tratamiento desproporcionado de datos personales sensibles", pues al constituir una obligación del titular del banco de datos personales, el recopilar únicamente los datos personales sensibles necesarios pertinentes y adecuados para cumplir con la finalidad determinada, explícita y lícita para la que requiere ser obtenidos, su incumplimiento tiene como consecuencia una sanción administrativa, todo ello se encuentra regulado, como hemos visto, en la LPDP quedando únicamente establecida en la disposición reglamentaria, la norma tipificadora.

77. Por lo tanto, la regulación legal y reglamentaria de la LPDP y su reglamento, este extremo, no resulta contrario al principio de tipicidad.

**Sobre el hecho infractor: "Realizar el tratamiento de los datos personales sensibles de los usuarios y clientes, al almacenar el dato biométrico referido a la imagen facial, en una base de datos propia, sin obtener válidamente el consentimiento del titular de los datos personales, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento"**

78. El artículo 5 de la LPDP reconoce como principio rector al consentimiento y en su artículo 13 contiene los alcances sobre el tratamiento de datos personales:

> ***"Artículo 5. Principio de consentimiento***
> *Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.*
>
> ***Artículo 13. Alcances sobre el tratamiento de datos personales***
> *(…)*
> *13.5 Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco*."

79. Por su parte el artículo 28 de la LPDP establece las obligaciones del titular y el encargado del tratamiento señalando lo siguiente:

> ***"Artículo 28. Obligaciones***
> *El titular y el encargado de tratamiento de datos personales, según sea el caso, tienen las siguientes obligaciones:*
> *Efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la presente Ley."*

80. Estas dos disposiciones normativas constituyen las normas sustantivas estipuladas en la LPDP; complementariamente el artículo 7 y 12 del Reglamento de la LPDP contienen la obligación referida al tratamiento mediando el consentimiento del titular de los datos personales, el mismo que deberá ser otorgado de manera previa, informada, expresa e inequívoca, disponiendo lo siguiente:

> ***"Artículo 7.- Principio de consentimiento.***
> *En atención al principio de consentimiento, el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones, deberá manifestarse en forma expresa y clara.*
>
> ***(…) Artículo 12.- Características del consentimiento***
> *Además de lo dispuesto en el artículo 18 de la Ley y en el artículo precedente del presente reglamento, la obtención del consentimiento debe ser:*
> *1. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales.*
> *(…)*
> *2. Previo: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.*
> *3. Expreso e Inequívoco: Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.*
> *(…)*
> *4. Informado: Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente:*
> *a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.*
> *b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.*
> *c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.*
> *d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda.*
> *e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.*
> *f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.*
> *g. En su caso, la transferencia nacional e internacional de datos que se efectúen."*

81. En este orden de ideas, el artículo 38 de la LPDP clasifica las infracciones en leves, graves o muy graves y el artículo 39 de la LPDP establece los márgenes de cuantía

de las posibles sanciones, con lo que queda claro que los incumplimientos de las normas sustantivas contenidas en la LPDP pueden dar origen a multa.

82. Por específica remisión legal en colaboración reglamentaria **la norma sustantiva** (artículos 5, 13 y 28 de la LPDP complementada por los artículos 7 y 12 del reglamento de la LPDP) **pasible de sanción** (artículos 38 y 39 de la LPDP) se encuentra **tipificada** en el artículo 132, numeral 2, literal b del reglamento de la LPDP que establece lo siguiente:

83. En efecto, cualquier administrado puede inferir del propio texto legal –con un grado de certeza suficiente– la acción prohibida: "tratamiento sin consentimiento válido", pues al constituir una obligación del titular del banco de datos personales, el contar con el consentimiento válido del titular del dato personal, su incumplimiento tiene como consecuencia una sanción administrativa, todo ello se encuentra regulado, como hemos visto, en la LPDP quedando únicamente establecida en la norma reglamentaria, la norma tipificadora.

84. Por lo tanto, la regulación legal y reglamentaria de la LPDP y su reglamento, este extremo, no resulta contrario al principio de tipicidad.

**Segundo Nivel del Principio de Tipicidad**

85. Mediante Resolución Directoral N.º 232-2023-JUS/DGTAIPD-DFI de 13 de octubre de 2023[45], la DFI resolvió iniciar procedimiento administrativo sancionador por la presunta comisión de los siguientes hechos infractores:

- *Realizar el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, al recopilar la fotografía del Documento Nacional de Identidad - DNI y la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica (dato sensible). Datos personales que no son necesarios pertinentes ni adecuados para cumplir con la finalidad de identificar al reclamante. Incumpliendo la obligación establecida en los artículos 7 y numeral 3 del artículo 28 de la LPDP.*
- *Realizar el tratamiento de los datos personales sensibles de los usuarios y clientes, al almacenar el dato biométrico referido a la imagen facial, en una base de datos propia, sin obtener válidamente el consentimiento del titular de los datos personales, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento.*

86. Mediante Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024[46] la DPDP resolvió lo siguiente:

- Sancionar al Banco de Crédito del Perú con la multa ascendente a veintisiete Unidades Impositivas Tributarias (27 UIT) por haber efectuado el tratamiento de datos sensibles (datos biométricos) que resultan excesivos, no necesario, adecuados ni pertinentes para el uso de su libro de reclamaciones virtual, en incumplimiento de lo dispuesto en los artículos 7 y numeral 3 del artículo 28 de la LPDP, configurando la infracción grave tipificada en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP.
- Sancionar al Banco de Crédito del Perú con la multa ascendente a treinta y seis Unidades Impositivas Tributarias (36 UIT) por haber efectuado el tratamiento de datos

[45] Obrante en los folios 223 al 255.
[46] Obrante en los folios 429 al 474.

sensibles (datos biométricos) de los usuarios de su libro de reclamaciones virtual, sin su consentimiento válido contrariando lo dispuesto en el numeral 13.5 y 13.6 del artículo 13 de la LPDP y el artículo 12 del Reglamento de la LPDP; infracción grave tipificada en el literal b) del inciso 2 del artículo 132 del Reglamento de la LPDP

87. Este Despacho advierte que los hechos imputados se subsumen en las infracciones cometidas que tiene como consecuencia las sanciones impuestas, por lo que tampoco se vulnera, en este nivel, el principio de tipicidad. En consecuencia, no se advierte ninguna transgresión a los principios de legalidad y tipicidad que inspiran el procedimiento sancionador, en tanto las normas que establecen las infracciones, sanciones y las medidas correctivas en materia de protección de datos personales tienen amparo en la Constitución, la LPDP y su reglamento.

88. Por tales razones, **no corresponde amparar** este extremo de la apelación presentada por la administrada.

## IV. CUESTIONES CONTROVERTIDAS

89. De acuerdo con lo señalado en el recurso de apelación, corresponde determinar lo siguiente:

- Si la DPDP motivó su resolución al momento de determinar la responsabilidad de la administrada por el tratamiento desproporcional de datos personales.
- Si la administrada es responsable por el tratamiento de datos personales sensibles sin el consentimiento de sus titulares.
- Si la medida correctiva respecto a suprimir los patrones biométricos faciales almacenados en la base de datos “BIOM” cumple con el objetivo de corregir o revertir los efectos que la conducta infractora.
- Determinar si DPDP ha realizado un correcto análisis de las multas impuestas.

## V. ANÁLISIS DE LAS CUESTIONES CONTROVERTIDAS

### La relevancia de la protección de los datos biométricos de las personas y su congruencia con las disposiciones normativas de los sectores económicos regulados

90. El derecho fundamental a la autodeterminación informativa se encuentra reconocido en el inciso 6 del artículo 2 de nuestra Constitución[47], y tal como ha señalado el Tribunal Constitucional en su jurisprudencia[48], consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos.

---

47 **Constitución Política del Perú**
Derechos fundamentales de la persona
**Artículo 2.-** Toda persona tiene derecho:
6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

48 Fundamento 15 del Pleno Sentencia del Tribunal Constitucional del 2 de febrero de 2021 (Exp. 02481-2019-HD/TC).

91. Ahora bien, el artículo 3 de la LPDP, al delimitar el ámbito de aplicación de la ley, establece que son objeto de especial protección los datos sensibles[49], los cuales son una categoría especial de datos personales, entre ellos, aquellos datos biométricos que por sí mismos pueden identificar al titular, conforme a lo regulado en el numeral 5 del artículo 2 de la citada norma.[50]

92. Conforme a lo ya señalado en anterior oportunidad por este Despacho[51], los datos biométricos son datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos; y, conforme a lo reconocido por el legislador, requieren una protección más reforzada, debido a que su vulneración ocasionaría daños de mayor gravedad.

93. Asimismo, un dato biométrico debe considerarse sensible, pues este tipo de datos contiene información sobre elementos tangibles, escrutables, vinculadas al ámbito más íntimo de la persona, como es la composición física y el funcionamiento de su cuerpo (fisiología); el cual puede abarcar cuestiones bioquímicas, neurológicas, relativas a la locomoción y a la determinación de la personalidad, cuyo manejo abarca riesgos variados, desde los concernientes a la suplantación de identidad hasta la predeterminación (en atención a la unicidad del dato biométrico, correspondiente solo a una persona perpetuamente) y posibilidad de interferencia en los procesos biológicos de su titular.

94. Precisamente, a través de la Opinión Consultiva N.º 032-2021-JUS/DGTAIPD de 17 de agosto de 2021 este Despacho advirtió que existen riesgos por el uso de sistemas de identificación biométrica, tales como: (i) la afectación del derecho a la privacidad, pues mantener el sistema requiere tratar datos biométricos que según la LPDP son definidos como sensibles, por lo que requieren una especial protección, dado que identifican plenamente al titular del dato personal y que, de ser vulnerados por terceros, podrían ser usados con fines ilegítimos, (ii) la utilización de mecanismos de obtención de datos biométricos con la finalidad de suplantación de identidad y, (iii) la afectación del derecho a la identidad de personas que están impedidas de acceder a este sistema por discapacidad o por imposibilidad.

---

49 **Ley N.° 29733, Ley de Protección de Datos Personales**
*"**Artículo 3.- Ámbito de aplicación***
*Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N.º 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de ministros. (…)".*

50 **Ley N.° 29733, Ley de Protección de Datos Personales**
***Artículo 2. Definiciones***
***(…)***
***5. Datos sensibles.** Datos personales constituidos por los **datos biométricos que por sí mismos pueden identificar al titular**; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual."*

51 Opinión Consultiva N.º 032-2021-JUS/DGTAIPD de 17 de agosto de 2021 disponible en el siguiente enlace: https://cdn.www.gob.pe/uploads/document/file/2096238/Sobre%20los%20datos%20biom%C3%A9tricos%20y%20su%20empleo%20en%20la%20identificaci%C3%B3n%20de%20personas%2C%20el%20tratamiento%20de%20datos%20personales%2C%20la%20obtenci%C3%B3n%20del%20consentimiento%2C%20la%20conservaci%C3%B3n%20de%20documentos%20digitales%2C%20la%20atenci%C3%B3n%20de%20derechos%20ARCO%20y%20registro%20de%20bancos%20de%20datos.pdf?v=1629379994
Última visita 09-09-2024

.

95. Cabe precisar que la administrada, en su escrito del 24 de octubre de 2024, presentó un informe legal elaborado por la consultora IA Law Digital Lawyers, en el cual se reconoce los riesgos que se pueden generar por el uso de sistemas de identificación biométrica (página 5 y 6).

96. Por lo tanto, es ineludible la obligación de proteger al titular de los datos personales frente a posibles abusos o riesgos derivados de la utilización de sus datos en especial los datos sensibles, incluso brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" (biométricos) y que no deben ser objeto de difusión ni de registro; así como otorgarle la facultad de poder oponerse a la transmisión y difusión de los mismos, tal como señaló el Tribunal Constitucional en su Sentencia recaída en el Exp. 300-2010-PHD/TC[52].

97. Es por ello que, la LPDP y su Reglamento establecen disposiciones que tienen como objeto garantizar el derecho fundamental a la protección de los datos personales, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales relacionados a éstos, debiendo los titulares y encargados del tratamiento de datos personales, ajustar sus actuaciones a los principios rectores contenidos en la LPDP, tal como dispone el artículo 12 de la citada norma.

98. Dentro de estos principios rectores, se encuentran los principios de proporcionalidad y finalidad contenidos en los artículos 6 y 7 de la LPDP[53], que obligan al titular o encargado del tratamiento de datos personales a recopilar aquellos datos que únicamente sean necesarios, pertinentes y adecuados para cumplir con la finalidad determinada, explícita y lícita para la que requiere ser obtenidos en su tratamiento.

99. Por otra parte, la LPDP establece como otro de sus principios rectores al consentimiento, señalando en su artículo 5 que, "para el tratamiento de los datos personales debe mediar el consentimiento del titular". En esa misma línea, el artículo 13, inciso 13.5, de la citada norma establece que "los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa"[54]; dicho consentimiento debe ser "previo, informado, expreso e inequívoco", siendo que sus características del consentimiento[55] son desarrolladas en el artículo 12° del

---

52 Fundamento 5 de la Sentencia del Tribunal Constitucional del 11 de mayo de 2010 (Exp. 300-2010-PHD/TC).

53 **Ley N.° 29733, Ley de Protección de Datos Personales**
***Artículo 7. Principio de proporcionalidad***
*Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados*.

***"Artículo 8.- Principio de finalidad.***
*(…)*
*Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales*

54 **Ley N.° 29733, Ley de Protección de Datos Personales**
***"Artículo 5. Principio de consentimiento***
*Para el tratamiento de los datos personales debe mediar el consentimiento de su titular*.

***Artículo 13. Alcances sobre el tratamiento de datos personales***
*(…)*
*13.5 Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco*."

55 **Reglamento de la Ley N.° 29733**

Reglamento de la LPDP; y, en el caso de datos sensibles, como son los datos biométricos, el consentimiento debe efectuarse por escrito; y, aun cuando mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.

100. En el presente caso, de las acciones de fiscalización (Acta n° 02-2023 del 27 de marzo de 2023), se verificó que la administrada usa el servicio de biometría facial con la finalidad de validar la identidad de las personas que requieren presentar un reclamo virtual en el sitio web www.viabcp.com, a través de las siguientes acciones:

- En la visita de fiscalización se comprobó que la persona que va a presentar un reclamo debe registrar su número de DNI, luego de ello el Gateway biométrico valida si el dato biométrico de la persona (fotografía) ya se encuentra en el repositorio interno (BASE DE DATOS BIOM), si es la primera vez que se va a someter a la persona a una validación biométrica, se procede a su enrolamiento haciendo uso del servicio de consulta de datos provisto por el RENIEC, de donde se obtiene la ficha que incluye la fotografía que luego será empleada para el análisis biométrico.

- Una vez obtenida la ficha RENIEC, se procede a hacer la validación biométrica haciendo un versus entre la fotografía que se requiere a la persona que va presentar el reclamo (obtenida en tiempo real desde su dispositivo móvil o PC) y la fotografía de la ficha otorgada por el RENIEC[56].

- Cuando una persona realiza un reclamo que requiera una validación biométrica facial por segunda vez, es decir si con anterioridad el banco ya ha realizado una validación biométrica facial, en las consultas ya no es necesario el uso del servicio de consulta de datos provisto por el RENIEC, toda vez que las consultas serán realizadas a la base de datos propia del banco, a la cual han denominado base de datos BIOM (ORACLE 19C), donde se almacenan las

***(…) Artículo 12.- Características del consentimiento***
*Además de lo dispuesto en el artículo 18 de la Ley y en el artículo precedente del presente reglamento, la obtención del consentimiento debe ser:*
*1. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales.*
*(…)*
*2. Previo: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.*
*3. Expreso e Inequívoco: Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.*
*(…)*
*4. Informado: Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente:*
*a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.*
*b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.*
*c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.*
*d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda.*
*e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.*
*f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.*
*g. En su caso, la transferencia nacional e internacional de datos que se efectúen."*

[56] Es necesario precisar que la validación biométrica es realizada con el componente tecnológico del banco provisto por el proveedor Facephi, el cual tiene las capacidades de validar el grado de similitud entre ambas imágenes, la prueba de vida (es decir si la imagen enviada por la persona corresponde a esta en tiempo real y no a una fotografía o video).

imágenes de las personas y/o imágenes del documento de identidad de las mismas debidamente encriptadas.

101. Conforme se puede apreciar, en el presente caso se advierte claramente dos acciones de tratamiento de datos personales sensibles al momento de interponer un reclamo a través del libro de reclamaciones virtual de la administrada:

- Recopilación en tiempo real de patrones biométricos faciales para la validación de identidad del usuario del libro de reclamaciones virtual.

- Recopilación y almacenamiento de patrones biométricos faciales encriptados para la validación de identidad en futuros reclamos, en la base de datos "BIOM".

102. Ahora bien, la administrada, en su recurso de apelación, ha señalado que estaría en la mejor posición para identificar riesgos y problemas de seguridad en el sistema financiero, por lo que ha adoptado la verificación biométrica en su libro de reclamaciones virtual como medida para enfrentar estos riesgos, teniendo en consideración que su decisión estaría protegida bajo la libertad de autoorganización (libertad de empresa).

