VERSIÓN PÚBLICA

Resolución Directoral N° 3482-2024-JUS/DGTAIPD-DPDP

Expediente N°
140-2023-JUS/DGTAIPD-PAS

Lima, 9 de octubre de 2024

VISTOS:

El Informe N° 024-2024-JUS/DGTAIPD-DFI del 23 de febrero de 2024[1], emitido por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DFI), y demás documentos que obran en el respectivo expediente, y;

CONSIDERANDO:

I. Antecedentes

1. Mediante la denuncia ingresada el 26 de octubre de 2022, la señora [redacted] (en adelante, la denunciante) reportó que había recibido un mensaje vía Whatsapp en el que se le mostraba una consulta extraída de los sistemas de Entel Perú S.A. (en adelante, la administrada) a la que había accedido la emisora de dicho mensaje instantáneo, en el que se apreciaba sus nombres completos, DNI, grado de instrucción, fotografía, huella digital, entre otros que se consignan en las fichas Reniec[2].

2. Por medio de la Orden de Visita de Fiscalización N° 137-2022-JUS/DGTAIPD-DFI del 7 de noviembre de 2022[3], se dispuso la realización de una fiscalización en el establecimiento de la administrada, a fin de atender la denuncia reseñada y comprobar si se cumplía o no con las disposiciones de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP) y su reglamento, aprobado por el Decreto Supremo N° 003-2013-JUS (en adelante, Reglamento de la LPDP).

3. En dicha visita de fiscalización, efectuada el 10 de noviembre de 2022[4], se entregó al personal de la administrada una copia de la denuncia, para luego anotarse en el acta respectiva lo siguiente:

[1] Folios 261 al 280
[2] Folios 2 al 15
[3] Folio 16
[4] Folios 17 al 30

- La captura de pantalla que se adjuntó a la denuncia, conteniendo los datos de la denunciante, corresponde al sistema "Siebel", con el que se procesa la información de los clientes de la administrada.
- Sobre dicho sistema, se constató que no genera ni mantiene registros de interacción lógica de las búsquedas o visualizaciones de los datos de cliente, así como tampoco de las exportaciones o descargas de documentos.
- Se verificó en una de las computadoras empleadas para operar tal sistema, de titularidad de la empresa VP Mobile S.A.C., tiene acceso a cuentas de correo personal, redes sociales y aplicaciones de mensajería instantánea.
- El personal de la administrada señaló que cuentan con el programa "Splunk" que podría permitir identificar al trabajador responsable de filtrar la información de la denunciante, pero no arroja resultados inmediatos.

4. Mediante el escrito ingresado con la Hoja de Trámite N° 462250-2022MSC del 22 de noviembre de 2022[5], la administrada indicó que ya cuentan con los resultados del rastreo efectuado con la herramienta "Splunk", para lo cual solicitó que se realice una segunda visita de fiscalización.

5. A su vez, por medio del escrito ingresado con la Hoja de Trámite N° 467340-2022MSC del 24 de noviembre de 2022[6], la administrada remitió sus documentos de gestión de accesos, de gestión de privilegios y de verificación periódica de privilegios.

6. Por medio de la Carta N° 579-2022-JUS/DGTAIPD-DPDP del 29 de noviembre de 2022[7], se programó la visita de fiscalización solicitada por la administrada para el 12 de diciembre de 2022.

7. En el acta de fiscalización correspondiente a esta visita de fiscalización[8], se anotó lo siguiente:

   - Se realizó una videoconferencia pudiendo comprobar que diez usuarios tuvieron acceso a la información de la denunciante, de acuerdo con el reporte obtenido.
   - Según lo investigado por la administrada, nueve de los mencionados accesos fueron justificados, mientras que el restante, de la usuaria [redacted] (en adelante, la señora [redacted]), tuvo acceso desde una cuenta habilitada para un módulo del centro comercial "Plaza Lima Sur".
   - Se verificaron dichos registros de interacción lógica del sistema "Siebel", generados por la herramienta "Splunk".

8. Mediante la Carta N° 092-2023-JUS/DGTAIPD-DFI del 16 de febrero de 2023[9], se solicitó a la administrada indicar cómo concluyen que la señora [redacted] accedió a la información de la denunciante, el cargo que ocupa (adjuntar contrato de trabajo y cláusulas de confidencialidad) y precisar el tipo de credenciales (accesos) que tiene la usuaria al sistema.

[5] Folios 32 al 37
[6] Folios 39 al 98
[7] Folios 99 al 117
[8] Folios 118 al 126
[9] Folios 127 al 145

9. Por medio del escrito ingresado con la Hoja de Trámite N° 108882-2023MSC del 17 de marzo de 2023[10], la administrada explicó que la señora [redacted] estuvo asignada a una isla de atención de Plaza Lima Sur y que, de lo advertido en el sistema, dicho acceso no derivó en la creación de órdenes ni tampoco interacciones en distintos días; informando también que la mencionada es parte del personal de la empresa Manpower Incorporated, representada por Manpower Professional Services S.A.C. (en adelante, Manpower), con quien mantiene el contrato laboral respectivo.

10. En el Informe Técnico N° 035-2023-DFI-ORQR del 24 de abril de 2023[11], se señaló que la señora [redacted], a través de su usuario [redacted] y su rol "AS VENTA_AG_ISLAS" en el sistema "Siebel", accedió 2 veces el 4 de septiembre del 2022, visualizando los datos personales de la denunciante.

11. En el Informe de Fiscalización N° 137-2023-JUS/DGTAIPD-DFI-EHCC del 17 de mayo de 2023[12], el Analista Legal de Fiscalización de la DFI, determina con carácter preliminar las circunstancias que justifican la instauración de un procedimiento administrativo sancionador contra la administrada por el incumplimiento de lo dispuesto en la LPDP, que configuraría la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del reglamento de dicha ley.

12. Dicho informe fue notificado a la administrada mediante las Cédulas de Notificación N° 455 y 456-JUS/DGTAIPD-DFI[13].

13. Mediante la Resolución Directoral N° 263-2023-JUS/DGTAIPD-DFI del 28 de noviembre de 2023[14], la DFI dispuso el inicio del procedimiento administrativo sancionador a la administrada por no haber garantizado la confidencialidad de los datos personales de la denunciante (nombre, número de DNI, fecha de nacimiento y número de teléfono), al haberse filtrado estos a una tercera persona, incumpliendo con lo dispuesto en el artículo 17 de la LPDP; con lo que se configuraría la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del reglamento de dicha ley.

14. Dicha resolución fue notificada a la administrada mediante la Cédula de Notificación N° 1039-2023-JUS/DGTAIPD-DFI el 29 de noviembre de 2023[15].

15. Por medio del escrito ingresado con el código N° 598757-2023MSC del 22 de diciembre de 2023[16], la administrada presentó los siguientes descargos:

    - A pesar de que las capturas de pantalla presentadas por la denunciante demuestren que el medio empleado para cometer la infracción fue el sistema "Siebel", también quedó claro que su usuaria, la señora [redacted] mantuvo su

[10] Folios 171 al 176
[11] Folios 177 al 186
[12] Folios 187 al 198
[13] Folios 199 al 219
[14] Folios 220 al 234
[15] Folios 235 al 251
[16] Folios 253 al 260

vínculo laboral con Manpower, con quien mantenían el vínculo de encargo de tratamiento de datos personales.
- Demostró contar con procedimientos documentados respecto a la gestión de privilegios y verificación periódica de privilegios, concernientes a su sistema "Siebel", así como el control de los registros de interacción lógica que permitieron la trazabilidad del mencionado acceso.
- En tal sentido, la acción infractora no le puede ser imputada la inobservancia del deber de confidencialidad, toda vez que se comprobó haber adoptado todas las medidas de seguridad necesarias; no obstante ello, están adoptando acciones para evitar que dicha infracción se vuelva a cometer.

16. Mediante el Informe N° 024-2024-JUS/DGTAIPD-DFI, la DFI remitió a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DPDP) los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando imponer la multa de veinticuatro coma setenta y cinco unidades impositivas tributarias (33,75 UIT) por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP.

17. Con la Resolución Directoral N° 045-2024-JUS/DGTAIPD-DFI del 26 de febrero de 2024[17], la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

18. Dichos documentos fueron notificados a la administrada mediante la Cédula de Notificación N° 184-2024-JUS/DGTAIPD-DFI[18].

19. Mediante el escrito presentado con la Hoja de Trámite N° 127035-2024MSC del 20 de marzo de 2024[19], la administrada presentó los siguientes alegatos:

- Existen diferencias esenciales entre el deber de contar con medidas de seguridad y el deber de confidencialidad, pese a su estrecha relación que subyace del artículo 32 del Reglamento de la LPDP; pues aquella obligación de contar con las medidas de seguridad hace referencia a contar con herramientas para preservar la información personal, mientras que, la obligación de confidencialidad hace alusión a la reserva de la información personal por parte del titular del banco de datos o del encargado de tratamiento.
- La misma DFI confirmó que contaban con las medidas de seguridad suficientes como para preservar los datos personales de sus clientes.
- Por ello, resulta carente de lógica que se les impute una infracción que se fundamenta justamente en la falta o deficiencia en las medidas de seguridad.
- La inobservancia fue cometida directamente por la señora [redacted], excolaboradora de Manpower.
- El contrato en el que se basa el encargo por parte de Manpower, se estipuló que esta debía tratar los datos personales para fines exclusivamente involucrados con el contrato, no debiendo transferirlos a terceros, de lo que

[17] Folios 281 al 284
[18] Folios 285 al 302
[19] Folios 311 al 388

subyace la obligación de la señora [redacted] de guardar confidencialidad de la información que recibía.
- Debe entenderse que no podía controlarse la conducta directa efectuada por la señora [redacted], la cual se pudo detectar a través de su plataforma "Splunk", quien además no era subordinada suya.

20. Mediante la Resolución Directoral N° 2721-2024-JUS/DGTAIPD-DFI del 9 de agosto de 2024[20], se dispuso la ampliación del plazo de caducidad por tres meses, desde el 28 de agosto de 2024 y se solicitó la siguiente información:

- Documentación, comunicaciones y sustentos de las medidas de control que haya adoptado respecto de la conducta de la señora [redacted] como usuaria del sistema "Siebel" relacionada con su acceso a los datos personales de la denunciante registrados en dicho sistema.
- Documentación de la resolución del contrato con Manpower, de ser el caso; u otra acción orientada hacia esta empresa respecto del hecho materia de imputación.

21. Por medio del escrito ingresado con la Hoja de Trámite N° 430061-2024MSC del 29 de agosto de 2024[21], la administrada dio respuesta al requerimiento efectuado, informando lo siguiente:

- La señora [redacted] cesó labores con Manpower el día 31 de diciembre de 2022, fecha anterior a la imputación de cargos, siendo que no se le renovó su contrato temporal, siendo dado de baja su usuario en el sistema "Siebel".
- No han resuelto el contrato con Manpower, ni realizado alguna acción legal contra esta, toda vez que el presente procedimiento todavía no ha concluido.

II. Competencia

22. De conformidad con el artículo 74 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, la DPDP es la unidad orgánica competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la DFI.

23. En tal sentido, la autoridad que debe conocer el presente procedimiento sancionador, a fin de emitir resolución en primera instancia, es la Directora de Protección de Datos Personales.

III. Normas concernientes a la responsabilidad de la administrada

24. Para la determinación de la responsabilidad de la administrada respecto de una infracción, se deberá tomar en cuenta lo establecido en el artículo 257 de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS (en adelante, la LPAG), en su calidad de norma común

[20] Folios 389 al 391
[21] Folios 405 al 411

para los procedimientos administrativos, conjuntamente con lo establecido en el Reglamento de la LPDP.

25. En tal sentido, se atiende al hecho de que el literal f) del numeral 1 de dicho artículo de la LPAG, establece como una causal eximente de la responsabilidad por infracciones, la subsanación del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos y a iniciativa voluntaria por parte de la administrada[22], sin provenir del mandato de la autoridad a través de algún documento mediante el cual se solicite subsanar el acto calificable como infracción, como señala adecuadamente Morón[23].

26. Por su parte, en lo que atañe a las atenuantes de la responsabilidad administrativa, se debe prestar atención a lo dispuesto en el numeral 2 del mismo artículo de la LPAG[24], en virtud del cual la aplicación de aquellas dependerá del reconocimiento expreso de la infracción, conjuntamente con los factores establecidos en la norma especial, el artículo 126 del Reglamento de la LPDP: El reconocimiento espontáneo, acompañado de acciones para su enmienda y colaboración con las acciones de la autoridad, factores que, de acuerdo con lo oportuno del reconocimiento y la efectividad de la enmienda, pueden conllevar la reducción motivada de la sanción hasta por debajo del rango previsto en la LPDP[25].

27. Por supuesto, la efectividad de los actos de enmienda mencionados, de acuerdo con el objetivo de las normas de protección de datos personales y del procedimiento administrativo, dependerá de su capacidad de diluir la trascendencia y los efectos antijurídicos de la conducta infractora, reparando la situación al punto de acercarla lo más posible al estado anterior al hecho infractor.

IV. Primera cuestión previa: Sobre la vinculación entre el Informe de Instrucción y el pronunciamiento de esta dirección

28. El artículo 254 de la LPAG establece como carácter fundamental del procedimiento administrativo sancionador, la separación entre la autoridad instructora y la autoridad sancionadora o resolutora:

---

[22] **Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**
1.- Constituyen condiciones eximentes de la responsabilidad por infracciones las siguientes:
(…)
f) La subsanación voluntaria por parte del posible sancionado del acto u omisión imputado como constitutivo de infracción administrativa, con anterioridad a la notificación de la imputación de cargos a que se refiere el inciso 3) del artículo 255.

[23] MORÓN URBINA, Juan Carlos: "Comentarios a la Ley del Procedimiento Administrativo General". Décimo quinta edición. Lima, Gaceta Jurídica, 2020, tomo II, p. 522.

[24] **Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**
(…)
2.- Constituyen condiciones atenuantes de la responsabilidad por infracciones las siguientes:
a) Si iniciado un procedimiento administrativo sancionador el infractor reconoce su responsabilidad de forma expresa y por escrito.
En los casos en que la sanción aplicable sea una multa esta se reduce hasta un monto no menor de la mitad de su importe.
b) Otros que se establezcan por norma especial.

[25] **Artículo 126.- Atenuantes.**
La colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes. Atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda, la atenuación permitirá incluso la reducción motivada de la sanción por debajo del rango previsto en la Ley.