103. Asimismo, manifiesta que las medidas adoptadas se realizan en cumplimiento de la Resolución SBS N.º 504-2021 del 19 de febrero de 2021, en específico lo establecido en su artículo 18 que exige que el enrolamiento de un usuario en un canal digital requiere verificar su identidad y tomar las medidas necesarias para reducir la posibilidad de suplantación, lo que incluye el uso de dos factores de autenticación diferentes; por lo cual, señala que la Autoridad de Datos debería otorgar discrecionalidad a las entidades reguladas que implementan medidas de seguridad adecuadas a su sector para resguardar la seguridad de los usuarios.

104. En primer lugar, se debe tener presente que, el derecho a la libertad de empresa, como cualquier otro derecho, no es absoluto y, por el contrario, el ejercicio de este derecho, a través de la libertad de organización del empresario, se encuentra limitado por el acceso o ejercicio de los derechos fundamentales de las personas, entre ellos, el derecho fundamental a la autodeterminación informativa.

105. Asimismo, tal como ha señalado el Tribunal Constitucional en su jurisprudencia[57], las intervenciones, injerencias, restricciones o limitaciones a los derechos fundamentales solo devienen inconstitucionales cuando no se encuentran justificadas. Una injerencia carece de justificación cuando no satisface los criterios formales o materiales que se derivan del contenido constitucionalmente protegido del derecho intervenido.

106. Precisamente, ni la LPDP o Reglamento impiden a la administrada que adopten medidas de seguridad para proteger la información que poseen, por el contrario, las normas citadas establecen medidas mínimas de seguridad para un adecuado tratamiento de los datos personales, de esta manera se garantiza que la administrada mantenga la facultad discrecional de implementar las medidas que mejor se adapten al tamaño, naturaleza y la complejidad de sus operaciones.

---

[57] Fundamento 34 del Pleno Sentencia del Tribunal Constitucional del 27 de agosto de 2014 (Exp. 0011-2013-PI/TC).

107. No obstante, las medidas adoptadas no eximen del cumplimiento de los demás principios rectores señalados en la LPDP, como el principio de consentimiento, principio de finalidad, proporcionalidad, entre otros que se encuentran señalados en la cuestión previa.

108. Es por ello que, al implementar las medidas de seguridad que involucran el tratamiento de datos personales, los administrados se encuentran obligados a implementar las medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento; reduciendo la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad, más aún cuando se realiza tratamiento de datos biométricos, que requieren una protección más reforzada, debido a que su vulneración ocasionaría daños perjudiciales a sus titulares.

109. Por otra parte, este Despacho no advierte que exista un conflicto entre las disposiciones establecidas por la SBS en la Resolución SBS N.º 504-2021 del 19 de febrero de 2021 para que las empresas supervisadas por ella cumplan con una adecuada gestión de la seguridad de la información y la ciberseguridad, respecto a los principios rectores y obligaciones en el tratamiento de datos personales establecidas por la LPDP y su Reglamento, toda vez que no implican que el titular o encargado del tratamiento de datos personales dejen de cumplir sus obligaciones correspondientes al sector en el cual desempeñan sus actividades; y, viceversa, el cumplimiento de las disposiciones establecidas en normativas sectoriales que tienen como finalidad defender otros intereses públicos, no implican, que se deba inobservar las citadas normas.

110. Es oportuno tener en cuenta que, el Tribunal Constitucional[58] ha señalado que la Constitución exige no sólo que no se cree legislación contraria a sus disposiciones, sino que la aplicación de tal legislación se realice en armonía con ella misma. Asimismo, nuestro ordenamiento jurídico presupone *la existencia de una normatividad sistémica, pues el derecho es una totalidad es decir, un conjunto de normas entre las cuales existe tanto una unidad como una disposición determinada. Por ende, se le puede conceptualizar como el conjunto o unión de normas dispuestas y ordenadas con respecto a una norma fundamental y relacionadas coherentemente entre sí*.[59] (Exp. N.° 047-2004-AI/TC) de fecha 24 de abril de 2006.

111. El presente caso aborda situaciones relacionadas con el tratamiento de datos biométricos (datos sensibles), por lo cual, es de obligatoria y relevante observancia la LPDP y su Reglamento; asimismo, teniendo en cuenta que su tratamiento está relacionado con la recopilación de los datos personales a través del Libro de Reclamaciones, se tiene que tomar en cuenta las disposiciones sectoriales que regulan su exigencia, y, determinar la exigibilidad de las disposiciones establecidas por la SBS en la Resolución SBS N.º 504-2021 del 19 de febrero de 2021 en el tratamiento que realizada la administrada, conforme se analizará a continuación.

---

58 Fundamento 19 del Pleno Jurisdiccional del Tribunal Constitucional - Caso Hoja de Coca (Exp. N.° 0020-2005-AI/TC y 0021-2005-AI/TC – acumulados).

59 Fundamento 47 del Pleno Jurisdiccional del Tribunal Constitucional (Exp. N.° 047-2004-AI/TC).

**V.1. Si la DPDP motivó su resolución al momento de determinar la responsabilidad de la administrada por el tratamiento desproporcional de datos personales**

112. El principio del debido procedimiento, como expresión administrativa del derecho constitucional al debido proceso, se encuentra reconocido en el numeral 1.2 del artículo IV del TUO de la Ley Nro. 27444. Dicha norma contiene una serie de derechos y garantías, dentro de los cuales se encuentran el derecho de defensa, a probar, a obtener una decisión motivada, entre otros, previstos con el fin de limitar la actuación de los poderes públicos.

113. Del mismo modo, Morón Urbina, refiere que el derecho al debido proceso comprende una serie de derechos que conforman un estándar mínimo de garantía para los administrados que, a grandes rasgos, significa la aplicación en sede administrativa de los derechos concebidos, en principio, para los procesos jurisdiccionales[60].

114. Asimismo, respecto de la motivación de las resoluciones, debe indicarse que en el numeral 4 del artículo 3º del TUO de la LPAG[61], en concordancia con el artículo 6º del citado instrumento[62], se establece que la motivación del acto administrativo debe ser expresa, mediante una relación concreta y directa de los hechos directos relevantes y concretamente probados del caso específico, y la exposición de las razones jurídicas y normativas que con referencia directa a los anteriores justifican el acto adoptado. Al respecto, cabe tener en cuenta el rol informador que cumple la motivación del procedimiento administrativo, ya que representa la exteriorización de las razones en cuya virtud se produce un acto administrativo, y permite, tanto al administrado como a los superiores con potestades de revisión del acto, asumir conocimiento de los hechos reales y jurídicos que fundamentan la decisión administrativa, para poder articular su defensa con posibilidad de criticar las bases en que se funda e impugnarla; o para que el superior al conocer el recurso pueda desarrollar el control examinando todos los datos y si se ajusta a ley. No solo constituye un cargo para la autoridad sino un verdadero derecho de los administrados

---

60 MORÓN URBINA, Juan Carlos. Comentarios a la Ley del Procedimiento Administrativo General. 9.ª edición, 2011, p. 64.

61 **TUO DE LA LPAG**
**Articulo 3.- Requisitos de validez de los actos administrativos**
Son requisitos de validez de los actos administrativos:(...) 4. Motivación. - El acto administrativo debe estar debidamente motivado en proporción al contenido y conforme al ordenamiento jurídico.

62 **TUO DE LA LPAG**
**Artículo 6.- Motivación del acto administrativo**
6.1 La motivación debe ser expresa, mediante una relación concreta y directa de los hechos probados relevantes del caso específico, y la exposición de las razones jurídicas y normativas que con referencia
directa a los anteriores justifican el acto adoptado.
6.2 Puede motivarse mediante la declaración de conformidad con los fundamentos y conclusiones de anteriores dictámenes, decisiones o informes obrantes en el expediente, a condición de que se les identifique de modo certero, y que por esta situación constituyan parte integrante del respectivo acto. Los informes, dictámenes o similares que sirvan de fundamento a la decisión, deben ser notificados al administrado conjuntamente con el acto administrativo.
6.3 No son admisibles como motivación, la exposición de fórmulas generales o vacías de fundamentación para el caso concreto o aquellas fórmulas que por su oscuridad, vaguedad, contradicción o insuficiencia no resulten específicamente esclarecedoras para la motivación del acto.
No constituye causal de nulidad el hecho de que el superior jerárquico de la autoridad que emitió el acto que se impugna tenga una apreciación distinta respecto de la valoración de los medios probatorios o de la aplicación o interpretación del derecho contenida en dicho acto. Dicha apreciación distinta debe conducir a estimar parcial o totalmente el recurso presentado contra el acto impugnado. ( ... )

a fin de apreciar el grado de regularidad con que su caso ha sido apreciado y resuelto[63].

115. El Tribunal Constitucional[64] desarrolló el contenido constitucionalmente protegido del derecho a la debida motivación de las resoluciones judiciales, precisando que éste se ve vulnerado, entre otros supuestos, por la inexistencia de motivación o motivación aparente, que ocurre cuando el Juez "no da cuenta de las razones mínimas que sustentan la decisión o [...] no responde a las alegaciones de las partes del proceso, o porque solo intenta dar un cumplimiento formal al mandato, amparándose en frases sin ningún sustento fáctico o jurídico".

116. En concordancia con lo antes expuesto, el derecho a la debida motivación de las decisiones administrativas que afecten la esfera jurídica de los administrados se verá transgredido cuando la respectiva resolución adolezca de una motivación aparente, es decir, cuando es inexistente debido a que no expone las razones mínimas que sustentan la decisión ni responde a las alegaciones de las partes del proceso[65].

117. Al respecto, la administrada señala que la Superintendencia de Banca y Seguros (SBS), a través de la Resolución SBS 504-2021, exigiría a las empresas del sistema financiero verificar la identidad del usuario en el acceso a los servicios que provea y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad. Asimismo, exigiría la utilización de dos factores de autenticación; es decir, serían dos factores biométricos o de dos factores de categorías diferentes.

118. Que, los servicios brindados por el BCP estarían íntimamente relacionados con aspectos patrimoniales, por lo que, bastaría con que se trate información financiera sensible y por lo tanto tendrían que tomar especiales medidas para cuidar de ello, no solamente cuando afectan directamente el secreto bancario. Asimismo, indica que no tendría sentido excluir a los clientes regulares de la necesidad de una adecuada

---

63 En la LPAG la motivación configura uno de los elementos determinantes del derecho al debido procedimiento que posee el administrado. MORÓN URBINA, Juan Carlos. Comentarios a la Ley del Procedimiento Administrativo General. 13era ed. Tomo I. Lima: Gaceta Jurídica, 2018. p. 235.

64 Sentencia del Tribunal Constitucional 00728-2008-PHC/TC (fundamento 7), del 13 de octubre de 2008, Expediente N° 00728-2008-PHC/TC

65 En esa línea, el Tribunal Constitucional ha manifestado en la sentencia emitida en el Expediente 00728-2008-PHC/TC lo siguiente:

*"7. El derecho a la debida motivación de las resoluciones judiciales es una garantía del justiciable frente a la arbitrariedad judicial y garantiza que las resoluciones no se encuentren justificadas en el mero capricho de los magistrados, sino en datos objetivos que proporciona el ordenamiento jurídico o los que derivan del caso. Sin embargo, no todo ni cualquier error en el que eventualmente incurra una resolución judicial constituye automáticamente la violación del contenido constitucionalmente protegido del derecho a la motivación de las resoluciones judiciales.*

*Así, en el Exp. N° 3943-2006-PA/TC y antes en el voto singular de los magistrados Gonzales Ojeda y Alva Orlandini (Exp. N° 1744-2005-PA/TC), este Colegiado Constitucional ha precisado que el contenido constitucionalmente garantizado de este derecho queda delimitado, entre otros, en los siguientes supuestos:*

***a) Inexistencia de motivación o motivación aparente**. Está fuera de toda duda que se viola el derecho a una decisión debidamente motivada cuando la motivación es inexistente o cuando la misma es solo aparente, en el sentido de que **no da cuenta de las razones mínimas que sustentan la decisión o de que no responde a las alegaciones de las partes del proceso, o porque solo intenta dar un cumplimiento formal al mandato, amparándose en frases sin ningún sustento fáctico o jurídico**.*
(…)"
(Subrayado y énfasis agregado)

verificación de identidad mediante biometría facial, especialmente considerando el aumento de delitos financieros y la facilidad con que se podría suplantar la identidad de los usuarios debido a la sofisticación tecnológica.

119. Señala que, la autenticación biométrica es el medio idóneo elegido por ella para garantizar la seguridad de sus usuarios; sin embargo, para la DPDP la utilización del factor biométrico en la utilización del libro de reclamaciones virtual sería intrusivo y desproporcional, a pesar que la SBS permitiría la utilización de este mecanismo de autenticación

120. Agrega que, la DPDP, tampoco habría realizado mayor análisis acerca de qué otros factores de autenticación podrían ser utilizados y cómo ello garantiza la seguridad del usuario; es decir, no existiría una ponderación de factores cuando la DPDP señala que, para el caso de clientes intermitentes, podría satisfacerse simplemente con la consignación del número de DNI, el cual sería un dato elemental y de muy fácil conocimiento, por lo que no cumpliría con la exigencia de la SBS. Además, la Dirección sugirió de manera genérica que existen otros datos para validar la identidad, pero no presentó alternativas concretas ni consideró la obligación regulatoria de utilizar dos factores de autenticación.

121. Que, la regulación sectorial autorizaría a la administrada a gestionar sus riesgos de la manera más adecuada, dentro de las opciones reconocidas, como la validación a través de la biometría facial y la constatación del DNI con lo registrado en la base de datos del RENIEC y, posteriormente, con la base de datos que ha recopilado. Así entonces, no existiría otro medio de validación de identidad a distancia por factibilidad por seguridad, siendo este el mismo mecanismo que utiliza el RENIEC para solicitudes de duplicado de DNI; además de que debería considerarse los riesgos advertidos por la SBS en el documento adjunto como Anexo 5-A.

122. Indica que, existiría un interés legítimo en el tratamiento de datos personales de clientes que han contratado un producto BCP, pues con la implementación de la validación biométrica, BCP buscaría (i) proteger la seguridad de sus usuarios; y, (ii) ejecutar la relación contractual con estos (en el marco del servicio prestado a través del LVR); por lo tanto, constituiría un tratamiento lícito.

123. Del recurso de apelación presentado por la administrada se advierte que no existe un cuestionamiento respecto a la realización del tratamiento de datos personales indicado en los hechos imputados respecto a la infracción I; es decir, que a través de su libro de reclamaciones virtual se recopilaría la fotografía del Documento Nacional de Identidad - DNI y la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica (datos biométricos).

124. Sin embargo, la administrada cuestiona que este tratamiento sea desproporcionado, puesto que considera que el mecanismo de validación biométrica es una exigencia legal establecida en la Resolución SBS 504-2021 y es el único mecanismo disponible para validar la identidad de un usuario en el libro de reclamaciones virtual, en todos los supuestos reclamables, en especial de los “no clientes” o también denominados “clientes intermitentes”.