> ***"Artículo 254.- Caracteres del procedimiento sancionador***
> *254.1 Para el ejercicio de la potestad sancionadora se requiere obligatoriamente haber seguido el procedimiento legal o reglamentariamente establecido caracterizado por:*
> *1. Diferenciar en su estructura entre la autoridad que conduce la fase instructora y la que decide la aplicación de la sanción.*
> *(…)"*

29. Por su parte, el artículo 255 de dicha ley establece lo siguiente:

> ***"Artículo 255.- Procedimiento sancionador***
> *Las entidades en el ejercicio de su potestad sancionadora se ciñen a las siguientes disposiciones:*
> *(…)*
> *5. Concluida, de ser el caso, la recolección de pruebas, la autoridad instructora del procedimiento concluye determinando la existencia de una infracción y, por ende, la imposición de una sanción; o la no existencia de infracción. La autoridad instructora formula un informe final de instrucción en el que se determina, de manera motivada, las conductas que se consideren probadas constitutivas de infracción, la norma que prevé la imposición de sanción; y, la sanción propuesta o la declaración de no existencia de infracción, según corresponda.*
> *Recibido el informe final, el órgano competente para decidir la aplicación de la sanción puede disponer la realización de actuaciones complementarias, siempre que las considere indispensables para resolver el procedimiento. El informe final de instrucción debe ser notificado al administrado para que formule sus descargos en un plazo no menor de cinco (5) días hábiles."*

30. De los artículos transcritos, se desprende que la separación de las dos autoridades, así como la previsión de ejercicio de actuaciones por parte de la autoridad sancionadora o resolutora, situaciones que implican la autonomía de criterio de cada una de ellas.

31. En tal sentido, la autoridad sancionadora o resolutora puede hacer suyos todos los argumentos, conclusiones y recomendaciones expuestos por la autoridad instructora, así como puede efectuar una distinta evaluación de los hechos comprobados o inclusive, cuestionar estos hechos o evaluar situaciones que si bien fueron tomadas en cuenta al momento de efectuar la imputación, no se evaluaron de la misma manera al finalizar la instrucción.

32. Por tal motivo, la resolución que emita una autoridad sancionadora o resolutora, puede apartarse de las recomendaciones del informe final de instrucción o incluso cuestionar los hechos expuestos y su valoración, haciendo una evaluación diferente, teniendo en cuenta la su naturaleza no vinculante de dicho informe, y sin que ello conlleve una vulneración de la predictibilidad o de la expectativa legítima del administrado, la cual no encuentra asidero en la normativa referida al procedimiento administrativo.

33. Por supuesto, la divergencia de criterios mencionada, no puede implicar vulneraciones al debido procedimiento, como el impedir el derecho de defensa de

los administrados, ni ampliar o variar los hechos imputados y su valoración como presuntas infracciones.

V. Segunda cuestión previa: Sobre la naturaleza del encargo de tratamiento de datos personales

34. En sus comunicaciones, la administrada indicó que la señora [redacted], que hizo las consultas de los datos personales de la denunciante y pudo haberlos remitido a un tercero, era parte de la planilla de Manpower, empresa que cumplía el rol de encargado del tratamiento de datos personales de sus clientes, para lo cual su personal tenía acceso al sistema "Siebel" y se había delegado a ella un usuario con cargo y rango "Promotor".

35. Como sustento de tales hechos, la administrada presenta copia del contrato entre dicha trabajadora y Manpower, en el que aquella se obligaba a guardar confidencialidad respecto de la información a la que haya podido acceder:

> *"DÉCIMA.- EL (LA) TRABAJADOR(A) se compromete a guardar estricto secreto de toda la información que llegue a su conocimiento, relacionada con los negocios de EL EMPLEADOR y/o sus clientes y asociados, incluyendo bases de datos, información comercial y/o empresarial, datos de clientes y otros que a criterio de EL EMPLEADOR se consideren como "Información Sensible". Esta obligación subsistirá incluso después de terminada la relación laboral con EL EMPLEADOR. En caso se compruebe el incumplimiento de este compromiso por parte de EL (LA) TRABAJADOR/(A), EL EMPLEADOR podrá accionar judicialmente su cumplimiento o resarcimiento por daños, de acuerdo a Ley."*

36. En la presente resolución directoral, en lo específicamente concerniente a las definiciones del rol del "encargado" y de la composición del "encargo", corresponde a esta Dirección tomar en cuenta la definición que la LPDP tiene del tratamiento de datos personales:

> *"**Artículo 2. Definiciones***
> *Para todos los efectos de la presente Ley, se entiende por:*
> (…)
> ***19. Tratamiento de datos personales.** Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales."*

37. De lo citado, se desprende que el "tratamiento" es una nomenclatura genérica, aplicable a cualquier acción o procedimiento, transitivo o no, realizado sobre un objeto, que es el dato o los datos personales.

38. A su vez, es pertinente tomar en cuenta las siguientes definiciones que contienen la LPDP y su reglamento, respectivamente:

> *"**Artículo 2. Definiciones***
> *Para todos los efectos de la presente Ley, se entiende por:*
> (…)
> ***7. Encargado de tratamiento de datos personales.** Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.*
>
> ***8. Encargo de tratamiento.** Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales.*
> *(…)*
> ***17. Titular del banco de datos personales.** Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad."*
>
> ***"Artículo 2.- Definiciones.***
> *Para los efectos de la aplicación del presente reglamento, sin perjuicio de las definiciones contenidas en la Ley, complementariamente, se entiende las siguientes definiciones:*
> *(…)*
> ***10. Encargado del tratamiento:** Es quien realiza el tratamiento de los datos personales, pudiendo ser el propio titular del banco de datos personales o el encargado del banco de datos personales u otra persona por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales.*
> *(…)*
> ***14. Responsable del tratamiento:** Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.*
>
> ***15. Tercero:** Es toda persona natural, persona jurídica de derecho privado o entidad pública, distinta del titular de datos personales, del titular o encargado del banco de datos personales y del responsable del tratamiento, incluyendo a quienes tratan los datos bajo autoridad directa de aquellos."*

39. Si bien se habla en las normas citadas de una "entrega" hacia la persona que ejerce el rol de encargado, estos conceptos hacen referencia concretamente a acciones de tratamiento que se encargan según lo que el titular del banco de datos personales y/o responsable del tratamiento estipule en el contrato del servicio, incluso en casos donde no exista un banco de datos personales; vale decir, se

encomiendan acciones a desarrollar de acuerdo con lo que disponga el responsable del tratamiento.

40. Asimismo, se evidencia una pluralidad de niveles de participación en el tratamiento, siendo el concepto más amplio el del responsable del tratamiento, definido llanamente como "quien decide sobre el tratamiento de datos personales", que a su vez comprende en sí al concepto de titular de los bancos de datos personales, que es una persona o entidad que decide sobre las actividades de tratamiento y la estructura, finalidad y preservación de los datos personales incorporados en un conjunto estructurado, el banco de datos personales.

41. En ambos casos, está presente el poder de decisión que tienen sobre los datos personales, estructurados o no en un banco de datos personales, que se ejerce a través de la elección de los datos personales que serán objeto de tratamiento (en el caso de los bancos de datos personales, en su contenido y estructura), de las actividades de tratamiento de datos personales a realizar, de quiénes intervienen en tales actividades y, principalmente, de la finalidad a alcanzar, relacionada con el interés del responsable que se busca atender con dicho tratamiento.

42. En tal sentido, debe entenderse que dicho interés se satisface a través de medios y recursos (acciones, actividades de tratamiento, recursos humanos, bienes empleados, datos personales objeto de tratamiento, bases de datos personales, entre otros), provistos o desarrollados por otras empresas, cuya contratación le resulta más provechosa que realizar la actividad encargada por su propia cuenta.

43. Sobre la finalidad y el correcto empleo de estos medios contratados, a fin de que sean compatibles con dicha finalidad, el responsable decide y ejerce el control supremo, ya que goza de los beneficios que surta la actividad que conlleva el tratamiento de datos personales.

44. Al estar orientados hacia la satisfacción del responsable del tratamiento, tales medios se emplean en favor de este y su interés, siendo estos cualesquiera con los que desarrollen alguna actividad de tratamiento de datos personales, los mismo que pueden ser proporcionados por el mismo responsable, por el encargado o por algún tercero subcontratado, según cada caso.

45. Al atenderse en un proceso comercial como el del caso, el interés del responsable del tratamiento, surge la obligación a su cargo de garantizar un lícito y adecuado tratamiento de datos personales a lo largo del mismo, a fin de que la satisfacción de su interés mantenga compatibilidad con el ordenamiento jurídico y con los derechos de las personas, los titulares de los datos personales.

46. Dichas circunstancias obligan al encargado y a los subcontratados por este, a ceñir su desempeño a lo que establezca el responsable y a los resultados que este requiera, situación que conlleva dos factores concernientes al responsable:

    - Llevar a cabo con diligencia, las acciones de control necesarias para que el encargo se cumpla de acuerdo con lo pactado, en protección de sus intereses, sin efectos ilícitos en la prestación.

- En lo relativo a evitar los efectos negativos señalados, la obligación de controlar y supervisar el cumplimiento de disposiciones legales y reglamentarias y/o evitar que algún daño ilícito se produzca como consecuencia de un desarrollo negligente de las actividades que satisfacen su interés, desarrolladas por los encargados y terceros subcontratados.

47. El control ejercido sobre la actuación del encargado se traduce en la instrucción sobre los objetivos y modalidades de tratamiento, provisión de medios e instrucciones necesarias (según se tenga previsto en los contratos) para el personal del encargado, así como en la implementación de medios de supervisión de su conducta y desarrollo de dicho tratamiento.

48. Asimismo, al estar obligado a ejercer dicho control, el responsable debe ser capaz de demostrar en cualquier momento que lo efectúa de manera efectiva, durante la vigencia del contrato de encargo, durante el período en el que se ejecutan las prestaciones respectivas, así como después de dicha vigencia y de haberse completado la mencionada ejecución, cuando haya efectos remanentes del tratamiento de datos personales objeto de encargo; situación que se aplica también a la subcontratación, sobre la conducta del tercero subcontratado.

49. Entonces, cuando en un contrato de encargo de tratamiento o en la subcontratación derivada de este, se configure la comisión de una infracción y/o de cualquier hecho que implique un daño efectivo o potencial, debe tomarse en cuenta respecto de la responsabilidad, lo siguiente:

- El principal obligado para preservar la licitud del tratamiento de los datos personales es el responsable de este, al ser necesario dicho tratamiento para satisfacer su interés, por lo que debe ejercer diligentemente el control del mismo y ser capaz de demostrar dicho control en todo momento.
- En caso de que el responsable no haya ejercido diligentemente su rol de control sobre el encargo de dicho tratamiento y sobre el objeto de la subcontratación en tal encargo y/o no demuestre tal actuación, deberá responder por la infracción.
- Sin perjuicio de lo anterior, la responsabilidad del encargado por el incumplimiento o el tratamiento ilícito, subsistirá respecto de aquellas acciones que implican una conducta distinta a la que se estipuló para el encargo y a las instruidas por el responsable durante la prestación del servicio.
- Igualmente, la responsabilidad del tercero subcontratado existe, en tanto haya efectuado acciones distintas a lo estipulado en el contrato suscrito con el encargado o a lo que este le haya instruido.
- En caso de que el responsable haya ejercido de forma diligente el control de las acciones de tratamiento de datos personales objeto de encargo y de sucesiva subcontratación, y sustente adecuadamente el haber ejercitado dicho control, no le serán imputables los hechos ilícitos o dañosos.
- En ese mismo caso, al detectarse un hecho infractor que haya sobrepasado el diligente control del responsable, el encargado o el tercero subcontratado serán responsables.

50. Ahora bien, la capacidad de ejercicio del control por parte del responsable del tratamiento de los datos personales, así como la de demostrar tal control, no puede evaluarse de la misma manera para todas las empresas ni para todos los rubros o actividades del mercado; debiendo obedecerse a las particularidades que se presentan en cada caso concreto.

51. Así, la exigencia de control y demostración de su ejercicio, será alta cuando el encargo se vincule con una actividad de alta extensión en el mercado o en un numeroso público objetivo, como los casos de productos de consumo masivo o la prestación de servicios de salud y educación, debiendo ser menor en los casos de actividades más reducidas o especializadas; también se evaluará tal factor en función a la mayor o menor especialización o alcances para aplicar la normativa de protección de datos personales, la posición de dominio, presencia, tamaño o reconocimiento de la presencia de la responsable en su mercado relevante.

52. De lo expuesto, se desprende que quien determina y controla las finalidades y modalidades de las actividades de tratamiento de datos personales, dirigidas a la satisfacción de su interés, es responsable por dicho tratamiento, debiendo ejercer el control sobre tales actividades encargadas de forma diligente y poder demostrar siempre tal ejercicio, asumiendo un rol proactivo para preservar los derechos de los titulares de los datos personales.

53. Por ello, para un mejor examen de la existencia de infracción y responsabilidades, es necesario examinar factores como el interés de la administrada, así como el ejercicio del control sobre las actividades dirigidas a satisfacerlo, por parte del o de los encargados, así como del o de los terceros subcontratados.

VI. Tercera cuestión previa: Acerca de la huella dactilar y su carácter de dato sensible biométrico

54. El análisis de esta cuestión previa debe partir de la definición de dato sensible, a nivel legal (LPDP), transcrita a continuación:

> *"**Artículo 2. Definiciones***
> *Para todos los efectos de la presente Ley, se entiende por:*
> *(…)*
> ***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."*

55. En la legislación nacional, se comprende dentro de los datos sensibles los datos biométricos cuyo tratamiento permita la identificación del titular, como en la práctica puede apreciarse que sucede con la huella dactilar

56. A nivel internacional, es relevante la definición prevista en el numeral 14 del artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que

respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, que se transcribe a continuación:

> ***"Artículo 4***
> *Definiciones*
> *A efectos del presente Reglamento se entenderá por:*
> *(…)*
> *14) «datos biométricos»: 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;"*

57. Por su parte, la Autoridad Nacional de Protección de Datos Personales, a fin de esclarecer el concepto del dato biométrico y la razón de su calificación como dato sensible, desarrolló en la Opinión Consultiva N° 032-2021-JUS/DGTAIPD lo siguiente:

> *"9. Cabe precisar que 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."*

58. De acuerdo con lo reseñado, se puede entender que el tratamiento técnico que constituiría el carácter de "dato biométrico", se centra en la etapa de obtención u extracción (toma de la huella dactilar o de la imagen del iris), pudiendo en otras acciones de tratamiento posteriores (almacenamiento, difusión, transferencia) prescindirse de aquel tipo de tratamiento sobre el soporte que contenga el dato.