125. Al respecto, la DPDP, en la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024, señaló los siguiente:

*"97. De la normativa sectorial emitida por la SBS, se deduce que para la autenticación de la identidad de los usuarios de servicios digitales, se tienen tres tipos de factores para su verificación, de los cuales pueden ser utilizados dos combinados en los casos de enrolamiento del usuario, cuando no se opte por la asignación de credenciales, o en los casos que requieran autenticación reforzada, previstos en el artículo 18 del Reglamento de la SBS.*
*(…)*
*103. Esta Dirección considera que si bien existe una disposición sectorial que tiene previsto el uso de la autenticación biométrica con lo almacenado en su base de datos "BIOM" como mecanismo de validación de identidad, este no es el único ni excluyente medio para tal fin, toda vez que se cuenta con la comprobación de factores como aquello que solo el usuario tiene y un elemento que solo el usuario conoce, pudiendo emplearse estos conjuntamente, en observancia del principio de proporcionalidad.*
*104. En efecto, la DFI pudo comprobar, al revisar el procedimiento de presentación de reclamaciones virtuales, que estas incluyen tanto la validación empleando el número de tarjeta asignado al usuario y la contraseña creada por este, que constituyen el factor que solo este "posee" y que solo este "conoce", en concordancia con el literal j) del artículo 2 del Reglamento de la SBS, y lo requerido en el artículo 18 de dicha norma.*
*105. Debe tenerse claro que el proceso anterior es aplicable a los portadores de las tarjetas señaladas, de quienes también se tiene otros datos personales preexistentes, recopilados al momento de haber adquirido algún producto financiero, que contribuyen a la verificación de la identidad, así como a la remisión de la información financiera a la persona titular de un número telefónico o correo electrónico inscrito como dato de contacto de este usuario, con lo cual es tangible la existencia de más elementos a emplear para la verificación de la identidad y para sostener una comunicación con el verdadero cliente, con la que este pueda estar al tanto de cualquier movimiento o proceso de reclamación.*
*106. Por otra parte, para otro tipo de usuarios de dicho libro de reclamaciones (denominados "clientes intermitentes" por la administrada), se emplea la imagen del DNI, así como la fotografía facial, en tiempo real, de la cual se obtienen los datos biométricos materia de tratamiento; acciones con las cuales, a entender de la administrada, se asegura la correcta verificación de la identidad, cumpliendo con el principio de Calidad de la LPDP.*
*(…)*
*112. Esta Dirección concuerda con la necesidad de una correcta verificación de la identidad de los usuarios en transacciones y reclamaciones financieras efectuadas en vía virtual, siendo una finalidad válida para cuyo alcance es necesario analizar opciones que sean menos intrusivas y perjudiciales para la privacidad de la información personal del usuario, como concreción de su derecho fundamental a la protección de datos personales; por lo que resulta necesario efectuar sobre este un test de proporcionalidad sobre su tratamiento, vale decir, la determinación de su idoneidad, necesidad y ponderación o proporcionalidad en sentido estricto, de acuerdo con lo establecido en la sentencia del Tribunal Constitucional recaída en el expediente N° 0045-2004-PI/TC, pudiendo determinar con ello si la obtención y empleo de los patrones biométricos faciales es necesaria o si existe una modalidad menos invasiva y riesgosa para la privacidad de los usuarios.*
*113. En cuanto a la idoneidad, entendida como la causalidad entre un determinado medio y su finalidad, justificando su adopción, se ve que en el presente caso, la administrada requiere alcanzar la válida finalidad de verificación de identidad de los reclamantes vía libro de reclamaciones virtual, para lo cual cuenta con una pluralidad de opciones: Uso del número de tarjeta y contraseña, y en casos en los que el usuario no posea tarjetas ni productos financieros, la imagen del DNI en conjunto con el dato biométrico obtenido, a ser contrastadas con las imágenes del Registro del Reniec y la base de datos "BIOM" de patrones biométricos.*

> *114. Esta Dirección aprecia que para el caso de titulares de tarjetas y productos financieros de la administrada, se aprecia la importancia de una mayor seguridad en la autenticación de la identidad, por lo que la administrada se sirve de la biometría facial, contrastando el patrón biométrico de una imagen tomada en tiempo real, con las de las imágenes del Reniec a las que tiene acceso y con los patrones biométricos almacenados en la base de datos "BIOM".*
> *115. En concordancia con lo explicado en el considerando 105 de esta resolución directoral, no es necesaria la recopilación ni uso de datos biométricos (patrón facial biométrico), existiendo claramente otros medios para la verificación de la identidad de los usuarios del libro de reclamaciones virtual que sean clientes y tengan algún producto financiero, así como para el posterior seguimiento de las comunicaciones y sus respuestas.*
> *116. Por su parte, para el específico caso de usuarios que no cuenten con tarjetas de la administrada, los denominados "clientes intermitentes", y/o quienes interpongan quejas, primordialmente comunicaciones en las que no es necesaria la información financiera, el movimiento de dinero u otra acción que implique un riesgo significativo para información patrimonial, la verificación de la identidad es necesaria, pero puede satisfacerse con la consignación del número de DNI en el formulario correspondientes.*
> *117. Ahora bien, dentro de este tipo de comunicaciones de los "clientes intermitentes", en supuestos menos comunes en los que podría comprometerse algún tipo de información patrimonial y/o pueda vulnerar la privacidad del usuario o algún cliente, podría ser necesaria una última verificación de identidad más rigurosa, dependiendo esto de algún dato que se consigne o se marque en el formulario correspondiente, como la existencia de dinero comprometido.*
> *118. Entonces, el empleo del patrón biométrico facial solo sería necesario para estos últimos casos, en los que usuarios sin productos financieros de la administrada comuniquen alguna disconformidad relacionada con algún movimiento de dinero, factor por el cual podría activarse tal modalidad de identidad, conjuntamente con la mención del número de DNI del usuario."*
>
> Subrayado nuestro

126. Este Despacho aprecia que para la DPDP existe un tratamiento desproporcionado en la recopilación de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, ya sean clientes o clientes intermitentes, toda vez que, en el caso de los primeros, la administrada ha identificado y puesto a disposición un mecanismo de validación de identidad menos intrusivo que la verificación biométrica, con el cual cumpliría con las exigencias de la disposición sectorial (Resolución SBS 504-2021) y a pesar de ello, también realizaría la verificación biométrica de los usuarios – clientes.

127. Por su parte, respecto a los usuarios no clientes o "clientes intermitentes", considera desproporcionado la utilización de mecanismos de verificación biométrica facial en todos los supuestos de reclamos, debiendo únicamente ser exigible en los supuestos donde se comprometa la información patrimonial y/o pueda vulnerar la privacidad del usuario o algún cliente, dependiendo esto de algún dato que se consigne o se marque en el formulario correspondiente, como la existencia de dinero comprometido.

128. Sin embargo, si bien este Despacho comparte la mayor parte de los fundamentos aportados por la DPDP, debe realizar algunas precisiones respecto al tratamiento de datos personales a través del libro de reclamaciones virtual para la atención del usuario reclamante y los mecanismos de seguridad que exigiría la SBS (Resolución SBS 504-2021).

**V.1.1. La Resolución SBS 504-2021 y la exigencia de su aplicación en relación al libro de reclamaciones de proveedores de servicios regulados y/o supervisados por la SBS**

129. La administrada, en su recurso de apelación, así como en los escritos e informes presentados de forma posterior a dicho recurso, ha reiterado que resulta válido y proporcional el uso de sistemas biométricos por parte de las entidades financieras para la verificación o autenticación de la identidad de sus clientes, considerando los riesgos de suplantación y sustracción de información que enfrentaría el mercado financiero, conforme a los reportes adjuntados en el procedimiento administrativo.

130. En primer lugar, tal como se señaló en la Opinión Consultiva N° 032-2021-JUS/DGTAIPD de fecha 17 de agosto de 2021, este Despacho considera proporcional que las entidades del sistema financiero puedan utilizar sistemas de identificación biométrica para efectos de la validación de la identidad de sus usuarios en la celebración de contratos de otorgamiento de créditos, el cual puede considerarse igualmente válido y proporcional para la celebración, ya sea de manera presencial o a través de un canal digital, de otros productos o servicios financieros conforme a su normativa especial, previa evaluación y gestión de los riesgos existentes por parte de la administrada, con la finalidad de reducir los casos de suplantación y sustracción de información señalados en su recurso de apelación.

131. Sin embargo, debemos precisar que el pronunciamiento de la DPDP respecto al primer hecho imputado a la administrada, no es sobre la licitud o la obtención del consentimiento para el tratamiento de los datos personales (biométricos) de los usuarios al momento de brindar sus servicios financieros, sino sobre el incumplimiento del principio de proporcionalidad por recopilar datos personales biométricos que no son estrictamente necesarios, pertinentes y adecuados para cumplir con la finalidad del libro de reclamaciones virtual, cuya implementación constituye un deber legal de todo proveedor de bienes o servicios.

132. Esta distinción es fundamental porque nos permite determinar la exigencia de los mecanismos de validación y autenticación de la identidad establecidos en la Resolución SBS 504-2021 para el acceso a los servicios financieros que brinda la administrada, respecto a aquellos que son necesarios, pertinentes y adecuados para cumplir con la finalidad del libro de reclamaciones virtual.

133. Al respecto, la Resolución SBS 504-2021, resolución que aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, señala en sus artículos 17 y 18 lo siguiente:

> ***Artículo 17. Implementación de los procesos autenticación***
> *17.1 La empresa debe implementar procesos de autenticación, conforme a la definición establecida en este Reglamento,* ***para controlar el acceso a los servicios que provea a sus usuarios por canales digitales****, previo a lo cual debe evaluar formalmente y tomar medidas sobre:*
> *a) El o los factores de autenticación que serán requeridos.*
>
> ***Artículo 18. Enrolamiento del usuario en servicios provistos por canal digital***
> *18.1 El enrolamiento de un usuario* ***en un canal digital*** *requiere por lo menos:*
> *a) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores*

> *biométricos o el uso de dos factores de categorías diferentes e independientes, según el literal j) del artículo 2 de este Reglamento, salvo se traten de productos de seguros incluidos en el régimen simplificado de debida diligencia de conocimiento del cliente, conforme a lo establecido en el artículo 31 del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS N° 2660-2015 y sus normas modificatorias, en cuyo caso se puede hacer uso de un único factor biométrico."*
> *b) Generar las credenciales y asignarlas al usuario*
> *18.2 La empresa debe gestionar el ciclo de vida de las credenciales que genere y asigne a sus usuarios, para lo cual debe prever los procedimientos para su activación, suspensión, reemplazo, renovación y revocación; así también, cuando corresponda, asegurar su confidencialidad e integridad*

134. En primer lugar, de acuerdo a las disposiciones de la Resolución SBS 504-2021, se advierte que no se ha considerado que la exigencia establecida en el artículo 18 de la Resolución SBS 504-2021 de verificar la identidad de un usuario a través de los factores de autenticación independientes y de diferentes categorías durante el enrolamiento de un usuario, implica necesariamente que este se realice en un canal digital a través del cual la administrada provea servicios a sus usuarios.

135. Precisamente, el literal d del artículo 2 de la Resolución SBS 504-2021 define al canal digital como el *"medio empleado por las empresas para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits."*

136. En el presente caso, si bien se ha verificado que la administrada ha puesto a disposición un canal digital en su página web para que los usuarios puedan presentar sus quejas o reclamos, ello no implica que automáticamente este canal de atención se convierta en un canal digital para proveer servicios, conforme al marco normativo dispuesto en la Resolución SBS 504-2021.

137. Precisamente, el Capítulo I, del Título III de la Sección Primera de la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, señala cuáles son los servicios que pueden proveer las empresas bancarias como la administrada[66], no advirtiéndose que la

---

[66] **Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros**
**Artículo 221.- Operaciones y servicios**
Las empresas podrán realizar las siguientes operaciones y servicios, de acuerdo a lo dispuesto por el capítulo I del título IV de esta sección segunda:
1. Recibir depósitos a la vista;
2. Recibir depósitos a plazo y de ahorros, así como en custodia;
3. a) Otorgar sobregiros o avances en cuentas corrientes
b) Otorgar créditos directos, con o sin garantía
c) Otorgar créditos de consumo, créditos de consumo de bajo monto y crédito para las pequeñas y microempresas. El crédito de consumo de bajo monto es el crédito cuyo monto es igual o menor a 2 UIT.**"**
4. Descontar y conceder adelantos sobre letras de cambio, pagarés y otros documentos comprobatorios de deuda;
5. Conceder préstamos hipotecarios y prendarios; y, en relación con ellos, emitir títulos valores, instrumentos hipotecarios y prendarios, tanto en moneda nacional como extranjera;
5-A. Conceder préstamos en la modalidad de hipoteca inversa, y con relación a estos emitir títulos valores e instrumentos hipotecarios tanto en moneda nacional como extranjera**"**
6. Otorgar avales, fianzas y otras garantías, inclusive en favor de otras empresas del sistema financiero;
7. Emitir, avisar, confirmar y negociar cartas de crédito, a la vista o a plazo, de acuerdo con los usos internacionales y en general canalizar operaciones de comercio exterior;
8. Actuar en sindicación con otras empresas para otorgar créditos y garantías, bajo las responsabilidades que se contemplen en el convenio respectivo;
9. Adquirir y negociar certificados de depósito emitidos por una empresa, instrumentos hipotecarios, warrants y letras de cambio provenientes de transacciones comerciales;

recepción y/o resolución de quejas o reclamos sea un servicio propio del sistema financiero; y, que por tal motivo deba sujetarse a lo dispuesto en la Resolución SBS 504-2021.

138. Aún más, la misma Resolución SBS 504-2021 en su artículo 19 señala cuáles son aquellos servicios que se brindan a través de canales digitales que sí requieren una autenticación reforzada (con combinación de factores independientes y distintos) cuando impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones.

139. Asimismo, en la Resolución SBS 504-2021 reconoce que existen servicios financieros a través de canales digitales que no requieren esta autenticación reforzada en su canal digital porque son, por ejemplo, aquellas operaciones de pago,

---

10. Realizar operaciones de factoring;
11. Realizar operaciones de crédito con empresas del país, así como efectuar depósitos en ellas;
12. Realizar operaciones de crédito con bancos y financieras del exterior, así como efectuar depósitos en unos y otros;
13. Comprar, conservar y vender acciones de bancos u otras instituciones del exterior que operen en la intermediación financiera o en el mercado de valores, o sean auxiliares de unas u otras, con el fin de otorgar alcance internacional a sus actividades. Tratándose de la compra de estas acciones, en un porcentaje superior al tres por ciento (3%) del patrimonio del receptor, se requiere de autorización previa de la Superintendencia;
14. Emitir y colocar bonos, en moneda nacional o extranjera, incluidos los ordinarios, los convertibles, los de arrendamiento financiero, y los subordinados de diversos tipos y en diversas monedas, así como pagarés, certificados de depósito negociables o no negociables, y demás instrumentos representativos de obligaciones, siempre que sean de su propia emisión;
15. Aceptar letras de cambio a plazo, originadas en transacciones comerciales;
16. Efectuar operaciones con commodities y con productos financieros derivados, tales como forwards, futuros, swaps, opciones, derivados crediticios u otros instrumentos o contratos de derivados, conforme a las normas que emita la Superintendencia.**";**
17. Adquirir, conservar y vender valores representativos de capital que se negocien en algún mecanismo centralizado de negociación e instrumentos representativos de deuda privada, conforme a las normas que emita la Superintendencia.**";**
18. Adquirir, conservar y vender acciones de las sociedades que tengan por objeto brindar servicios complementarios o auxiliares, a las empresas y/o a sus subsidiarias;
19. Adquirir, conservar y vender, en condición de partícipes, certificados de participación en los fondos mutuos y fondos de inversión;
20. Comprar, conservar y vender títulos representativos de la deuda pública, interna y externa, así como obligaciones del Banco Central;
21. Comprar, conservar y vender bonos y otros títulos emitidos por organismos multilaterales de crédito de los que el país sea miembro;
22. Comprar, conservar y vender títulos de la deuda de los gobiernos, conforme a las normas que emita la Superintendencia.**"**
23. Operar en moneda extranjera;
24. Emitir certificados bancarios en moneda extranjera y efectuar cambios internacionales;
25. Servir de agente financiero para la colocación y la inversión en el país de recursos externos;
26. Celebrar contratos de compra o de venta de cartera;
27. Realizar operaciones de financiamiento estructurado y participar en procesos de titulización, sujetándose a lo dispuesto en la Ley del Mercado de Valores;
28. Adquirir los bienes inmuebles, mobiliario y equipo;
29. Efectuar cobros, pagos y transferencias de fondos, así como emitir giros contra sus propias oficinas y/o bancos corresponsales;
30. a) Emitir cheques de gerencia;
    b) Emitir órdenes de pago;
31. Emitir cheques de viajero;
32. Aceptar y cumplir las comisiones de confianza que se detalla en el artículo 275;
33. Recibir valores, documentos y objetos en custodia, así como dar en alquiler cajas de seguridad;
34. Expedir y administrar tarjetas de crédito y de débito;
(…)

pagos periódicos o transferencia hacia un beneficiario que se encuentra registrado previamente por el usuario como beneficiario de confianza o sean operaciones que presentan un nivel de bajo riesgo de fraude.

140. De lo anterior, se puede concluir que las disposiciones de la Resolución SBS 504-2021 no exigen que los proveedores de servicios financieros realicen un procedimiento de enrolamiento de usuario o de autenticación reforzada para verificar la identidad de los usuarios que solicitan el libro de reclamaciones virtual, puesto que esta es una herramienta donde los usuarios informan sobre una queja o un reclamo, pero no constituye un canal digital para proveer servicios financieros de la administrada.

141. Para confirmar el criterio expuesto, no solo se toma en consideración las disposiciones de la Resolución SBS 504-2021, sino que, teniendo en cuenta que el tratamiento de los datos personales que se realiza a través del libro de reclamaciones debe observarse la normativa especial que regula el procedimiento de atención de reclamos y quejas, en especial, los relacionados a servicios financieros.

142. Al respecto, el numeral 4 del artículo IV del Título Preliminar del Código de Protección y Defensa al Consumidor, Ley N.º 29571, señala que un servicio ***es cualquier actividad de prestación de servicios*** *que se ofrece en el mercado, inclusive las de naturaleza bancaria, financiera, de crédito, de seguros, previsionales y los servicios técnicos y profesionales. No están incluidos los servicios que prestan las personas bajo relación de dependencia*.

143. Por su parte, los artículos 150 y 152 del Código de Protección y Defensa al Consumidor, Ley N.º 29571, señalan que los establecimientos comerciales deben contar con un libro de reclamaciones, en forma física o virtual, a través del cual los consumidores formular su queja o reclamo respecto de los productos o servicios ofertados. Además, su reglamento en el numeral 3.1 del artículo 3 define al Libro de Reclamaciones como el documento de naturaleza física o virtual provisto por proveedores en el cual **los consumidores podrán registrar quejas o reclamos** sobre los productos o servicios ofrecidos.

144. Asimismo, el citado Reglamento del Libro de Reclamaciones define al Reclamo como la "***manifestación*** *que un consumidor realiza al proveedor a través de una Hoja de Reclamación del Libro de Reclamaciones, mediante la cual* ***expresa una disconformidad*** *relacionada a los bienes expendidos o suministrados o a los servicios prestados";* mientras que la queja constituye la **expresión de *malestar o descontento*** *del consumidor respecto a la atención al público*.