59. Ahora bien, dada la cualidad de identificar por sí mismo a su titular (por medios técnicos u otros distintos a los empleados en su obtención), es que el uso no adecuado de la huella dactilar implica riesgos como los relativos a la suplantación de identidad, la cual puede conllevar a actividades delictivas, como el robo o hurto de bienes a los que se pueda acceder gracias a tal suplantación, como sucede con el *"SIM Swapping"*, consistente en el uso de una tarjeta SIM de un teléfono móvil asignada a la persona cuya identidad se suplanta.

60. Tales situaciones demuestran los daños a los que se expone al titular de la huella dactilar, cuando este dato personal que una vez obtenido puede identificarlo unívocamente, es expuesto o se sujeta a un tratamiento que no guarda las garantías necesarias para evitar su acceso o difusión no autorizada.

VII. Cuestiones en discusión

61. Para emitir pronunciamiento en el presente caso, se debe determinar lo siguiente:

- Si la administrada es responsable por no haber garantizado la confidencialidad de los datos personales de la denunciante (nombre, número de DNI, fecha de

nacimiento y número de teléfono), al haberse filtrado estos a una tercera persona, incumpliendo con lo dispuesto en el artículo 17 de la LPDP.

- En el supuesto de resultar responsable, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, según lo previsto en el numeral 1 del artículo 257 de la LPAG, o las atenuantes, de acuerdo con lo dispuesto en el artículo 126 del reglamento de la LPDP, en consonancia con el numeral 2 del artículo 257 de la LPAG.
- Determinar la multa que corresponde imponer, tomando los criterios de graduación contemplados en el numeral 3) del artículo 248 de la LPAG.

VI. Análisis de las cuestiones en discusión

Sobre el incumplimiento del deber de confidencialidad sobre los datos personales

62. La Constitución Política del Perú, establece en el artículo 2, numeral 6, que toda persona tiene derecho "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar", es decir toda persona tiene derecho a la autodeterminación informativa, y por lo tanto a la protección de sus datos personales.

63. El Tribunal Constitucional, máximo intérprete de la Constitución Política del Perú, ha definido el derecho a la autodeterminación informativa en la sentencia recaída en el Expediente N° 04739-2007-PHD/TC, de la siguiente forma:

> *"el derecho a la autodeterminación informativa 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. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal. Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen (…). En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos"*

64. Por su parte, la LPDP tiene como objeto, conforme con su artículo 1, *"garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen".*

65. Con la finalidad de hacer efectivo tal derecho de forma permanente durante las operaciones del tratamiento, se tienen en el Título II de dicha ley, los deberes que toda persona, natural o jurídica, a los que debe sujetarse el accionar del responsable del tratamiento de datos personales, a fin de preservar el derecho a la autodeterminación informativa de los titulares de tal información.

66. Entre tales deberes, se recoge la confidencialidad sobre los datos personales, en el artículo 17 de la misma ley, transcrita a continuación:

> ***"Artículo 17. Confidencialidad de datos personales***
> *El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.*
> *El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional."*

67. A través de dicho artículo, se exige a cualquiera de los intervinientes en los procesos de tratamiento de datos personales (responsables, titulares de los bancos de datos personales, encargados o cualquier otra persona partícipe) la preservación de la confidencialidad respecto de los datos personales que estén bajo su control o sobre los que tenga conocimiento.

68. Dicha situación implica el deber de evitar el acceso a los datos personales por parte de quienes no estén autorizados para ello, así como el deber de no transmitir o compartir tal información personal con personas no autorizadas; vale decir, un deber de tomar todas las medidas necesarias para prevenir el acceso no autorizado mencionado y una faceta negativa, consistente en no compartir o transmitir los datos personales.

69. Entonces, quien realiza el tratamiento de datos personales debe dar prioridad a la privacidad de los datos personales, evitando la intervención de personas cuyas funciones no se vinculen a las finalidades del tratamiento o cuyas funciones específicas no requieran de tal tratamiento; así como las salidas de los datos personales de tal entorno que impliquen riesgo de acceso no autorizado (muchas veces, desconocido por la responsable del tratamiento), lo cual, a su vez, conlleva a la pérdida del dominio sobre tales datos que ejercía su titular.

70. En el caso de las entidades que realizan el tratamiento de datos personales, el incumplimiento del mencionado deber se configura en los siguientes supuestos:

- El acceso a los datos personales por parte de personas no autorizadas o no legitimadas, sean terceros externos a la organización o de personas de la misma que no cumplen algún cargo o función que haga necesario tal acceso.

- Cualquier forma de salida de los datos personales hacia personas que no se encuentran autorizadas o legitimadas para conocerlos o darles tratamiento, aun cuando no se haya configurado un acceso no autorizado al interior de la entidad.
- Una omisión relevante al interior de la organización, que permita que los datos personales bajo su responsabilidad o custodia, sean accesibles para terceros no autorizados.

71. De lo expuesto, se desprende que el deber de confidencialidad requiere que la organización, empresa o persona que realice el tratamiento, garantice tomar todas las medidas técnicas, organizativas y legales, asegurándose de evitar los accesos no autorizados a los datos personales, a fin de que se restrinja que terceros que no tengan legitimación alguna puedan efectuar su tratamiento.

72. Por supuesto, en consonancia de la prevalencia de la voluntad del titular de los datos personales, la obligación de evitar tales accesos se dispensa cuando este otorga el consentimiento válido para ello, emitido luego de evaluar los riesgos para su privacidad que entrañaría una eventual exposición, transferencia o acceso a sus datos personales por parte de un tercero.

73. De otro lado, para esclarecer los hechos específicos del presente caso, es necesario tomar en cuenta las definiciones de datos sensibles de la LPDP, de acuerdo con lo desarrollado en la tercera cuestión previa de esta resolución directoral.

74. La denunciante detalló haber recibido un mensaje de Whatsapp que contenía una consulta de fichas Reniec, las cuales habrían sido obtenidas de los sistemas de la administrada; verificándose en las visitas de fiscalización que hubo acceso a tales datos por parte de diez usuarios, siendo solo el de la señora [redacted] injustificado y realizado desde un módulo de venta.