145. De las normas citadas se advierte que el libro de reclamaciones no constituye un servicio financiero, sino una obligación legal que deben cumplir todos los proveedores de bienes o servicios y tiene la característica de ser registro en el cual se incorporan los reclamos o quejas que pueden presentar los usuarios (persona natural o jurídica que utiliza o puede utilizar los productos y servicios ofrecidos por las empresas).

146. Ahora bien, la administrada, al ser un proveedor de servicios financieros, es decir, un proveedor de servicios regulados y/o supervisados por la SBS, se encuentra obligada, entre otros, en habilitar **sistemas de registro** de quejas y reclamos los cuales deberán encontrarse a **disposición inmediata y accesible al consumidor;**

asimismo, también debe cumplir, la regulación que establezca la SBS, conforme a lo señalado en el artículo 2° del citado reglamento.

147. Precisamente, mediante Resolución SBS 4036-2022 de 28 de diciembre de 2022, la SBS aprobó el "Reglamento de Gestión de Reclamos y Requerimientos", el cual es de alcance obligatorio para la administrada, conforme a lo dispuesto en su artículo 1; y, define al servicio como aquel servicio del sistema financiero, de seguros y/o de pensiones o servicio accesorio o auxiliar; es decir, para el caso de la administrada, serían aquellos regulados en la Ley 26702.

148. Por su parte, en su artículo 4 define al reclamo como las comunicaciones presentadas por los usuarios o terceros en nombre de los usuarios, relacionados únicamente con los productos y servicios contratados, o con las operaciones asociadas a estos, en las que expresan su insatisfacción con la operación, producto o servicio recibido o por el incumplimiento de las obligaciones contempladas en los contratos o en el marco normativo vigente, o manifestando la presunta afectación de su legítimo interés. Por lo tanto, se puede diferenciar con mayor claridad entre un canal de atención de reclamos y un canal digital a través del cual la administrada brinda un servicio financiero.

149. Cabe precisar que, para la atención de estos reclamos, se exige distintos canales de atención o recepción de reclamos, los cuales para una empresa de la categoría de la administrada se constituyen, **como mínimo,** a través a) la red de oficinas de atención al público, en caso cuenten con estas; **b) vía telefónica**; c) página web; e incluso, pueden implementar canales digitales, tales como **correo electrónico**, aplicación de dispositivos móviles, aplicaciones de mensajería, entre otros similares, con la finalidad de brindar una atención oportuna y objetiva de las comunicaciones presentadas por los usuarios, conforme a lo detallado en su artículo 8.

150. Ahora bien, la administrada, dentro de sus descargos e incluso en su recurso de apelación, ha indicado que a través de la recepción de reclamos se puede brindar atención a solicitudes relacionadas a los diversos servicios financieros que brinda, pero este argumento no hace más que confirmar que el reclamo no constituye propiamente un servicio financiero, sino que es una manifestación de disconformidad en relación al servicio ofertado y tiene como finalidad que el proveedor de servicios brinde una respuesta oportuna, ya sea a favor o de manera negativa, conforme al literal d del artículo 9 del el Reglamento de Gestión de Reclamos y Requerimientos.

151. Es más, para que un usuario pueda expresar su disconformidad con un servicio financiero, debe brindar al proveedor cierta información obligatoria[67] relacionada al

---

[67] **Decreto Supremo que aprueba el Reglamento del Libro de Reclamaciones del Código de Protección y Defensa del Consumidor - DECRETO SUPREMO N.º 011-2011-PCM**
***Artículo 5.- Características de la Hoja de Reclamación***
*Cada Hoja de Reclamación de naturaleza física deberá contar con tres (03) hojas desglosables, una (01) original y dos (02) autocopiativas; la original será obligatoriamente entregada al consumidor al momento de dejar constancia de su queja o reclamo, la primera copia quedará en posesión del proveedor y la segunda copia será remitida o entregada al INDECOPI cuando sea solicitada por éste.*

*Las Hojas de Reclamaciones, tanto de los Libros de Reclamaciones de naturaleza física como virtual, deberán contener como mínimo la información consignada en el formato del Anexo I del presente Reglamento. Dicha información incluye:*
*- Denominación que permita identificar claramente a la Hoja de Reclamación como tal, incluyendo la razón social del proveedor, número de Registro Único de Contribuyentes y dirección del establecimiento comercial, los cuales estarán impresos o deberán aparecer por defecto, según corresponda.*

producto o servicios contratados (identificación del producto o servicio contratado, monto del producto o servicio contratado objeto del reclamo, detalle de la reclamación o queja), la descripción de la operación, así como sus datos de identificación, incluyendo aquellos necesarios para notificar la respuesta (documento de identidad, domicilio, correo electrónico, teléfono o celular), a fin que el proveedor pueda brindarle una respuesta positiva o negativa en relación a su reclamo, pudiendo incluso, requerir al usuario documentación o información específica o complementaria sobre aspectos relacionados al reclamo, siempre que no cuenten con esta o no la puedan obtener, de manera sustentada, otorgando un plazo no menor a dos (2) días hábiles para su presentación, informándose al usuario las consecuencias derivadas de incumplir con presentar la información solicitada[68].

---

*- Numeración correlativa impresa o que deberá aparecer por defecto*
*- Código de identificación impreso, o que deberá aparecer por defecto, de conformidad con lo establecido en el Artículo 8, según corresponda.*
*- Fecha del reclamo o queja.*
*- **Nombre, domicilio, número de documento de identidad, teléfono y correo electrónico del consumidor.***
***- Nombre, domicilio, teléfono y correo electrónico de uno de los padres o representantes del consumidor, en caso se trate de un menor de edad**.*
*- **Identificación del producto o servicio contratado**.*
*- **Monto del producto o servicio contratado objeto del reclamo**.*
*- **Detalle de la reclamación o queja**.*
*- **Pedido concreto del consumidor respecto al hecho que motiva el reclamo o queja**.*
*- Espacio físico para que el proveedor anote las observaciones y acciones adoptadas con respecto a la queja o reclamo.*
*- Firma del Consumidor en el caso del Libro de Reclamaciones físico.*
*- Nombre del destinatario de la hoja de reclamaciones impreso (consumidor, proveedor, INDECOPI)*
*En caso que el consumidor no consigne como mínimo su nombre, DNI, domicilio o correo electrónico, fecha del reclamo o queja y el detalle de los mismos, estos se considerarán como no presentados."*

[68] **Reglamento de Gestión de Reclamos y Requerimientos, modifican la denominación del Título VI del Reglamento del Régimen Especial para la Gestión de Conducta de Mercado del Sistema Financiero, incorporan procedimiento en el TUPA de la SBS y dictan otras disposiciones**
**Artículo 9. Registro, análisis y respuesta a los reclamos**
9.1 Al momento de la presentación de los reclamos, las empresas deben registrar los datos de identificación del usuario y aquellos necesarios para poder efectuar la notificación de la respuesta. Una vez informados los canales disponibles de respuesta a los reclamos, salvo la excepción indicada en el párrafo 8.2, se registra el canal elegido por el usuario. En caso el usuario no indique el canal para recibir la respuesta al reclamo o en caso este sea presentado por un tercero, la empresa la envía a la dirección domiciliaria o al correo electrónico registrado por el usuario.
9.2 Cuando el reclamo se presenta en una oficina de atención al público, la empresa debe entregar al usuario un reporte que contenga como mínimo la siguiente información:
a) Fecha y hora de la presentación del reclamo.
b) Identificación de la empresa
c) Fecha estimada de respuesta.
d) Código del reclamo.
**e) Canal de respuesta, según elección del usuario.**
**f) Datos de identificación del usuario, incluyendo aquellos necesarios para notificar la respuesta.**
**g) Descripción de la operación, producto y/o servicio vinculado al reclamo.**
**h) Detalle del reclamo y/o solicitud del cliente**.
9.3 En caso el reclamo se presente por un canal distinto al indicado en el párrafo 9.2, se debe comunicar al usuario al momento de su presentación, el código del reclamo, la fecha y hora de su presentación. La empresa debe poner a disposición del usuario, el reporte con los datos señalados en el párrafo 9.2 en el canal elegido por el usuario para recibir la respuesta al reclamo, según lo dispuesto en el párrafo 9.1, a más tardar al día hábil siguiente de la presentación del reclamo.
9.4 **Las empresas pueden requerir al usuario documentación o información específica o complementaria sobre aspectos relacionados al reclamo, siempre que no cuenten con esta o no la puedan obtener, de manera sustentada, otorgando un plazo no menor a dos (2) días hábiles para su presentación, informándose al usuario las consecuencias derivadas de incumplir con presentar la información solicitada en este párrafo. Durante dicho periodo, el plazo de atención señalado en el párrafo 7.1 del artículo 7 se suspende y las empresas deben orientar a los usuarios para la obtención de dicha documentación.** La reanudación del plazo ocurre al vencimiento del plazo concedido por la empresa o desde que la empresa recibe la información remitida por el usuario, lo que ocurra primero. Si vencido dicho plazo el usuario no cumple con lo requerido, las empresas pueden proceder con la anulación del reclamo, sin perjuicio de mantener su registro.
9.5 En caso el usuario presente comunicaciones reiterativas sobre un mismo reclamo, su registro debe encontrarse vinculado al reclamo previo, conforme a lo señalado en el Anexo 1-A del Reglamento.

152. Es decir, es el propio usuario quien, al momento de registrar su queja o reclamo, no solo debe brindar los datos personales que permitan su identificación sino a su vez los datos personales que permitan a la administrada identificar el producto o servicio financiero contratado, las operaciones asociadas a estos o la situación que generó la insatisfacción o inconveniente relacionados a sus productos o servicios. Estos datos son necesarios para que la entidad financiera pueda brindar una adecuada atención a su queja o reclamo; e inclusive, ante la falta de los mismos puedan realizar observaciones respecto de la información brindada, no porque la autoridad de datos personales lo considera como mecanismo adicional de validación de la identidad de los usuarios que presentan quejas o reclamos, sino porque es una disposición establecida en la normativa especial de atención de reclamos conforme a lo señalado en el artículo 9 de citado reglamento.

153. Comprender la finalidad de la presentación de un reclamo así como los alcances de la respuesta que deba otorgarse a los usuarios, es importante, porque no solo la distingue de otros servicios financieros que brinda la administrada, sino también de cualquier otro servicio que pueden ofrecer terceros distintos a las entidades financieras, a través de sus distintos canales digitales, como por ejemplo del Registro Nacional de Identificación y Estado Civil - RENIEC, que a través de sus servicios, necesariamente debe transferir los datos personales que solicitan sus usuarios; por lo cual, en esos casos sí se encuentra justificado la implementación de un mecanismo de autenticación reforzada que acredite la identidad del titular de estos datos[69].

154. Así entonces, un reclamo no está dentro de la categoría de servicios que la administrada provee a sus clientes o usuarios, sino que este se genera como consecuencia de la insatisfacción a la calidad de los servicios que la administrada ofrece en el mercado, por lo cual, la administrada, si bien está obligada a implementar procedimientos de autenticación, este procedimiento de autenticación está directamente relacionado a la prestación de los servicios propios de su objeto comercial, lo cual no aplica para un usuario o cliente, **e incluso un tercero a favor del usuario**, que considere necesario interponer un reclamo a través de su Libro de Reclamaciones.

155. Como se puede apreciar de las normas legales citadas, el libro de reclamaciones es un registro de los reclamos o quejas que pueden presentar los usuarios (persona natural o jurídica que utiliza o puede utilizar los productos y servicios ofrecidos por las empresas) que no constituye un servicio financiero, sino una **obligación legal** que deben cumplir todos los proveedores de bienes o servicios; y, en el caso de la administrada, al ser un proveedor de servicios regulados y/o supervisados por la SBS**,** debe cumplir con las disposiciones establecidas por este organismo en el Reglamento de Gestión de Reclamos y Requerimientos; sin perjuicio, de las demás disposiciones aplicables referidas a los reclamos y requerimientos comprendidas en las normas de protección al consumidor y en especial, en Reglamento del Libro de

---

69 Sin perjuicio de lo señalado, este Despacho debe precisar que, en su oportunidad ha ejercido sus facultades fiscalizadoras y sancionadoras para verificar un adecuado tratamiento de los datos personales contenidos en los bancos de datos de la RENIEC (p.ej. Exp. 116-2022-JUS/DGTAIPD-PAS); ha emitido opiniones consultivas respecto al suministro de información en las bases de datos que administra dicha entidad (Opinión Consultiva N.º 09-2018-JUS/DGTAIPD y Opinión Consultiva N.º 034-2023-DGTAIP); y, ha precisado, en su oportunidad, que el RENIEC es la única entidad encargada de organizar y mantener el registro único de identificación de personas naturales, incluyendo sus datos biométricos, a través los registros dactiloscópico y pelmatoscópico de las personas (Opinión Consultiva N.º 032-2021-JUS/DGTAIPD).

Reclamaciones aprobado por el Decreto Supremo N° 011-2011-PCM y sus normas modificatorias (disposición complementaria segunda final).

156. Asimismo, tal como ha señalado la DFI en el fundamento 15 de su Resolución Directoral N.º 232-2023-JUS/DGTAIPD-DFI de 13 de octubre de 2023, en la medida que el reclamo no constituye una prestación de un servicio que ofrece la administrada, sino la manifestación de una disconformidad sobre el mismo, para el procedimiento de registro y/o recepción de un reclamo presentado por un usuario o inclusive un tercero a favor del usuario, la administrada no se encuentra obligada a implementar en su Libro de Reclamaciones Virtual las medidas de enrolamiento de usuario y/o de autenticación de identidad contenidas en la Resolución SBS N.º 504-2021, pues estos procedimientos sólo se aplican para los servicios financieros que puedan brindar a sus usuarios.

157. En consecuencia, la validación biométrica y la exigencia de cargar una fotografía o imagen escaneada del DNI de sus usuarios y clientes no se encuentra expresamente establecida en la Ley o Reglamento para su utilización en el canal de atención, ya sea físico o virtual, del Libro de Reclamaciones, sino únicamente para los servicios financieros que ofrece la administrada, en cumplimiento de las disposiciones de la SBS y en el marco de los servicios financieros que ofrece según la Ley 26702; por lo que, corresponde analizar la necesidad, pertinencia y adecuación de recopilar datos personales a través de la validación biométrica de la imagen facial del titular de los datos personales y la exigencia de cargar una fotografía o imagen escaneada de su DNI para que pueda presentar un reclamo a través del cual pueda manifestar la insatisfacción de un servicio prestado, el mismo que puede ser un cliente o potencial cliente de la administrada, e incluso un tercero en representación de los mismos.

#### V.1.2. Sobre el análisis realizado por la DPDP para determinar el tratamiento desproporcionado

158. Como se ha aclarado en el análisis previo, el mecanismo de validación de identidad a través de la verificación biométrica de usuarios clientes y no clientes en el Libro de Reclamaciones Virtual de la administrada no constituye una obligación establecida por la SBS; por lo cual, corresponde analizar si su implementación facultativa como medida de seguridad implica un tratamiento desproporcionado de datos personales sensibles y, por tanto, confirmar o no el criterio de la DPDP al respecto.