75. En el Informe de Fiscalización N° 137-2023-JUS/DGTAIPD-DFI-EHCC, se desarrolló al respecto lo siguiente:

> *"29. Sobre el particular, es necesario hacer referencia a lo manifestado por ENTEL PERÚ S.A. en el Acta de Fiscalización n.° 02-2023 (f. 119) y en su escrito ingresado el 17 de marzo de 2023 con Hoja de Trámite n.° 000108882-2023MSC (f. 170 a 176), a través del cual, señaló que de la investigación que efectuaron se verificó que diez (10) usuarios hicieron consultas en el sistema SIEBEL sobre los datos personales de la denunciante, comprobando que solo la señora (…) accedió a la mencionada información sin contar con una justificación válida o motivo aparente.*
> *30. También se ha verificado que, el número de teléfono del cual se envía la ficha de datos personales de la denunciante extraída del sistema de la administrada, a través de la aplicación móvil WhatsApp es el +52* [redacted] *el mismo que por la cantidad de dígitos que contiene y el código +52, se ha determinado que corresponde a un número internacional correspondiente al país de México; por tanto, los datos personales de la denunciante incluso han sido enviados a un tercero que reside en el extranjero.*

> *31. Al respecto, debe tenerse en cuenta que una de las obligaciones que tienen los responsables y encargados del tratamiento de datos personales, es garantizar la confidencialidad de la información que poseen; no obstante, como lo ha mencionado la denunciante, su información le ha sido proporcionada a un tercero.*
> *32. Ahora bien, el deber de confidencialidad supone, el resguardo, la protección de los datos personales, para que estos no puedan ser accedidos por terceros que no tengan vinculación directa en el tratamiento de los datos personales; es decir, supone una protección contra terceros que no estén directamente involucrados con el tratamiento de los mismos, para lo cual se requiere que se implementen todas las medidas técnicas, organizativas y legales a fin de garantizar la confidencialidad de los datos personales.*
> *(…)*
> *35. Así, con respecto a la implementación de medidas de seguridad para restringir la copia o reproducción de documentos que contengan datos personales; durante las actuaciones de fiscalización se solicitó a la administrada acceder al sistema SIEBEL en tiempo real, a fin de realizar unas pruebas, para lo cual, gestionó con su socio de negocio VP MOBILE S.A.C. dicho acceso. Así que, se accedió a la computadora asignada al personal de ventas de la mencionada empresa, verificándose que tiene acceso a cuentas de correo electrónico personal (Hotmail y Yahoo!), redes sociales (Facebook) y aplicaciones de mensajería instantánea (WhatsApp), lo cual genera riesgo de fuga de información, toda vez que a través de estos canales, puede filtrarse la información que contiene el sistema SIEBEL, ya que en la computadora verificada se registran las altas y bajas de líneas telefónicas, lo cual supone el acceso al sistema proporcionado por la administrada.*
> *36. Por lo tanto, ENTEL PERÚ S.A. como responsable y titular del banco de datos de "clientes" debe cerciorarse que sus socios comerciales cumplan con lo establecido en el artículo 43° del RLPDP, estableciendo criterios adecuados y necesarios, así como tomando acciones que permitan verificar el cumplimiento de lo dispuesto en el artículo antes citado.*
> *(…)*
> *40. En ese sentido, ENTEL PERÚ S.A. como titular del banco de datos personales de clientes tiene la obligación de guardar confidencialidad respecto de los mismos, así como la responsabilidad de adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos personales que evite su alteración, pérdida, tratamiento o acceso no autorizado, lo que en el presente caso no habría ocurrido, ya que, tal como se ha mencionado y de acuerdo a la evidencia recabada, los datos de la denunciante se han filtrado a una tercera persona, situación que vulneró el deber de confidencialidad dispuesto en el artículo 32° del RLPDP."*

76. Este hecho constituyó el sustento de la imputación efectuada con la Resolución Directoral N° 263-2023-JUS/DGTAIPD-DFI, que desarrolló lo siguiente:

> *"s. En este contexto, la confidencialidad implica la protección de los datos personales para prevenir el acceso no autorizado por parte de terceros no involucrados en su tratamiento, para lograrlo es esencial implementar todas las medidas técnicas, organizativas y legales necesarias.*

> *t. Es importante destacar que la confidencialidad es la característica que mantiene la información en privado y evita su divulgación a personas no autorizadas, característica que se ha visto comprometida en este caso.*
> *u. El titular del banco de datos personales debe establecer y mantener las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales que posee, además, debe asegurarse de que estos datos no se traten ni divulguen sin el consentimiento de la persona o la autoridad competente autorizada.*
> *v. En caso de una filtración de información, el titular del banco de datos debe notificar a las personas cuyos datos puedan haber sido comprometidos, permitiéndoles tomar medidas de protección y estar alertas ante cualquier uso indebido de los datos, ya sea intencional o no, por parte del titular del banco de datos hacia terceros no autorizados."*

77. Al respecto, la administrada señaló en sus descargos que, al contar con las medidas de seguridad para su sistema "Siebel" requeridas por el Reglamento de la LPDP, no se le puede imputar inobservancia del deber de confidencialidad.

78. Por su parte, en su comunicación de marzo de 2024, la administrada señala que existen diferencias entre las medidas de seguridad y la obligación de confidencialidad, siendo que esta última versa sobre la reserva de la información.

79. Para tratar estos argumentos, es pertinente volver a lo señalado en el considerando 70 de esta resolución directoral, debiendo saber que en la visita de fiscalización del 10 de noviembre de 2022, se verificaron deficiencias concernientes a la carencia de registros de interacción lógica del sistema "Siebel", sobre las cuales la administrada señaló que contaban con el programa "Splunk" que podría permitir identificar al trabajador responsable de filtrar la información de la denunciante, pero no arroja resultados inmediatos.

80. Así también, se verificó en algunos equipos en los que se maneja este sistema (ubicados en el primer piso del establecimiento visitado), manejados por personal de la empresa VP Mobile S.A.C., que contaban con acceso a internet, cuentas de correo electrónico personal, redes sociales y aplicaciones de mensajería instantánea, de acuerdo con lo que el personal de fiscalización apuntó en su momento.

81. Tales circunstancias delatan omisiones en el tratamiento automatizado de los datos personales de sus clientes, a través del sistema "Siebel", relevantes, toda vez que facilitaban tanto el acceso a tales datos personales, así como su salida, a través de la posibilidad del envío vía correo electrónico o servicios de mensajería instantánea.

82. No obstante ello, es pertinente tomar en cuenta también que en la segunda visita de fiscalización, se pudo comprobar la generación de registros de interacción lógica, lo cual posibilitó verificar que un acceso no justificado desde la cuenta asignada a la señora [redacted] (promotora), trabajadora de Manpower, toda vez que no se creó ninguna orden de venta ni tampoco hubo mayores interacciones.

83. En esta segunda visita de fiscalización, efectuada con recursos remotos, se pudo verificar el acceso que tuvo la señora [redacted] desde la cuenta que se le habilitó; sobre lo cual, la administrada, en marzo de 2023, informó que se trataba de una empleada de Manpower, encargada del tratamiento de los datos personales de los clientes que compraban equipos de líneas móviles.

84. Al respecto, cabe tener en cuenta que de acuerdo con lo verificado en dicha diligencia, la señora [redacted] pudo acceder a los datos personales del panel detallado de la denunciante: Nombre, DNI, servicios, líneas asociadas, servicios del hogar y otros no detallados.

85. De lo expuesto, se aprecian deficiencias con el empleo del programa "Splunk", que no arroja resultados inmediatos respecto de los registros de interacción lógica, lo cual califica como una omisión relevante que permite situaciones como el acceso no autorizado, como el del presente caso.

86. Ahora bien, es pertinente señalar que la administrada, en sus comunicaciones, no informó sobre otras medidas para prevenir una posterior salida no autorizada de los datos personales.

87. Sobre esto último, esta Dirección solicitó en agosto de 2024, información sobre las medidas de control adoptadas sobre el mencionado acceso no autorizado, sobre Manpower, en su calidad de encargada, y la trabajadora de esta.