159. En primer lugar, tal como ha señalado la administrada, el Tribunal Constitucional, a través de la Sentencia del 29 de octubre de 2005 en el Exp. N.º 045-2004-PI/TC, ha establecido que el análisis de proporcionalidad esencialmente está compuesto de tres aspectos:

> ***"(…)38. Examen de idoneidad***. *La idoneidad consiste en la relación de causalidad, de medio a fin, entre el medio adoptado, a través de la intervención legislativa, y el fin propuesto por el legislador. Se trata del análisis de una relación medio-fin. Tratándose del análisis de una intervención en la prohibición de discriminación, el análisis consistirá en examinar si el tratamiento diferenciado adoptado por el legislador conduce a la consecución de un fin constitucional. En caso de que el tratamiento diferenciado no sea idóneo, será inconstitucional.*
> *En el examen de idoneidad, el análisis del vínculo de causalidad tiene dos fases: (1) el de la relación entre la intervención en la igualdad - medio- y el objetivo, y (2) el de la relación entre objetivo y finalidad de la intervención.*

***39. Examen de necesidad**. Bajo este test ha de analizarse si existen medios alternativos al optado por el legislador que no sean gravosos o, al menos, que lo sean en menor intensidad. Se trata del análisis de una relación medio-medio, esto es, de una comparación entre medios; el optado por el legislador y el o los hipotéticos que hubiera podido adoptar para alcanzar el mismo fin. Por esto, el o los medios hipotéticos alternativos han de ser igualmente idóneos.*
*Ahora bien, el presupuesto de este examen es que se esté ante un medio idóneo, puesto que si el trato diferenciado examinado no lo fuera, no habría la posibilidad conceptual de efectuar tal comparación entre medios. En el examen de necesidad se compara dos medios idóneos. El optado por el legislador -la intervención en la igualdad- y el o los hipotéticos alternativos. Por esta razón, si el primero estuviera ausente, debido a que no habría superado el examen de idoneidad, el test de necesidad no tendrá lugar.*
*El examen según el principio de necesidad importa el análisis de dos aspectos: (1) la detección de si hay medios hipotéticos alternativos idóneos y (2) la determinación de (2.1) si tales medios -idóneos- no intervienen en la prohibición de discriminación, o, (2.2) si, interviniéndolo, tal intervención reviste menor intensidad. El análisis de los medios alternativos se efectúa con relación al objetivo del trato diferenciado, no con respecto a su finalidad. El medio alternativo hipotético debe ser idóneo para la consecución del objetivo del trato diferenciado. En consecuencia, si del análisis resulta que (1) existe al menos un medio hipotético igualmente idóneo que (2.1) no interviene en la prohibición de discriminación o que (2.2), interviniendo, tal intervención es de menor intensidad que la adoptada por el legislador, entonces, la ley habrá infringido el principio-derecho de igualdad y será inconstitucional.*

***40. Proporcionalidad en sentido estricto**. La proporcionalidad en sentido estricto o ponderación (Abwagung), proyectada al análisis del trato diferenciado, consistirá en una comparación entre el grado de realización u optimización del fin constitucional y la intensidad de la intervención en la igualdad. La comparación de estas dos variables ha de efectuarse según la denominada ley de ponderación. Conforme a ésta:*
*"Cuanto mayor es el grado de la no satisfacción o de la afectación de un principio, tanto mayor tiene que ser la importancia de la satisfacción del otro".*
*Como se aprecia, hay dos elementos: la afectación -o no realización- de un principio y la satisfacción -o realización- del otro. En el caso de la igualdad es ésta el principio afectado o intervenido, mientras que el principio, derecho o bien constitucional a cuya consecución se orienta el tratamiento diferenciado -la "afectación de la igualdad" - es el fin constitucional. Por esto, la ponderación en los casos de igualdad supone una colisión entre el principio-derecho igualdad y el fin constitucional del tratamiento diferenciado.*
*Proyectada la ley de ponderación al análisis de la intervención de la igualdad, la ley de ponderación sería enunciada en los siguientes términos:*
*"Cuanto mayor es el grado de afectación -intervención- al principio de igualdad, tanto mayor ha de ser el grado de optimización o realización del fin constitucional". Se establece aquí una relación directamente proporcional según la cual: cuanto mayor es la intensidad de la intervención o afectación de la igualdad, tanto mayor ha de ser el grado de realización u optimización del fin constitucional. Si esta relación se cumple, entonces, la intervención en la igualdad habrá superado el examen de la ponderación y no será inconstitucional; por el contrario, en el supuesto de que la intensidad de la afectación en la igualdad sea mayor al grado de realización del fin constitucional, entonces, la intervención en la igualdad no estará justificada y será inconstitucional."*
***41. Forma de aplicación.** Los subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto o ponderación han de aplicarse sucesivamente. Primero, se ha de examinar la idoneidad de la intervención; si la intervención en la igualdad -el trato diferenciado- no es idónea, entonces, será inconstitucional. Por tanto, como se afirmó, no corresponderá examinarlo bajo el subprincipio de necesidad. Por el contrario, si el trato diferenciado -la intervención- fuera idóneo, se procederá a su examen bajo el subprincipio de necesidad. Si aun en este caso, el trato diferenciado*

*superara el examen bajo este principio, corresponderá someterlo a examen bajo el principio de proporcionalidad en sentido estricto o ponderación."*

160. Al respecto, se advierte que, la DPDP en su resolución ha realizado un análisis diferenciado entre los usuarios – clientes, y los usuarios – no clientes o "clientes intermitentes" de la administrada, para determinar si la aplicación del mecanismo de validación de identidad a través de la verificación biométrica es proporcional al tratamiento de datos personales. Por lo tanto, se procederá a revisar dicho análisis.

**A. Verificación biométrica de usuarios – clientes**

161. Sobre el particular, respecto al **examen de idoneidad** se advierte que, en el fundamento 112, 113 y 114 de la resolución la DPDP ha considerado que sí se encuentra justificado la adopción de medidas que permitan la validación de la identidad del reclamante al hacer uso del libro de reclamaciones virtual, Al respecto, siendo que la administrada, en su recurso de apelación, no cuestiona esta conclusión de la DPDP, corresponde proseguir con el examen de necesidad de exigir la verificación biométrica facial en el uso del libro de reclamaciones virtual por parte de sus clientes.

162. Respecto al **examen de necesidad**, la DPDP en sus fundamentos 105 y 115 de la resolución impugnada ha determinado que no es necesaria la recopilación ni el uso de datos biométricos (patrón facial biométrico), existiendo claramente otros medios para la verificación de la identidad de los usuarios del libro de reclamaciones virtual, como por ejemplo, aquellos datos mínimos que son recopilados al momento de adquirir algún producto financiero, consignando como ejemplo, el número telefónico o correo electrónico inscrito como dato de contacto de este usuario, e incluso la misma administrada ha implementado como medida de seguridad idónea el uso del número de tarjeta y la contraseña del cliente.

163. Por su parte, la administrada indica que el artículo 18 de la Resolución SBS N.º 504-2021, en concordancia con el literal j del artículo 2 de la citada resolución, le exigiría a la administrada implementar la autenticación de los reclamantes a través del uso de dos factores biométricos o el uso de dos factores de categorías diferentes e independientes, como se señala a continuación:

> ***Artículo 18. Enrolamiento del usuario en servicios provistos por canal digital***
> *18.1 El enrolamiento de un usuario **en un canal digital** requiere por lo menos:*
> *(:..)*
> *c) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores biométricos o el uso de dos factores de categorías diferentes e independientes, según el literal j) del artículo 2 de este Reglamento, salvo se traten de productos de seguros incluidos en el régimen simplificado de debida diligencia de conocimiento del cliente, conforme a lo establecido en el artículo 31 del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS N° 2660-2015 y sus normas modificatorias, en cuyo caso se puede hacer uso de un único factor biométrico."*
>
> ***Artículo 2. Definiciones***
> *Para efectos de la aplicación del presente Reglamento deben considerarse las siguientes definiciones:*

> ***j) Factores de autenticación de usuario:*** *Aquellos factores empleados para verificar la identidad de un usuario, que pueden corresponder a las siguientes categorías:*
> *- Algo que solo el usuario conoce.*
> *- Algo que solo el usuario posee.*
> *- Algo que el usuario es, que incluye las características biométricas."*

164. Señala que cumpliría con las exigencias de la SBS a través de la recopilación de la imagen frontal y posterior del DNI de cada reclamante conjuntamente con la verificación biométrica facial, el cual considera el único medio idóneo para autenticar la identidad del reclamante, conforme a las misivas o comunicaciones establecidas por dicha entidad para garantizar la seguridad de sus clientes.

165. En primer lugar, tal como se indicó en el acápite **V.1.1.** de esta resolución, la Resolución SBS 504-2021 no constituye normativa obligatoria para el uso del libro de reclamaciones virtual, ya que este no se considera un servicio ofrecido a través de un canal digital. Por lo tanto, considerando la finalidad del libro de reclamaciones, la administrada no estaba obligada a realizar proceso de autenticación o enrolamiento establecido en el artículo 18 de la Resolución SBS 504-2021.

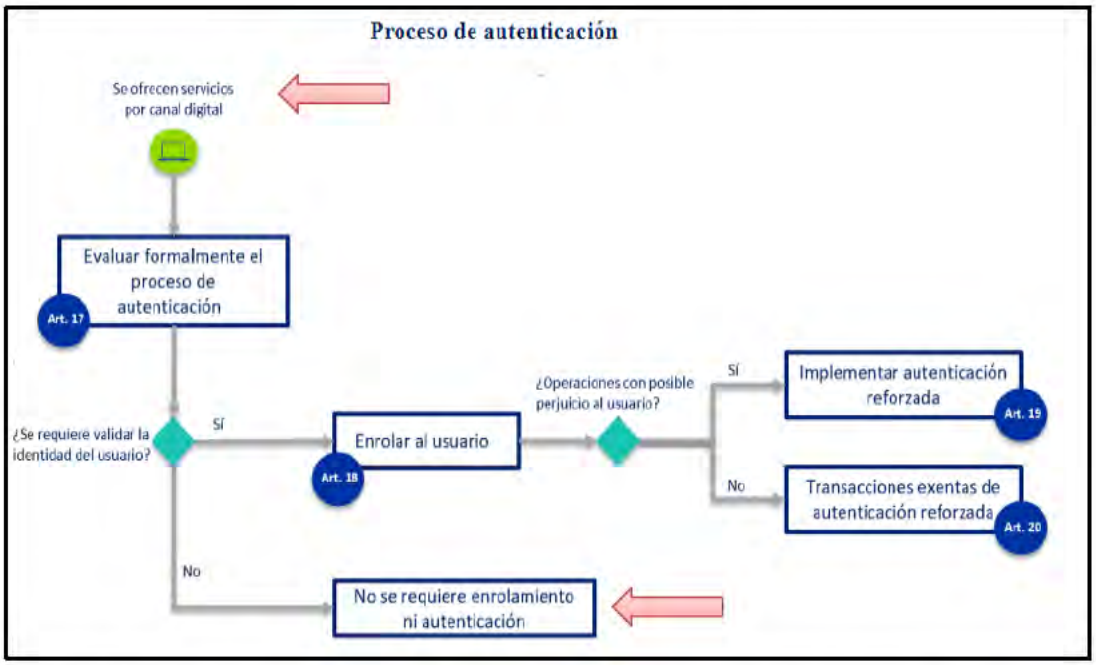
166. Inclusive, si la administrada consideraba que debía implementar algunas medidas de seguridad establecidas en la Resolución SBS 504-2021 para garantizar que la confidencialidad información y que la respuesta se brinde de manera oportuna al usuario a favor de quien se interpone el reclamo, también debió tener presente lo dispuesto en su artículo 4 que señala lo siguiente:

> ***Artículo 4. Proporcionalidad del sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C)***
> *4.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) de la empresa debe ser proporcional al tamaño, la* ***naturaleza y la complejidad de sus operaciones****.*
>
> Énfasis nuestro.

167. Precisamente, la propia SBS señala que no todos los servicios que las empresas reguladas, como la administrada, ofrecen por canales digitales, requieren de un proceso de autenticación y enrolamiento, conforme al siguiente diagrama publicado en su boletín oficial web[70] que se aprecia a continuación:

(ver imagen en la siguiente página)

[70] Disponible en el siguiente enlace: https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222/1000 Última visita 09-09-2024




168. El libro de reclamaciones web de la administrada es precisamente un registro implementado como un canal de atención virtual que no requiere ni enrolamiento ni autenticación al no constituir medio por el cual la administrada brinda productos o servicios financieros para sus usuarios, pues su finalidad es permitir al usuario expresar su disconformidad relacionada a los productos o servicios que son prestados o podrían ser contratados.

169. Sin embargo, la administrada al implementar la validación de identidad a través de la biometría facial y la constatación del DNI con lo registrado en la base de datos del RENIEC, decidió implementar la medida más intrusiva en el tratamiento de datos personales sensibles, pese a que ya existía otra medida igualmente idónea para el mismo fin y que actualmente implementa, como es el uso del número de tarjeta y contraseña única de cada cliente, conforme se encuentra acreditado en las acciones de fiscalización (acta de fiscalización del 27 de septiembre[71] e Informe Técnico N.° 107-2023-DFI-ORQR de 02 de octubre de 2023[72]).

170. Ahora bien, la administrada ha señalado que los usuarios – clientes son libres de elegir de manera alternativa el medio por el cual podrían validar su identidad a través de un medio lícito. Al respecto, en el primer hecho imputado no se está cuestionando el incumplimiento de la administrada de obtener el consentimiento libre de los usuarios para permitir la recopilación de sus datos biométricos (principio de consentimiento), o que estos se estén recopilando datos sensibles a través de un medio ilícito (principio de legalidad), lo que se está cuestionando en el primer hecho imputado es el incumplimiento de la administrada de recopilar los datos que sean estrictamente necesarios, pertinentes y adecuados para cumplir para la finalidad del tratamiento a través del libro de reclamaciones virtual.

71 Obrante en los folios 206 al 216.
72 Obrante en los folios 217 al 222.

171. Es importante resaltar nuevamente que el titular y el encargado de tratamiento de datos personales únicamente está facultado a recopilar aquellos datos necesarios en relación a los fines para los que son tratados, debido a que la LPDP solo permite recabar aquellos datos mínimos necesarios para cumplir con la finalidad prevista, por lo que al momento de recopilar datos personales sensibles que exceden este marco de actuación, se contraviene directamente con el principio de proporcionalidad.

172. Más aún cuando hemos señalado que parte del contenido fundamental del derecho a la autodeterminación informativa involucra la protección especial de los datos sensibles (datos biométricos), a través de la exclusión del registro de este tipo de datos cuando no son necesarios, pertinentes y ni adecuados a la finalidad de identificación del titular que utiliza el libro de reclamaciones virtual para expresar su disconformidad sobre los bienes o servicios ofrecidos por la administrada o únicamente expresa su malestar por la atención al cliente brindado.

173. Cabe precisar que, al desarrollar las medidas técnicas y organizativas implementadas por los responsables en el tratamiento de datos personales deben seguir el principio de *Privacy by Design*, es decir, privacidad desde el diseño, previendo cuáles serán **los datos mínimos que requerirá un tratamiento en concreto para alcanzar la finalidad propuesta**, **antes de comenzar dicho tratamiento** (por ejemplo, para captar clientes potenciales a través de un formulario web, en principio solo es necesario un nombre y una dirección de correo electrónico)[73].

174. A mayor abundamiento, la Agencia Española de Protección de Datos Personales al diseñar las estrategias de diseño de la privacidad reconoce como fundamental la acción de minimizar recoger y tratar la mínima cantidad de datos posible, de modo que, evitando el procesamiento de datos que no sean necesarios para las finalidades perseguidas en el tratamiento, se limitan los posibles impactos en la privacidad[74].

175. Precisamente, para registrar la disconformidad del usuario respecto a los servicios que brinda y posteriormente enviar una ulterior respuesta, ya sea negativa o positiva al reclamo, la administrada debió evaluar aquellos datos mínimos indispensables que debería exigir al usuario para tal finalidad, pero dicho análisis no ha sido realizado, limitándose a señalar que el Reglamento del Libro de Reclamaciones exige datos de identificación mínimos que pueden ser ampliados en virtud de su libertad de empresa y la especialidad de los servicios que brinda, sin evaluar los efectos de su decisión en el tratamiento de los datos personales de los usuarios, aspecto que no puede ser convalidado por este Despacho.

176. Además, si bien la administrada ha señalado que busca la protección de los usuarios para evitar intentos de suplantación o afectación de patrimonio no ha fundamentado por qué al momento de interponer un reclamo a través del libro de reclamaciones virtual, la validación de identidad a través uso del número de tarjeta y contraseña única han resultado insuficientes para identificar al reclamante.

177. Precisamente, el numeral 17.2 del artículo 17 de la Resolución SBS 504-2021 señala que, los procesos de autenticación deben ser reevaluados siempre que la tecnología

---

73 https://protecciondatos-lopd.com/empresas/principio-minimizacion-datos/

74 Guía de Privacidad desde el Diseño de la AEPD, disponible en: https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf

utilizada para su implementación deje de contar con el soporte del fabricante, o tras el descubrimiento de nuevas vulnerabilidades que pueden exponerlos; sin embargo, la administrada no ha acreditado ninguno de estos dos supuestos, limitándose a señalar reportes generales de suplantación de identidad durante la contratación de servicios financieros o reportes de operaciones fraudulentas asociadas a *sim swapping*[75] o *phishing*[76], pero que no detallan su relación causal con el uso del libro de reclamaciones virtual de la administrada.

178. Además, la administrada tampoco ha presentado documentos que acrediten que, de los más de trece mil trescientos cincuenta y siete reclamos recibidos en el 2023 por el canal de atención virtual del libro de reclamaciones, o reclamos presentados en años anteriores, se han identificado supuestos de suplantación o los usuarios han reportado la existencia de reclamos presentados a su nombre que ellos no reconocen; y, por estos motivos, se requiera reforzar la seguridad en la validación de identidad a través de los datos de la tarjeta y la clave que posee cada uno de sus usuarios – clientes.

179. Finalmente, si la administrada consideraba indispensable incrementar los niveles de seguridad en la atención del libro de reclamaciones virtual para usuarios – clientes, tal como ha señalado la DPDP en el fundamento 105 de la resolución impugnada, antes de recurrir a la recopilación de datos biométricos para validar la identidad del usuario, debió evaluar otros medios adicionales para identificar al reclamante, tales como el número telefónico o correo electrónico previamente inscrito por el cliente al adquirir un producto financiero; o inclusive, debió evaluar si era pertinente autenticar a través medios que demuestran la posesión de dispositivos previamente registrados por el usuario como son las notificaciones push y/o tokens digitales.

180. No obstante, dicha evaluación no ha sido acreditada ni sustentada; y, menos aún ha demostrado que tales medios resultaron fallidos para validar la identidad del reclamante en el uso del libro de reclamaciones virtual, por lo cual **no se satisface el examen de necesidad**.