88. Ante ello, la administrada solo informó sobre el cese de la señora [redacted], por parte de Manpower, sin informar sobre otras acciones encaminadas más directamente a la corrección y prevención de accesos no autorizados como los del presente caso.

89. Dicha situación implica que la administrada no ha demostrado haber adoptado medidas como acciones de instrucción u otras medidas preventivas de accesos no autorizados, aparte de la búsqueda de registros realizados con el programa "Splunk"; ni tampoco de acciones de tipo organizativo respecto de Manpower, en su calidad de encargada, que le corresponden por ser responsable del tratamiento.

90. Estos factores, de los últimos tres considerandos están relacionados con lo desarrollado por la administrada en sus alegatos: La supuesta imposibilidad del control de la conducta de la señora [redacted], por ser ella empleada de su encargada (Manpower).

91. Por lo expuesto en dichos considerandos, tanto como en la segunda cuestión previa, esta Dirección debe concluir que al satisfacerse el interés comercial de la administrada con los servicios prestados por Manpower, aquella tiene el deber de controlar y garantizar que dichos servicios se presten de forma lícita, concordante con lo dispuesto en la LPDP y su reglamento.

92. En vista de las situaciones descritas, se tienen claros los siguientes hechos:

- De acuerdo con lo verificado en la segunda visita de fiscalización, solo se accedió a los siguientes datos personales de la denunciante: Nombres, DNI, líneas asociadas, servicios contratados.
- La administrada tuvo la opción de consultar para obtener los registros de interacción lógica del usuario de la señora [redacted], no obteniéndolos oportunamente; no obstante ello, se le pudo identificar con tales registros.
- No sustentó el haber adoptado otras medidas de control necesarias sobre dicha actividad de tratamiento encargada a Manpower.

93. Se comprueba entonces un acceso no autorizado a los datos personales de la denunciante, como hecho imputado a la administrada, en el marco de las omisión señalada respecto de la obtención oportuna de los registros de interacción lógica del usuario de la señora [redacted] y respecto de otras acciones de control; configurándose con ello una acción de enmienda parcial sobre tal responsabilidad.

94. En consecuencia, la administrada es responsable por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP; responsabilidad que será atenuada, de acuerdo con lo explicado en el considerando anterior, en aplicación del artículo 126 de dicho reglamento.

95. Cabe informar que se aplica esta sanción por las acciones de tratamiento de los datos personales de la denunciante, específicamente realizadas con el usuario asignado a la señora [redacted]; lo que implica que, en caso se vuelva a reportar una salida o acceso no autorizado de tales datos personales o de los de otro cliente, se podrá iniciar otras acciones de fiscalización, por tratarse de nuevos hechos, y de ser el caso, iniciar otro procedimiento sancionador.

VIII. Sobre la determinación de la sanción a aplicar

96. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, modificó el artículo 38 de la LPDP que tipificaba las infracciones a la LPDP y su reglamento, incorporando el artículo 132 al Título VI sobre Infracciones y Sanciones de dicho reglamento, que en adelante tipifica las infracciones.

97. Por su parte, el artículo 39 de la LPDP establece las sanciones administrativas calificándolas como leves, graves o muy graves y su imposición va desde una multa de cero coma cinco (0,5) unidades impositivas tributarias hasta una multa de cien (100) unidades impositivas tributarias[26], sin perjuicio de las medidas

[26] Ley N° 29733, Ley de Protección de Datos Personales
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).
(…)

correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[27].

98. En el presente caso, se ha establecido la responsabilidad de la administrada por no haber garantizado la confidencialidad de los datos personales de la denunciante (nombre, número de DNI, fecha de nacimiento y número de teléfono), al haberse filtrado estos a una tercera persona, en incumplimiento del artículo 17 de la LPDP.

99. Con el objeto de establecer criterios para el cálculo del monto de las multas aplicables por infracciones a las normas de protección de datos personales, en ejercicio de la potestad sancionadora de la Autoridad Nacional de Protección de Datos Personales, se aprobó la Metodología para el Cálculo de Multas en materia de Protección de Datos Personales, aprobada mediante la Resolución Ministerial N° 0326-2020-JUS

100. En tal contexto, se procederá a calcular la multa correspondiente.

Sobre el incumplimiento del deber de confidencialidad sobre los datos personales de la denunciante

Se ha determinado la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP, a la cual, de acuerdo con lo establecido en el inciso 2 del artículo 39 de la LPDP, corresponde una multa desde más de cinco (5) UIT hasta cincuenta (50) UIT.

El beneficio ilícito no se ha podido determinar, pues en el trámite del procedimiento administrativo sancionador se ha verificado que la administrada compensó el obtenido con la atención a la denunciante, toda vez que llegó a una transacción extrajudicial; así como tampoco se tiene información sobre el monto que ahorró, ahorraría o pensaba ahorrar cometiendo la infracción (costos evitados).

En la medida de ello, para determinar el monto de la multa corresponde aplicar la "multa prestablecida", cuya fórmula general es:

***M = Mb x F**, donde:*

M	Multa preestablecida que corresponderá aplicar en cada caso.
Mb	Monto base de la multa. Depende de la gravedad del daño del bien jurídico protegido: variable absoluta y relativa.
F	Criterios o elementos agravantes o atenuantes.

[27] **Artículo 118.- Medidas cautelares y correctivas**.
Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley Nº 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones.

Bajo la fórmula de la multa prestablecida, el monto de la misma es producto del Monto Base (variable absoluta y la variable relativa) por los factores atenuantes o agravantes que se hayan presentado, conforme al inciso 3 del artículo 248 de la LPAG, así como los artículos 125 y 126 del Reglamento de la LPDP.

La variable absoluta da cuenta del rango en el que se encontraría la multa aplicable, dependiendo de si es una infracción muy grave, grave o leve. Por su parte, la variable relativa determina valores específicos dependiendo de la existencia de condiciones referidas al daño al bien jurídico protegido, como se aprecia en el siguiente gráfico:

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 g) del numeral 2 del artículo 132 del Reglamento de la LPDP, por la remisión de datos personales de la denunciante a un tercero, corresponde el grado relativo "3" lo cual significa que la multa tendrá como Mb (Monto base) **22,50 U.I.T.**, conforme al siguiente gráfico:

N°	Infracciones graves	Grado relativo
2.g	Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733 2.g.3. Datos no sensibles	3

Ahora, conforme a lo expuesto, el Mb debe multiplicarse por F, el valor atribuido a cada uno de los factores agravantes y atenuantes previstos en la normativa.