181. Por los motivos anteriormente expuesto, se concluye que el uso de la validación biometría facial para identificar al usuario – cliente cuando utiliza el libro de reclamaciones virtual de su sitio web, si bien cumple con el examen de idoneidad, no supera el examen de necesidad del principio de proporcionalidad, por lo que, no corresponde realizar mayor análisis de la *proporcionalidad en sentido estricto.*

182. Por tales motivos, en este extremo de su recurso de apelación resulta infundado.

**A. Verificación biométrica de usuarios – no clientes**

183. Sobre el particular, respecto al **examen de idoneidad** se advierte que, en el fundamento 116, 117 y 118 de la resolución la DPDP ha considerado que sí se encuentra justificado la adopción de medidas que permitan la validación de la identidad del reclamante al hacer uso del libro de reclamaciones virtual; no obstante, precisa que únicamente cuando se comprometa algún tipo de información patrimonial

[75] SIM Swapping, procedimiento de cambio de chip que se efectúa ante el operador de telefonía móvil que, obtenido mediante suplantación del titular, puede dar a lugar a operaciones fraudulentas en servicios financieros, mediante la vulneración del factor de autenticación en posesión del usuario (dispositivo móvil).

[76] Phishing, modalidad de ciber ataque que busca hacer que la víctima revele datos personales a través de páginas web que fingen ser sitios legítimos

y/o pueda vulnerar la privacidad del usuario o algún cliente, podría ser necesaria una última verificación de identidad más rigurosa como es el caso de empleo del patrón biométrico facial.

184. Al respecto, la administrada, en su recurso de apelación, cuestiona que la DPDP haya considerado que el empleo del patrón biométrico facial se limite a algunos casos en los que se requiera validar la identidad del reclamante, cuando supuestamente se debería aplicar a todo usuario del libro de reclamaciones virtual, en especial los no clientes, debido a que toda la información que posee el banco se encuentra vinculada con aspectos patrimoniales o dinerarios y, debido a que el reclamo se presentaría de manera virtual por usuarios de los que no cuenta mayor información, no existiría otra forma de validar su identidad.

185. En ese sentido, la DPDP no cuestiona la idoneidad de la medida sino la necesidad de utilizar el patrón biométrico facial para todo tipo de usuario – no cliente, por lo que, a partir de dichos argumentos expuestos por la administrada, corresponderá confirmar o revocar el criterio de la DPDP expuesto en su **examen de necesidad.**

186. Sobre el particular, este Despacho advierte que para la DPDP uno de los supuestos que no requiere verificación de identidad con biometría es aquel a través del cual el usuario – no cliente expresa su disconformidad respecto a la atención al público brindada por la administrada, toda vez que, en este supuesto, no involucra información financiera o movimiento de dinero.

187. Al respecto, en su recurso de apelación, la administrada no niega que estos casos no estén relacionados con aspectos patrimoniales o dinerarios, simplemente se limita a indicar que se presentan en pocas ocasiones. Sin embargo, este hecho evidencia la existencia de reclamos presentados, lo cual hace que la verificación biométrica facial en el uso del libro de reclamaciones virtual para estos casos resulta innecesaria y, por tanto, su exigencia, no supera el **examen de necesidad.**

188. Por otra parte, la DPDP aclara que también existen comunicaciones en las que no es necesaria la información financiera, el movimiento de dinero u otra acción que implique un riesgo significativo para información patrimonial, por lo que, si bien la verificación de la identidad es necesaria, también puede satisfacerse con la consignación del número de DNI en el formulario correspondientes.

189. Al respecto, este Despacho concuerda con la DPDP pues tal como se ha señalado en el apartado V.1.1., de la presente resolución, a través del libro de reclamaciones se brinda un registro de disposición inmediata y accesible al consumidor para que pueda expresar una disconformidad relacionada a servicios ofrecidos y/o prestados por la administrada, pero no por ello, implica el reemplazo del canal digital o procedimiento que la administrada emplea para brindar los servicios financieros que previamente hayan sido solicitados o puedan solicitarse.

190. Precisamente, cuando un usuario – no cliente presenta un reclamo, se encuentra obligado a brindar información relacionada al *detalle de la reclamación,* así como el *monto del producto o servicio ofrecido (incluida la identificación del producto o servicio contratado o por contratar)*, así como los motivos de su disconformidad con el servicio ofrecido o proporcionado previamente por la administrada a través del

canal físico o digital correspondiente, conforme a lo dispuesto en el artículo 5 del Reglamento de Libro de Reclamaciones.

191. De esta manera, es el usuario quien proporciona a la administrada la información relacionada al servicio financiero que contrató o por contratar, la misma que queda evidenciada en el registro del reclamo u hoja de reclamación que se imprime o envía al correo electrónico indicado por el usuario, dejándose constancia de la fecha y hora de presentación del reclamo o queja, conforme a lo dispuesto en el artículo 4B del Reglamento del Libro de Reclamaciones.

192. Asimismo, la administrada solo se encuentra obligada a proporcionar al usuario la información estrictamente necesaria para la atención de su reclamo, conjuntamente con la respuesta positiva o negativa de la atención del reclamo. Cabe precisar que, la administrada puede considerar como no presentado un reclamo si el usuario no ha señalado datos mínimos de su identificación, así como el detalle del servicio reclamado, conforme a lo dispuesto en el último párrafo del artículo 5 del Reglamento del Libro de Reclamaciones, pero no extiende su aplicación a otros datos de identificación que deba proporcionar el usuario.

193. Ahora bien, la administrada ha manifestado reiteradamente que, al estar en la mejor posición para identificar riesgos y problemas de seguridad en el sistema financiero, se encuentra facultada a decidir cuál es la mejor medida para enfrentarlos.

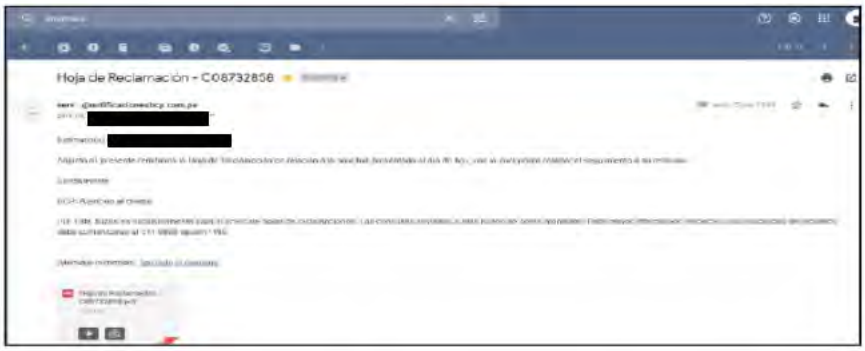
194. Sin embargo, al igual que en el tratamiento de datos sensibles de los usuarios – clientes, tampoco ha acreditado las deficiencias de la validación de identidad en el registro de los reclamos presentados por los usuarios – no clientes, limitándose a enunciar los motivos de seguridad por los cuales sería necesario implementar la validación biométrica, sin distinguir, como se ha señalado en los párrafos previos, que sí existen quejas y también reclamos en los cuales no es necesaria la respuesta que implique información financiera, movimiento de dinero u otra acción que implique un riesgo significativo para información patrimonial, como son aquellos reclamos relacionados con ofertas no cumplidas, problemas en la contratación de un servicio o negativas a la obtención de un documento; situaciones en las cuales previamente el reclamante ha tenido que detallar el tipo de servicio solicitado, la respuesta o negativa del proveedor y los motivos por los cuales interpone el reclamo.

195. Precisamente, el caso de la denunciante es uno de ellos, pues tal como señala en su denuncia (folio 4), el día 15 de junio de 2022, a través vía telefónica al número 013119898 de la Banca por teléfono de la administrada solicitó una constancia de no adeudo respecto al contrato de préstamo hipotecario que mantuvo con la administrada, generándose la hoja de reclamación C-08732858, conforme se aprecia del correo electrónico que confirma el registro de la solicitud con asunto “Hoja de reclamación C-08732858” (folio 28).

196. La administrada en sus descargos presentados (folio 270) no niega que el reclamo haya sido registrado o que este haya sido recibido de manera telefónica, únicamente precisa que este reclamo en realidad constituye parte del servicio que brinda como banco en relación de un crédito hipotecario que mantuvo con la administrada y que fue canalizado como un reclamo, conforme se aprecia a continuación:

crédito hipotecario con el BCP que terminó de pagar. Fue por lo que solicitó al banco una constancia de no adeudo, tal como explicó ella misma en su denuncia y como se puede constatar en la hoja de reclamación que presentó como Anexo 2-B[5]:

7.3. Con fecha 15.06.2022, vía llamada telefónica al número 01 3119898 de la Banca por teléfono del BCP, la suscrita solicita la CONTANCIA DE NO ADEUDO respecto a la Contrato de Préstamo Hipotecario de fecha 18.01.2013, generándose así una hoja de reclamación C-08732858 (denominado solicitud de constancia de no adeudo), tal como se evidencia de la imagen adjunta. Ver. Anexo I-B




25. Estamos ante una solicitud de emisión de una carta de no adeudo producto del pago de su hipoteca, lo que constituye parte del servicio que el banco le brindó en tanto cliente y deudora de un crédito hipotecario. En ese sentido, resulta claro que no estamos ante un reclamo y ciertamente que esta solicitud haya sido canalizada a través de dicho canal no la convierte en un reclamo.

197. En consecuencia, de la revisión del expediente administrativo, no se advierte razonabilidad en exigir la verificación biométrica del usuario para registrar su reclamo o queja en el libro de reclamaciones, donde además debe detallar información sobre el producto o servicio solicitado; y, a su vez, no exija este mismo mecanismo de seguridad cuando un usuario – no cliente, solicite **vía telefónica**, que también es un **canal no presencial de atención**, un servicio que proporciona la administrada, como es la constancia de no adeudo, registrando la solicitud de tal servicio sin la necesidad de requerir la verificación biométrica facial para resguardar la información que pueda brindar con su atención.

198. Así entonces, debe desestimarse el argumento de la administrada en su recurso de apelación a través del cual señala que la verificación biométrica facial es la única medida idónea y necesaria para registrar un reclamo relacionado a un producto o servicio a través de un canal **no presencial**, puesto que sería inconsistente que, para brindar la atención de un servicio de manera no presencial requiera medidas de autenticación no reforzadas, pero para atender la disconformidad relacionado con este servicio sí exija medidas más invasivas en el tratamiento de datos personales como es la verificación biométrica facial, motivo por el cual, esta medida de seguridad tampoco satisface el **examen de necesidad.**

199. Además, de acuerdo al Reglamento de Gestión de Reclamos y Requerimientos, para la atención de estos reclamos, la administrada se encuentra obligada a implementar, **como mínimo,** canales de atención a través **a) la red de oficinas** de atención al público, en caso cuenten con estas; **b) vía telefónica**; **c) página web;** e incluso, puede implementar canales digitales, tales como correo electrónico, aplicación de dispositivos móviles, aplicaciones de mensajería (incluido chatbots), entre otros similares.

200. La diversidad de canales de atención exigidos por la SBS para que los usuarios puedan presentar sus reclamos y requerimientos, no podría permitir que la administrada estandarice la biometría facial como el único procedimiento de identificación del usuario para el registro de su reclamo, por el contrario, se encuentra obligada a evaluar e implementar medios menos invasivos pero igualmente funcionales para la validación de identidad de sus usuarios, de lo contrario no cumpliría con la finalidad de brindar un registro de disposición inmediata y accesible al consumidor.

201. Finalmente, la administrada alegó que la DPDP habría analizado incorrectamente la actividad de almacenamiento en el Hecho Imputado I, debido a que en su resolución señala que el hecho imputado se limitaría a la recopilación para fines de validación de identidad; mientras que, en el Hecho imputado II, se evaluaría si se requiere consentimiento para almacenar dichos datos en su base de datos; pero, de la revisión de los fundamentos 123, 125, 131 y 133 se mezclarían ambos conceptos, lo que afectaría la claridad y precisión del análisis, no siendo coherente que la DPDP se pronuncie sobre una supuesta desproporcionalidad en el almacenamiento de los datos personales.

202. Sobre este aspecto, se debe tener presente que la DPDP ha precisado el ámbito de su pronunciamiento respecto a cada hecho imputado, siendo que, en el fundamento 142 de la resolución impugnada ha precisado que existen dos acciones de tratamiento de los datos biométricos (patrones biométricos faciales) efectuadas a través del libro de reclamaciones virtual:

    - Recopilación en tiempo real para la validación de identidad del usuario del libro de reclamaciones virtual.
    - Recopilación y almacenamiento para la validación de identidad a futuro, en la base de datos “BIOM”.

203. Asimismo, ha indicado que, respecto al hecho imputado I, únicamente se analizó la proporcionalidad de la recopilación de datos para la identificación del usuario, y solo para ese momento, deduciéndose el carácter excesivo de la recopilación de los datos biométricos para la validación en tiempo real, ante la existencia de medios menos invasivos e igualmente funcionales, según cada tipo de usuario y comunicación.

204. Por tales motivos, este Despacho aprecia que la DPDP ha delimitado el ámbito de su pronunciamiento respecto al primer hecho imputado, ha explicado las razones por las cuales considera que existe un tratamiento desproporcionado en la recopilación en tiempo real de los datos personales sensibles (datos biométricos) de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, ya sean clientes o clientes intermitentes.

205. Asimismo, a pesar de que existe una diferencia de criterios respecto a la exigibilidad del enrolamiento y la autenticación de los usuarios del libro de reclamaciones virtual, se aprecia que la DPDP ha justificado las razones por las cuales considera que, la recopilación en tiempo real de los datos biométricos (patrones biométricos faciales) para la validación de identidad del usuario del libro de reclamaciones virtual, constituye un tratamiento desproporcionado al no superar el examen de necesidad, siendo innecesario evaluar el examen de proporcionalidad en sentido estricto.

206. Por tales razones, **no corresponde amparar** este extremo de la apelación presentada por la administrada.

207. Sin perjuicio de lo anterior, este Despacho advierte que la conducta de la administrada puede constituir una posible afectación a los derechos de los consumidores de los servicios financieros y, a las disposiciones a lo dispuesto en la Resolución SBS 4036-2022 de 28 de diciembre de 2022 que aprueba el "Reglamento de Gestión de Reclamos y Requerimientos", por lo cual, se dispone poner en conocimiento de la Superintendencia de Banca y Seguros – SBS, copia de los principales actuados del presente procedimiento administrativo, a fin de que actúe de acuerdo a sus competencias.

208. Por otra parte, considerado lo señalado en el artículo 4 de la Resolución SBS 504-2021[77]; y, que no todos los servicios que las empresas reguladas ofrecen por canales digitales, requieren de un proceso de autenticación y enrolamiento del usuario, tal como ha indicado la SBS, corresponde remitir copia de los actuados del presente procedimiento administrativo sancionador a la DFI a fin que, en el ámbito de sus competencias, verifique si el tratamiento de datos personales biométricos realizado por la administrada a través de otras aplicaciones mediante las cuales brinda servicios financieros ("Yape", "seguros", "Dinero al instante", "Cocos y Lucas", "Banca Móvil", tarjetas", entre otros, señalados en el Acta N.º 02-2023[78]), es conforme a las disposiciones de la Ley N.º 29733, Ley de Protección de Datos Personales.

### V.2. Si la administrada es responsable por el tratamiento de datos personales sensibles sin el consentimiento de sus titulares

209. La administrada señala que la DPDP no tomaría en cuenta que el almacenamiento de datos biométricos no responde a un interés comercial de la administrada (perfilamiento, envío de publicidad), sino que se realiza únicamente para fines de posteriores validaciones de identidad como parte de la debida ejecución de una relación contractual; y, para la protección de intereses legítimos del titular de los datos personales, toda vez que el tratamiento se realizaría con la finalidad de resguardar su seguridad y evitar que su información se comparta con terceros no autorizados.

210. Señala que almacenaría estos datos biométricos faciales de los usuarios y datos biométricos que evidencia la aprobación de una operación a nombre del usuario, de manera encriptada y segura, de tal modo que la información de sus usuarios estaría debidamente protegida y no sería posible que algún tercero pueda "ver" los datos ni "operar" con ellos ante una serie de números y letras que no tienen mayor valor individual, es decir, no podría identificar a una persona.

211. Agrega que, la evaluación de la DPDP se centraría el almacenamiento de datos biométricos faciales, pero no debería extenderse al almacenamiento de valores biométricos con fines de evidencia (cuando la operación autorizada mediante validación biométrica requiere que se almacene un registro de uso de biometría que

---

[77] **Resolución SBS 504-2021 - Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad**
***Artículo 4. Proporcionalidad del sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C)***
*4.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) de la empresa debe ser proporcional al tamaño, la* ***naturaleza y la complejidad de sus operaciones****.*

[78] Obrante en los folios 206 al 216.

sirva como sustento de que fue precisamente el cliente quien aprobó la operación), aspecto sobre el cual se debe pronunciarse el revisor.