Cuadro 3
Valores de factores agravantes y atenuantes

f_n	Factores agravantes o atenuantes	Valor
f_1	**(d) Perjuicio económico causado**	
$f_{1.1}$	. No existe perjuicio.	0.00
$f_{1.2}$	. Existiría perjuicio económico sobre el denunciante o reclamante.	0.10
f_2	**(e) Reincidencia**	
$f_{2.1}$	. No hay reincidencia.	0.00
$f_{2.2}$	. Primera reincidencia.	0.20
$f_{2.3}$	. Dos o más reincidencias.	0.40

f_n	Factores agravantes o atenuantes	Valor
f_3	**(f) Las circunstancias**	
$f_{3.1}$	. Cuando la conducta infractora genere riesgo o daño a una persona.	0.10
$f_{3.2}$	. Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas.	0.20
$f_{3.3}$	. Cuando la conducta infractora haya afectado el interes público.	0.30
$f_{3.4}$	. Cuando la infracción es de carácter instantáneo y genera riesgo de afectación de otros derechos.	0.15
$f_{3.5}$	. Cuando la duración de la infracción es mayor a 24 meses.	0.25
$f_{3.6}$	. Entorpecimiento en la investigación y/o durante el procedimiento.	0.15
$f_{3.7}$	. Reconocimiento de responsabilidad expreso y por escrito de las imputaciones, después de notificado el inicio del procedimiento sancionador.	-0.30
$f_{3.8}$	. Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador.	-0.15
$f_{3.9}$	. Colaboración con la autoridad, reconocimiento espontáneo y acción de enmienda, después de notificado el inicio del procedimiento sancionador.	-0.30
f_4	**(g) Intencionalidad**	
$f_{4.1}$	. Se advierte conocimiento y voluntad de cometer la conducta infractora	0.30

En el presente caso, en concordancia con el beneficio ilícito, se genera un perjuicio económico a la denunciante.

De otro lado, debe tomarse en consideración que en el expediente N° 018-2021-JUS/DGTAIPD-DFI, se sancionó a la administrada por la comisión de la infracción tipificada en el literal g) del numeral 2 del artículo 132 del Reglamente de la LPDP, consistente en la remisión de documentos de remisión de documentos de facturación a una persona distinta al titular de las líneas telefónicas, notificándose la Resolución Directoral N° 3127-2022-JUS/DGTAIPD-DPDP, notificada el 22 de agosto de 2022, adquiriendo firmeza el 14 de septiembre de 2022, fecha en que venció el plazo para interponer recursos impugnatorios en su caso.

De otro lado, la conducta del presente expediente se configuró en una fecha en la que dicha resolución no se encontraba firme, sino en período para interponer las mencionadas impugnaciones, por lo que no se podría aplicar la reincidencia en el presente caso.

En cuanto a las circunstancias de la infracción, debe señalarse que el incumplimiento del artículo 17 de la LPDP implica la vulneración del derecho de los titulares de los datos personales a evitar todo acceso no autorizado a tales datos, con lo que se busca proteger tanto su voluntad y autodeterminación informativa reconocida por el Tribunal Constitucional en la sentencia recaída en el expediente N° 04387-2011-PHD/TC; existiendo la obligación de prevenir los riesgos y efectivas vulneraciones, a través de accesos no autorizados a los datos personales.

Siguiendo el análisis del caso concreto y conforme a lo expuesto en la presente resolución directoral, en relación a los factores relacionados a las circunstancias de la infracción (f_3) corresponde aplicar las siguientes calificaciones para efectos del cálculo, el factor f3.8, relativo a la colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador.

En total, los factores de graduación suman un total de -15%, así como se muestra en el siguiente cuadro:

Factores de graduación	Calificación
f1. Perjuicio económico causado	0%
f2. Reincidencia	0%
f3. Circunstancias f3.8 Colaboración con la autoridad y acción de enmienda, después de notificado el inicio del procedimiento sancionador	-15%
f4. Intencionalidad	0%
f1+f2+f3+f4	**-15%**

Considerando lo señalado anteriormente, luego de aplicar la fórmula preestablecida para el cálculo de la multa, el resultado es el siguiente:

Componentes	Valor
Monto base (Mb)	22,50 UIT
Factor de agravantes y atenuantes (F)	0.85
Valor de la multa	**19,12 UIT**

Por las consideraciones expuestas y de conformidad con lo dispuesto por la LPDP y su reglamento, la LPAG, y el Reglamento del Decreto Legislativo N° 1353;

SE RESUELVE:

Artículo 1.- Sancionar a Entel Perú S.A. con la multa ascendente a diecinueve coma doce Unidades Impositivas Tributarias (19,12 UIT) por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP.

Artículo 2.- Imponer a Entel Perú S.A. como medida correctiva, acreditar la adopción e implementación de medidas de control consistentes en la revisión de las medidas de seguridad técnicas sobre los equipos empleados por sus encargados y de ser el caso, por sus propios trabajadores, para operar los sistemas con los que se acceda y se realice el tratamiento de los datos personales de sus clientes.

Para el cumplimiento de tal medida correctiva, se otorga el plazo de cincuenta y cinco días hábiles (55) días hábiles contados a partir de la notificación de la presente resolución. En caso de presentar recurso impugnatorio el plazo para el cumplimiento de la medida correctiva es de cuarenta (40) días hábiles de notificada la resolución que resuelve el recurso y agota la vía administrativa.

Artículo 3.- Informar a Entel Perú S.A. que el incumplimiento de la medida correctiva dispuesta en el marco de un procedimiento sancionador constituye la comisión de una infracción muy grave, de conformidad con el literal d) del numeral 3 el artículo 132 del Reglamento de la LPDP[28].

[28] **Artículo 132.- Infracciones**
Las infracciones a la Ley Nº 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley. (…)
2. Son infracciones graves:
(…)

Artículo 4.- Informar a Entel Perú S.A. que, contra la presente resolución directoral, de acuerdo con lo indicado en el artículo 218 de la LPAG, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación[29].

Artículo 5.- Informar a Entel Perú S.A. que vencido el plazo para interponer recurso impugnatorio se entiende que el acto administrativo que resuelve el procedimiento administrativo queda firme conforme a lo dispuesto en el artículo 222 de la LPAG; o, de interponerse recurso impugnatorio, al resolverse este será ejecutiva cuando ponga fin a la vía administrativa, es decir, al día siguiente de notificada la resolución que resuelve el recurso impugnatorio que pone fin a la vía administrativa, ello de acuerdo con lo establecido en el numeral 258.2 del artículo 258 de la LPAG; y, que se considera inscrita la sanción impuesta en esta resolución directoral, en el Registro Nacional de Protección de Datos Personales.

Artículo 6.- Informar a Entel Perú S.A. que deberá realizar el pago de la multa en el plazo de veinticinco (25) días hábiles desde el día siguiente de notificada la presente resolución directoral[30].

Artículo 7.- En caso se presente recurso impugnatorio, el plazo para pagar la multa es de diez (10) días hábiles de notificada la resolución que agota la vía administrativa, plazo que se contará desde el día siguiente de notificada dicha resolución de segunda instancia administrativa.

Artículo 8.- Se entenderá que cumplió con pagar la multa impuesta, si antes de que venzan los plazos mencionados, cancela el sesenta por ciento (60%) de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP[31]. Para el pago de la multa, se deberá tener en cuenta el valor de la UIT del año 2022.

Artículo 9.- Notificar a Entel Perú S.A. la presente resolución.

---

h) No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley Nº 29733, a pesar de haber sido requerido para ello por la Autoridad en el marco de un procedimiento sancionador.
(…)
3. Son infracciones muy graves:
(…)
d) No cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador o de un procedimiento trilateral de tutela.

[29] **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.

[30] El pago de la multa puede ser realizado en el Banco de la Nación con el código 04759.

[31] **Artículo 128.- Incentivos para el pago de la sanción de multa.**
Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta.

Artículo 10.- Notificar al denunciante la presente resolución directoral, con fines informativos.

Regístrese y comuníquese.

María Alejandra González Luna
Directora (e) de Protección de Datos Personales

MAGL/rvr