212. Sobre el particular, se debe tener presente que, a través de la Resolución Directoral N.º 232-2023-JUS/DGTAIPD-DFI de 13 de octubre de 2023[79], sobre el segundo hecho imputado, la DFI ha señalado lo siguiente:

> ***Hecho imputado N.º 2:*** *Haber realizado el tratamiento de los datos personales sensibles de los usuarios y clientes,* ***al almacenar el dato biométrico referido a la imagen facial, en una base de datos propia****, sin obtener válidamente el consentimiento del titular de los datos personales, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento, lo que configuraría la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP .*
> *(…)*
> *s. Una vez obtenida la ficha RENIEC, se procede a hacer la validación biométrica haciendo un versus entre la fotografía que se requiere a la persona que va presentar el reclamo (obtenida en tiempo real desde su dispositivo móvil o PC) y la fotografía de la ficha otorgada por el RENIEC. Es necesario precisar que la validación biométrica es realizada con el componente tecnológico del banco provisto por el proveedor Facephi, el cual tiene las capacidades de validar el grado de similitud entre ambas imágenes, la prueba de vida (es decir si la imagen enviada por la persona corresponde a esta en tiempo real y no a una fotografía o video). Cuando una persona realiza una transacción, operación o reclamo que requiera una validación biométrica facial por segunda vez, es decir si con anterioridad el banco ya ha realizado una validación biométrica facial, en las consultas ya no es necesario el uso del servicio de consulta de datos provisto por el RENIEC, toda vez que las consultas serán realizadas a la base de datos propia del banco a la cual han denominado base de datos BIOM (ORACLE 19C), donde se almacenan las imágenes de las personas y/o imágenes del documento de identidad de las mismas debidamente encriptadas.*
> *(…)*
> *v. Por su parte, la administrada ha señalado que una vez que el usuario seleccione la opción de reconocimiento facial y antes de continuar con dicho procedimiento, se le solicita que* ***obligatoriamente consienta que ha leído la información respecto al tratamiento de sus datos personales****. Igualmente, ha manifestado que este proceso de reconocimiento biométrico se realiza con el objetivo de velar por la seguridad de sus usuarios, obedeciendo a lo exigido por la Superintendencia de Banca y Seguros, a través de la Resolución n° 504-2021 de fecha 19 de febrero de 2021.*
> *(…)*
> *cc. Como puede verse, la administrada en la información que traslada al usuario o cliente, señala que almacenará la información que consta en el DNI así como la imagen del reclamante, sin que haya establecido un mecanismo adecuado a través del cual la persona pueda otorgar válidamente su consentimiento para que la administrada almacene el dato biométrico referido a la imagen facial, por lo cual se infiere que almacena este dato personal sin la obtención del consentimiento del titular de los datos..*

[79] Obrante en los folios 223 al 255.

> *dd. Por lo tanto, el tratamiento del dato personal referido a la imagen biométrica, no se legitima con la sola información al titular de los datos personales acerca de su tratamiento, sino que es necesario que se recabe el consentimiento, y que este además cumpla con los requisitos ya mencionados anteriormente, de otra manera, la conducta de la administrada configura una infracción.*
> *(…)*

213. Por su parte la DPDP en los fundamentos 142 y 144 de la resolución impugnada delimita el análisis del hecho imputado de la siguiente forma:

> *142. En el presente caso, es necesario distinguir las dos acciones de tratamiento de los datos biométricos (patrones biométricos faciales) efectuadas a través del libro de reclamaciones virtual:*
> - *Recopilación en tiempo real para la validación de identidad del usuario del libro de reclamaciones virtual.*
> - ***Recopilación y almacenamiento para la validación de identidad a futuro, en la base de datos "BIOM".***
>
> *(…)*
> *144. Esclarecida la anterior ilicitud, en el presente subtítulo se analiza si la recopilación y almacenamiento de tales datos sensibles en la mencionada base de datos, para posteriores validaciones, se sostiene en la obtención del consentimiento válido de parte de sus titulares, esto último como factor que legitimaría tal tratamiento.*

214. Como se puede apreciar de los hechos imputados, así como el pronunciamiento de la DPDP, la administrada ha sido sancionada por recopilar y almacenar en su base de datos "BIOM" los datos biométricos (patrones biométricos faciales) correspondientes a las imágenes de las personas y/o imágenes del documento de identidad de las mismas debidamente encriptadas, obtenidas de la primera validación de identidad por biometría facial realizada a través de su canal de atención "libro de reclamaciones virtual".

215. Ahora bien, respecto a las supuestas excepciones al consentimiento alegadas por la administrada, que estarían contenidas en los numerales 5 y 9 del artículo 14 de la LPDP, se debe precisar lo ya desarrollado en el punto controvertido anterior: El libro de reclamaciones virtual es un registro implementado por la administrada en virtud de una obligación legal, a través del cual el usuario puede manifestar su disconformidad sobre un servicio brindado, por lo tanto, no constituye por sí mismo un procedimiento a través del cual se brinda un servicio; y, mucho menos una condición necesaria para la debida ejecución contractual, como alega la administrada, toda vez que en el mismo el usuario tiene la posibilidad de expresar su malestar sobre la atención al público brindada por la administrada, incluso denunciar algún hecho discriminatorio que imposibilita su acceso a algún servicio ofrecido por la administrada; y, por otra parte existen vías administrativas y judiciales específicas para requerir el cumplimiento de las obligaciones a cargo de la administrada.

216. Por otra parte, tampoco puede validarse el argumento de la administrada de estar exceptuada del consentimiento por realizar tratamiento de datos personales con la finalidad de proteger los intereses legítimos de los titulares de los datos personales, toda vez que, conforme a lo determinado en el punto controvertido anterior la verificación de la identidad de los usuarios del libro de reclamaciones virtual a través

del empleo de los patrones biométricos faciales resulta excesivo, por lo que excede del ámbito necesario para la finalidad de este registro (las reclamaciones y quejas), no configurando los supuestos previstos en numerales 5 y 9 del artículo 14 de la LPDP.

217. Adicionalmente, tal como lo ha sancionado la DFI, y ha sido determinado por la DPDP en sus fundamentos 148 y 149 de la resolución impugnada, la continuidad del proceso de presentar un reclamo a través del libro de reclamaciones virtual depende del marcado del sitio web cuando se efectúa la validación con la imagen facial, de la cual se obtiene un patrón biométrico a contrastar; el mismo que informa sobre la finalidad, plazo de conservación, no transferencia de tales datos biométricos, pero no brinda alguna posibilidad de denegar expresamente tal consentimiento, a la vez que se hace mención al contraste con la información que almacena RENIEC, sin señalar su base de datos "BIOM".

218. Así entonces, la conducta de la administrada tampoco concretaría la obtención del consentimiento sin cumplir completamente con el requisito de información, ni mucho menos los del consentimiento libre y expreso; lo cual es necesario para legitimar el tratamiento de los patrones biométricos faciales para la validación de identidad, toda vez que las normas sectoriales, como ya se vio, no obligan a la administrada a emplear la verificación de ese tipo.

219. Por tanto, se advierte que la recopilación y almacenamiento de las imágenes de las personas y/o imágenes del documento de identidad de las mismas debidamente encriptadas obtenidas de la primera validación de identidad por biometría facial realizada a través de su canal de atención "libro de reclamaciones virtual", constituyen un tratamiento de datos personales sensibles (biométricos) sin el consentimiento informado, libre y expreso del titular de los datos personales, evidenciándose la responsabilidad de la administrada respecto a este segundo hecho imputado.

220. Por otra parte, la administrada señala que el análisis de la DPDP se centraría en el almacenamiento de datos biométricos faciales, pero no debería extenderse al almacenamiento de valores biométricos con fines de evidencia; es decir, cuando la operación autorizada mediante validación biométrica requiere que se almacene un registro de uso de biometría que sirva como sustento de que fue precisamente el cliente quien aprobó la operación.

221. Asimismo, estos datos evidencian la aprobación de una operación a nombre del usuario, de manera encriptada y segura, de tal modo que la información de sus usuarios estaría debidamente protegida y no sería posible que algún tercero pueda "ver" los datos ni "operar" con ellos ante una serie de números y letras que no tienen mayor valor individual, es decir, no podría identificar a una persona.

222. Sobre el particular, tal como ha sido señalado por la DPDP en los fundamentos 142 y 144, su pronunciamiento está delimitado a la recopilación y almacenamiento de los valores biométricos en la base de datos "BIOM" para la validación de identidad de los usuarios del "libro de reclamaciones virtual"; y, efectivamente, no se advierte que su pronunciamiento se haya extendido al almacenamiento de valores biométricos con fines de evidencia.

223. Por tales razones, **no corresponde amparar** este extremo de la apelación presentada por la administrada.

### V.3. Si la medida correctiva respecto a suprimir los patrones biométricos faciales almacenados en la base de datos "BIOM" cumple con el objetivo de corregir o revertir los efectos de la conducta infractora

224. La administrada, en su recurso de apelación, señala que la DPDP solo dedicaría un párrafo a motivar la decisión adoptada de imponer medidas correctivas; en el cual se hace una referencia a la supuesta necesidad de aplicar una medida correctiva al término del análisis del Hecho Imputado 1 (proporcionalidad de validar identidad a través de biometría), a pesar de que la medida correctiva versa esencialmente sobre el cese de almacenamiento y supresión de lo almacenado (Hecho Imputado 2).

225. Agrega que, no se realizaría un análisis sobre cómo estas medidas son efectivas, si son las más idóneas, ni se habría evaluado otras alternativas; tampoco se acreditaría su adecuación y proporcionalidad. Asimismo, durante el procedimiento se habría evaluado el mecanismo de validación de identidad de los usuarios del LRV (Libro de reclamaciones virtual) y el almacenamiento de estos valores biométricos en la base de datos "BIOM", sin embargo, al ordenar que se supriman todos los valores biométricos faciales de la base de datos excede el alcance de este procedimiento, dado que es una base de datos general.

226. Indica que los datos biométricos almacenados en esta base de datos no serían únicamente aquellos usados para fines de validación biométrica, sino también los que se guardan a modo de evidencia de la aprobación de operaciones; por lo que, la medida de cese de todo uso de biometría para validación de los usuarios en el LRV no tiene motivación y excede su alcance.

227. Respecto a la decisión del órgano decisor en imponer medidas correctivas en el presente procedimiento administrativo sancionador, debe tenerse presente que, conforme a lo dispuesto en el numeral 251.1 del artículo 251 del TUO de la LPAG, las sanciones administrativas que se impongan al administrado son compatibles con el dictado de medidas correctivas conducentes a ordenar la reposición o la reparación de la situación alterada por la infracción a su estado anterior, incluyendo la de los bienes afectados.

228. Para el dictado de tales medidas, la norma no exige que estas deban estar expresa y directamente motivadas en la resolución, sino que, estas deben estar previamente tipificadas, ser razonables y ajustarse a la intensidad, proporcionalidad y necesidades de los bienes jurídicos tutelados que se pretenden garantizar en cada supuesto concreto.

229. Cabe precisar que, conforme a lo establecido en el artículo 38 de la LPDP, sin perjuicio de las sanciones que en el marco de su competencia imponga la DPDP, esta puede ordenar la implementación de una o más medidas correctivas, con el objetivo de corregir o revertir los efectos que la conducta infractora hubiere ocasionado o evitar que ésta se produzca nuevamente.

230. Asimismo, el artículo 118 del Reglamento de la LPDP señala que se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los

efectos de las infracciones, caso contrario, dichas medidas no cumplirían con el examen de razonabilidad, intensidad, proporcionalidad y necesidad.

231. Ahora bien, la DPDP en el fundamento 82 de la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024 señaló como cuestiones en discusión los siguientes puntos respecto a la responsabilidad de la administrada:

> ***VIII. Cuestiones en discusión***
> *82. Para emitir pronunciamiento en el presente caso, se debe determinar lo siguiente:*
> *82.1 Si la administrada es responsable por:*
> - *Haber realizado el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, al recopilar imágenes del DNI y de la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica, los cuales no son adecuados, necesarios ni pertinentes para la finalidad de identificar plenamente al reclamante, incumpliendo lo dispuesto en los artículos 7 y numeral 3 del artículo 28 de la LPDP.*
>
> - *Haber realizado el tratamiento de los datos personales de quienes generan un reclamo, al almacenar el dato biométrico de la imagen facial en una base de datos propia, sin obtener válidamente el consentimiento de sus titulares, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento.*
> *(…)"*
>
> **Subrayado nuestro**

232. Por otra parte, en el artículo 3 de la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP, ha dispuesto las medidas correctivas siguientes:

> - ***Suprimir los patrones biométricos faciales almacenados en la base de datos "BIOM.***
> - *Cesar el almacenamiento de patrones biométricos obtenidos desde la imagen facial de los usuarios de su libro de reclamaciones virtual, así como el uso de estos para la validación de las identidades de estos.*
> - *Remitir documentación sustentatoria de la implementación de ambas medidas correctivas*.
> (…)"

233. Sobre el particular, se advierte que tanto la segunda y tercera medida correctiva se encuentran intrínsecamente relacionados a evitar que se sigan generando los efectos de las infracciones sancionadas en el presente procedimiento administrativo; y, por lo tanto, que la administrada acredite que ha cesado en la recopilación y almacenamiento de patrones biométricos obtenidos desde la imagen facial de los usuarios de su libro de reclamaciones virtual.

234. Por otra parte, respecto a la primera medida correctiva, este Despacho advierte que, efectivamente la DPDP no ha distinguido si su aplicación responde exclusivamente

a los patrones biométricos faciales obtenidos a partir del uso del libro de reclamaciones virtual y almacenados en la base de datos "BIOM", o también a los obtenidos a través del uso de otras aplicaciones mediante las cuales brinda servicios financieros ("Yape, seguros, Dinero al instante, Cocos y Lucas, Banca Móvil, tarjetas") tal y como ha manifestado la administrada durante el desarrollo de la segunda visita de inspección (Acta N.º 02-2023[80]).

235. En virtud que los aspectos señalados de forma precedente no han sido objeto de pronunciamiento en la resolución de primera instancia; y, considerando lo señalado por la DPDP en los fundamentos 82 y 142 de la resolución impugnada[81], corresponde circunscribir y delimitar la primera medida correctiva ordenada en la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024 al ámbito de discusión del presente procedimiento.

236. Por otra parte, la administrada ha indicado que la base de datos "BIOM" es también una base de datos general que también almacena valores biométricos con fines de evidencia; es decir, para determinar si fue precisamente el cliente quien aprobó la operación realizada al momento de brindar sus servicios.

237. Sobre este aspecto, si bien la medida correctiva ordenada tampoco alcanzaría a los valores biométricos con fines de evidencia que se hayan obtenido en las operaciones realizadas a través del uso de otras aplicaciones mediante las cuales brinda servicios financieros por no ser objeto del presente procedimiento, no corresponde realizar tal distinción en caso de aquellos valores biométricos obtenidos a través del LRV, pues el tratamiento realizado para la obtención de la citada información no supera el análisis de proporcionalidad, tal como se detalló en la primera cuestión controvertida.

238. Además, cabe precisar nuevamente que la administrada no ha acreditado ni reportado casos en los cuales los usuarios de su "libro de reclamaciones virtual" hayan cuestionado su identidad en el registro de algún reclamo presentado, por lo cual, conforme al principio de calidad[82], es responsable de evaluar la necesidad del almacenamiento de estos valores biométricos con fines de evidencia.

239. En consecuencia, corresponde declarar fundado dicho extremo de la apelación presentada y reformular la medida correctiva de la siguiente forma: "*Suprimir los patrones biométricos faciales almacenados en la base de datos BIOM obtenidos mediante la validación biométrica realizada a través de su libro de reclamaciones virtual; o, en el caso que no contar con la posibilidad técnica para realizar discriminadamente la supresión indicada, deberá acreditar tal situación.*"

---

80 Obrante en los folios 206 al 216.

81 ***Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024***
*(… )*
*142. En el presente caso, es necesario distinguir las dos acciones de tratamiento de los datos biométricos (patrones biométricos faciales) efectuadas a través del libro de reclamaciones virtual:*
- *Recopilación en tiempo real para la validación de identidad del usuario del libro de reclamaciones virtual.*
- *Recopilación y almacenamiento para la validación de identidad a futuro, en la base de datos "BIOM"*

82 **Ley N.° 29733, Ley de Protección de Datos Personales**
**Artículo 8. Principio de calidad**
Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.

**V.4 Si la DPDP ha realizado un correcto análisis de la multa**

240. La administrada señala que al Hecho Imputado No. 1, la Dirección habría establecido un monto base incorrecto, que debería ser de 5 UIT y no 22.5 UIT; por lo que, se aumentaría ilegalmente 17.5 UIT sin ninguna justificación legítima. Agrega que, aplicando la metodología utilizada, el monto base de 22.5 UIT se establecería incorrectamente en función de la variable relativa 3, pero en ninguna circunstancia se acreditaría la existencia de un daño. Señala que, si se quiere aplicar un monto base superior a 5 UIT, este debería ser máximo de 7.5 UIT. De igual manera, respecto al Hecho imputado No. 2 ocurriría lo mismo, aumentando ilegalmente 25 UIT

241. Por otro lado, indica que no se habría considerado como factores atenuantes la falta de perjuicio económico causado, que no es reincidente y que no existió intencionalidad al cometer la conducta infractora, tampoco sería posible sostener que exista un beneficio ilícito, lo cual debe ser tomado en cuenta por la autoridad al momento de determinar la multa, al igual que la DPDP habría reconocido que existen supuestos válidos de recopilación de datos biométricos faciales con fines de validación de identidad; que existen fines legítimos para este mecanismo de validación de identidad, es decir, no existe un beneficio ilícito; y, que no puede existir desproporcionalidad porque existe un mecanismo de identidad optativo para la mayoría de casos, por lo que la multa debería ser menor.

242. Señala que la DPDP concluyó que ambas conductas infractoras generaron un riesgo o daño a una persona y aplicó una agravante del 20% sobre la multa base; sin embargo, no se acreditaría riesgo o daño en ningún extremo de la resolución impugnada, y el argumento al aplicar la agravante sería idéntico en ambas imputaciones. Por otra parte, no resultaría válido que la sola conducta constituye la infracción y el hecho agravante. La Dirección concluyó que se habría generado un riesgo o daño.

**Respecto al hecho imputado 1: Realizar tratamiento de datos sensibles (datos biométricos) que resultan excesivos, no necesario, adecuados ni pertinentes para el uso de su libro de reclamaciones virtual**

243. Sobre el particular, en el en el fundamento 162[83] de la resolución impugnada, efectuó la graduación de la multa respecto a la infracción de tratamiento desproporcionado de los datos personales sensibles de quienes generan un reclamo a través del libro de reclamaciones virtual, de acuerdo con los siguiente:

Cuadro 2
Montos base de multas preestablecidas (Mb),
según variable absoluta y relativa de la infracción

| Gravedad de la infracción | Multa UIT | | Variable relativa y monto base (Mb) | | | | |
|---|---|---|---|---|---|---|---|
| | Min | Máx | 1 | 2 | 3 | 4 | 5 |
| Leve | 0.5 | 5 | 1.08 | 2.17 | 3.25 | | |
| Grave | 5 | 50 | 7.50 | 15.00 | 22.50 | 30.00 | 37.50 |
| Muy grave | 50 | 100 | | | 55.00 | 73.33 | 91.67 |

[83] Obrante a folios 466 al 469

Siendo que en el presente caso se ha acreditado la responsabilidad administrativa de la administrada conforme a la tipificación establecida en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP, corresponde el grado relativo "3" lo cual significa que la multa tendrá como Mb (Monto base) **22,50 UIT**, conforme al siguiente gráfico:

| N° | Infracciones graves | Grado relativo |
|---|---|---|
| 2.d | Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. | 3 |

244. En efecto, la DPDP, al momento de determinar la multa impuesta, empleó la Metodología para el cálculo de multas en materia de Protección de Datos Personales (en adelante, la **Metodología**), aprobada mediante Resolución Ministerial N.º 326-2020-JUS de 23 de diciembre de 2020, disponiendo en su artículo 3 que entraba en vigencia a los 30 días calendario contados a partir del día siguiente de su publicación, fecha en la cual fue de aplicación a todos los procedimientos sancionadores de la Autoridad Nacional de Protección de Datos Personales, incluyendo aquellos que se encuentren en trámite.

245. Dicha metodología, tiene como finalidad: (i) Brindar a los administrados pautas y criterios uniformes, predecibles y objetivos que le permitan tomar conocimiento de cómo se calculan las multas por la comisión de infracciones a la normativa de protección de datos personales y así garantizar el principio de predictibilidad o de confianza legítima previsto en la normativa administrativa actual; (ii) Asegurar que la labor de la Autoridad Nacional de Protección de Datos Personales se realice con arreglo al principio de razonabilidad que rige el procedimiento sancionador; (iii) Desincentivar la comisión de infracciones a la normativa de protección de datos personales permitiéndoles prever la cuantía de las multas a aplicar por violación de la normativa de protección de datos personales.

246. Ahora bien, la infracción por el hecho imputado N.º 1 es una infracción grave cuyo rango de multa corresponde de más de 5 a 50 UIT, conforme a lo dispuesto en el numeral 2 del artículo 139 de la LPDP; por calcular el valor exacto dentro de este rango de multa, la DPDP, bajo el principio de legalidad, aplicó la fórmula empleada por la Metodología para determinar la multa, la cual es el siguiente: M= Mb (Multa base) x F (Factor atenuante o agravante).

247. Ahora bien, para fijar la Multa Base (Mb) debe tenerse en cuenta la variable absoluta y relativa. La variable absoluta, es el nivel de gravedad de acuerdo a lo establecido en el artículo 132 del RLPDP[84] y la relativa en la que se han establecido valores vinculados a la afectación al bien jurídico protegido en la cual se determinó escalas del 1 al 5 dependiendo el nivel de infracción:

---

[84] En concordancia con el artículo 39 de la LPDP que señala:
***Artículo 39. Sanciones administrativas***
*En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:*
*1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).*
*2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).*
*3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT). (...)*

Para infracciones leves: Escala del 1 al 3
Para infracciones graves: Escala del 1 al 5
Para infracciones muy graves: Escala del 3 al 5

248. De ese modo el presente cuadro (citado en la resolución apelada) muestra las escalas mencionadas de acuerdo al nivel de infracción:

| Gravedad de la infracción | Multa UIT | | Variable relativa y monto base (Mb) | | | | |
|---|---|---|---|---|---|---|---|
| | Min | Máx | 1 | 2 | 3 | 4 | 5 |
| Leve | 0.5 | 5 | 1.08 | 2.17 | 3.25 | | |
| Grave | 5 | 50 | 7.50 | 15.00 | 22.50 | 30.00 | 37.50 |
| Muy grave | 50 | 100 | | | 55.00 | 73.33 | 91.67 |

249. La determinación de cada escala depende fundamentalmente a la afectación directa o indirecta del bien jurídico protegido y la vulneración de los principios rectores establecidos en la LPDP.

250. En materia de protección de datos personales, el bien jurídico protegido se refiere precisamente al control o disposición de los datos personales, siendo el tratamiento inadecuado de dichos datos personales lo que genera afectación directa o indirecta a la persona física, más aún cuando se trata de datos sensibles como el presente caso (datos biométricos).

251. Asimismo, para la asignación de las variables relativas, la Metodología ha considerado elementos vinculados a la afectación al bien jurídico protegido y la tipificación de las infracciones, como, por ejemplo: la categoría de los datos personales, el tipo específico de afectación del derecho, el número de banco de datos, el número de medidas de seguridad que no han sido implementadas, el cumplimiento de las características para un consentimiento válido, entre otros datos relevante.

252. Ahora bien, la Metodología determina la escala que corresponde aplicar en cada caso concreto, y en lo particular para la infracción grave establecida en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos"* **corresponde aplicar la escala 3**, conforme se aprecia a continuación:

| N° | Infracciones graves | Grado relativo |
|---|---|---|
| 2.d | Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. | 3 |

Cuadro 2
Montos base de multas preestablecidas (Mb),
según variable absoluta y relativa de la infracción

| Gravedad de la infracción | Multa UIT | | Variable relativa y monto base (Mb) | | | | |
|---|---|---|---|---|---|---|---|
| | Min | Máx | 1 | 2 | 3 | 4 | 5 |
| Leve | 0.5 | 5 | 1.08 | 2.17 | 3.25 | | |
| Grave | 5 | 50 | 7.50 | 15.00 | 22.50 | 30.00 | 37.50 |
| Muy grave | 50 | 100 | | | 55.00 | 73.33 | 91.67 |

Siendo que en el presente caso se ha acreditado la responsabilidad administrativa de la administrada conforme a la tipificación establecida en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP, corresponde el grado relativo "3" lo cual significa que la multa tendrá como Mb (Monto base) **22,50 UIT**, conforme al

253. Por lo que, según lo señalado en la Metodología, el monto base de multa a imponer por el hecho infractor establecido en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP es de 22.50 UIT. Este valor debe ser graduado de acuerdo a los factores agravantes y/o atenuantes comprobados en el caso en concreto. En ese sentido, queda claro que el monto base fue correctamente determinado por la DPDP de acuerdo a la normativa legal obligatoria y vigente sobre la materia.

254. Asimismo, este Despacho advierte del análisis de la resolución impugnada, que la DPDP evaluó cada uno de los criterios establecidos en el numeral 3 del artículo 248 del TUO de la LPAG, referidos a la graduación de la sanción; a saber: (i) el beneficio ilícito resultante por la comisión de las infracciones el cual es indeterminado por lo que se aplicó la fórmula de multa predeterminada, conforme a lo señalado de manera precedente; (ii) la probabilidad de detección de las infracciones, el cual es indeterminado por lo que se aplicó la fórmula de multa predeterminada; (iii) la gravedad del daño al interés público y/o bien jurídico protegido, el cual esta predeterminado en el valor de cada variable relativa, según la Metodología; (vi) las circunstancias de la comisión de la infracción.

255. Respecto al argumento referido a que la DPDP debió tomar en cuenta como factor atenuante la falta de perjuicio económico, intencionalidad y que la administrada no sería reincidente en el cálculo de la multa de ambas sanciones; corresponde señalar que, de acuerdo con la Metodología, tanto el "perjuicio económico", "intencionalidad" como la "no reincidencia" no son considerados como factores atenuantes que reduzcan el porcentaje del valor de la multa, pues estos conceptos cuentan con el valor de "0.00", en caso se determine que no se han configurado, y en el caso de su configuración agravan el valor del monto base de la multa al constituir circunstancias agravantes de la responsabilidad.

256. Finalmente, respecto a las circunstancias de la comisión de la infracción la administrada no reconoció responsabilidad alguna ni presentó medios de sustento de acciones de enmienda; por lo cual, no se aplicó ningún factor atenuante que reduzca la multa; por lo contrario, a través de la vulneración del principio de proporcionalidad por la recopilación innecesaria de datos personales de un gran número de usuarios clientes y no clientes la DPDP concluyó que la conducta de la administrada generó un riesgo de vulneración a los derechos de sus titulares y riesgo de pérdida del dominio sobre su información personal, riesgos que pueden conllevar afectaciones más graves a los derechos de las personas, cuando se trata de datos sensibles (datos biométricos), como el caso analizado; por lo cual, se incrementó el monto base de la multa en un 20%.

257. En consecuencia, los factores de graduación suman un total de 20%, el cual luego de aplicar la fórmula preestablecida para el cálculo de la multa, el resultado es de 27 UIT tal como lo determinó la DPDP y de acuerdo al detalle siguiente:

| **Componentes** | **Valor** |
|---|---|
| Monto base (Mb) | 22,50 UIT |
| Factor de agravantes y atenuantes (F) | 1.20 |
| **Valor de la multa** | **27 UIT** |

258. Por lo tanto, en la determinación de la multa impuesta se aplicó correctamente el valor relativo (el cual fue fijado según lo establecido en el Anexo de la Resolución Ministerial N.º 0326-2020-JUS de fecha 23 de diciembre de 2020 correspondiendo aplicar la escala 3 y por ende el monto de multa es de 22,50 UIT) así como el factor agravante, correspondiendo en este caso incrementar el 20% por el riesgo causado al bien jurídico protegido por la LPDP referido al inadecuado tratamiento de datos (recopilación de datos biométricos).

**Respecto al hecho imputado 2: Realizar tratamiento de los datos sensibles (datos biométricos) sin obtener el consentimiento válido de sus titulares**

259. Sobre el particular, en el fundamento 162[85] de la resolución impugnada, se efectuó la graduación de la multa respecto a la infracción de tratamiento de los datos personales de quienes generan un reclamo, al almacenar el dato biométrico de la imagen facial en una base de datos propia, sin obtener válidamente el consentimiento de sus titulares:

Cuadro 2
Montos base de multas preestablecidas (Mb),
según variable absoluta y relativa de la infracción

| Gravedad de la infracción | Multa UIT | | Variable relativa y monto base (Mb) | | | | |
|---|---|---|---|---|---|---|---|
| | Min | Máx | 1 | 2 | 3 | 4 | 5 |
| Leve | 0.5 | 5 | 1.08 | 2.17 | 3.25 | | |
| Grave | 5 | 50 | 7.50 | 15.00 | 22.50 | 30.00 | 37.50 |
| Muy grave | 50 | 100 | | | 55.00 | 73.33 | 91.67 |

Siendo que en el presente caso se ha acreditado la responsabilidad administrativa de la administrada conforme a la tipificación establecida en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP, con la circunstancia de tratarse del tratamiento de datos sensibles (datos biométricos), corresponde el grado relativo "4", lo cual significa que la multa tendrá como Mb (Monto base) **30 UIT**, conforme al siguiente gráfico:

| N° | Infracciones graves | Grado relativo |
|---|---|---|
| 2.b | Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley N° 29733 y su Reglamento.<br>Datos sensibles (salud y biométricos)<br>2.b.8. Consentimiento no cumple con la característica de ser libre. | 4 |

260. En efecto, al igual que el hecho imputado I, la DPDP al momento de determinar la multa impuesta por el hecho imputado II, empleó la Metodología para determinar el monto base de la multa, considerando que es una infracción grave, y en lo particular para la infracción grave establecida en el literal b) del numeral 2 del artículo 132 del

[85] Obrante a folios 469 al 472

Reglamento de la LPDP: *"Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley N.º 29733 y su Reglamento"*, en específico datos sensibles (salud y biométricos), **corresponde aplicar la escala 4,** es decir, el monto base de **30 UIT**.

261. Asimismo, este Despacho advierte del análisis de la resolución impugnada, que la DPDP evaluó cada uno de los criterios establecidos en el numeral 3 del artículo 248 del TUO de la LPAG, referidos a la graduación de la sanción; a saber: (i) el beneficio ilícito resultante por la comisión de las infracciones, (ii) la probabilidad de detección de las infracciones, (iii) la gravedad del daño al interés público y/o bien jurídico protegido; (iv) el perjuicio económico causado; (v) la reincidencia en la comisión de las infracciones; (vi) las circunstancias de la comisión de la infracción; y (vii) la existencia o no de intencionalidad en la conducta del infractor, aplicando el mismo razonamiento considerado en el hecho imputado I, situaciones que permitieron determinar el monto final de la multa para esta infracción grave.

262. A mayor abundamiento, respecto a las circunstancias de la comisión de la infracción la administrada no reconoció responsabilidad alguna ni presentó medios de sustento de acciones de enmienda; por lo cual, no se aplicó ningún factor atenuante que reduzca la multa; por lo contrario, la DPDP concluyó que, se habría configurado el factor agravante f3.2 porque la conducta *generó riesgo o daño a más de dos personas o grupo de personas*, debido a que la conducta infractora de la administrada implica "(…) *la vulneración de uno de los principios del tratamiento de datos personales, como es el principio de Consentimiento, el cual es la* ***principal garantía de la autodeterminación informativa*** *reconocida por el Tribunal Constitucional en la sentencia recaída en el expediente N° 4387-2011-PHD/TC y que adquiere mayor importancia al tratarse de datos biométricos por el mayor riesgo que conlleva su tratamiento de datos personales*."

263. Precisamente, este Despacho concuerda con el criterio de la DPDP y advierte que la conducta de la administrada obliga a sus usuarios a dar su consentimiento respecto al almacenamiento de su dato personal sensible relacionado a un dato biométrico para el reconocimiento facial, para recién poder generar su relamo en el libro de reclamaciones.

264. En consecuencia, los factores de graduación suman un total de 20%, el cual luego de aplicar la fórmula preestablecida para el cálculo de la multa, el resultado es de 36 UIT tal como lo determinó la DPDP y de acuerdo al detalle siguiente:

| **Componentes** | **Valor** |
|---|---|
| Monto base (Mb) | 30 UIT |
| Factor de agravantes y atenuantes (F) | 1.20 |
| **Valor de la multa** | **36 UIT** |

265. En este sentido, la DPDP valoró cada uno de los criterios legales establecidos por el numeral 3 del artículo 248 del TUO de la LPAG, en la LPDP y su Reglamento, a través de un análisis conciso sobre los fundamentos que motivaron su decisión en cada hecho imputado. Por tanto, no se establece contravención al principio de razonabilidad.

Por las consideraciones expuestas y de conformidad con lo dispuesto por la Ley N.º 29733, Ley de Protección de Datos Personales, su reglamento aprobado por el Decreto Supremo N.º 003-2013-JUS, el Texto Único Ordenado de la Ley N.º 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N.º 004-2019-JUS, el artículo 71, literal l, del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N.º 013-2017-JUS, y el Reglamento del Decreto Legislativo N.º 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses aprobado por Decreto Supremo N.º 019-2017-JUS;

**RESOLUCIÓN**

**PRIMERO.** **FUNDADO EN PARTE** el recurso de apelación presentado por **BANCO DE CRÉDITO DEL PERÚ S.A.**; y, en consecuencia:

- **REFORMULAR** el artículo 3 de la parte resolutiva de la Resolución Directoral N° 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024, reformulando la primera medida correctiva de la manera siguiente: "*Suprimir los patrones biométricos faciales almacenados en la base de datos BIOM obtenidos mediante la validación biométrica realizada a través de su libro de reclamaciones virtual; o, en el caso que no contar con la posibilidad técnica para realizar discriminadamente la supresión indicada, deberá acreditar tal situación"*.

- **CONFIRMAR** la Resolución Directoral N.º 2271-2024-JUS/DGTAIPD-DPDP de 01 de julio de 2024, en todos sus demás extremos.

**SEGUNDO.** **NOTIFICAR** la presente resolución, la cual agota la vía administrativa.

**TERCERO.** **DISPONER** la devolución del expediente a la Dirección de Protección de Datos Personales para los fines pertinentes.

**Regístrese y comuníquese.**

PERÚ
MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Firmado digitalmente por LUNA CERVANTES Eduardo Javier FAU 20131371617 soft

**Eduardo Luna Cervantes**
Director General
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales