



Resolución Directoral N° 708-2020-JUS/DGTAIPD-DPDP

Expediente N°
121-2018-JUS/DGTAIPD-PAS

Lima, 17 de febrero de 2020

VISTOS:

El Informe N° 084-2019-JUS/DGTAIPD-DFI del 31 de julio de 2019¹, 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), junto con los demás documentos que obran en el respectivo expediente; y,

CONSIDERANDO:

I. Antecedentes

1. Mediante Hoja de Trámite N° 42139-2018MSC de fecha 4 de julio de 2018, la [REDACTED] (en adelante, la denunciante) interpuso denuncia² por actos contrarios a la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, la "LPDP") y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, el "Reglamento de la LPDP") contra Entel Perú S.A (en adelante, la administrada).

2. La denunciante manifestó lo siguiente:

- Que, el 21 de marzo de 2018 adquirió un celular en ENTEL y solicitó la portabilidad de su número telefónico móvil a ENTEL.
- Que, ENTEL portó el número telefónico de otra persona y se lo asignaron a la denunciante.
- Que, ante el reclamo del titular del número telefónico asignado a la denunciante, ENTEL, le proporcionó a este último una ficha con todos los datos personales de la denunciante (nombre completo, celular, dirección, DNI, RUC, número de solicitud de portabilidad, la fecha y hora en la que la solicitó, la persona que la atendió y plan tarifario).
- Que, la denunciante tomó conocimiento de este hecho cuando fue contactada por el titular del número telefónico que le había sido asignado, quien a su vez le reenvió la ficha con sus datos personales, obtenida de ENTEL.



GONZALEZ I

¹ Folios 69 a 73

² Folios 2 a 8

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

3. Mediante Oficio N° 473-2018-JUS/DGTAIPD-DFI³, se corrió traslado a la administrada de la denuncia presentada en su contra, la misma que le fue notificada el día 31 de julio de 2018.

4. Mediante escrito ingresado con Hoja de Trámite N° 52605-2018⁴ el 14 de agosto de 2018, la administrada solicitó una prórroga para presentar descargos.

5. Con fecha 23 de agosto de 2018, la administrada presentó sus descargos a la denuncia mediante escrito ingresado con Hoja de Trámite N° 54786-2018⁵, alegando lo siguiente:

- 5.1. Que, ha solicitado a Recursos Humanos tomar manifestación de lo ocurrido al asesor que habría proporcionado los datos personales de la denunciante, a efectos de evaluar las sanciones a imponerle.
- 5.2. Que, los contratos de trabajo suscritos por sus trabajadores contienen una cláusula de confidencialidad, donde se indica que debido a las funciones que realizarán tendrán acceso a información privada de los abonados.
- 5.3. Que, sobre la información privada de los abonados (que contempla información personal de los mismos), el trabajador se compromete a (i) no utilizarla para fines ajenos con la ejecución de funciones asignadas por la administrada, (ii) no divulgarla a terceros, (iii) coadyuvar a su protección y (iv) cumplir con las disposiciones relativas al resguardo de la misma que dicte la administrada.
- 5.4. Que, el incumplimiento de la obligación de confidencialidad hace responsable al trabajador ante la administrada por todo daño.
- 5.5. Que, el Reglamento Interno de Trabajo (en adelante, el RIT) establece como obligaciones de los trabajadores las siguientes:

5.5.1. Literal t) del artículo 61 del RIT:

"(i) Guardar absoluta reserva y confidencialidad sobre cualquier información comercial, técnica, administrativa o corporativa que resulte esencial para el funcionamiento y desarrollo de Entel así como respecto de información personal de los colaboradores de la empresa, a la que hubieren tenido acceso con ocasión de sus funciones o en forma indirecta, especialmente aquella que concierne a los servicios que brinda la empresa, sin que sea necesario que haya sido previamente calificada como tal, debiendo abstenerse de proporcionar igualmente dicha información a terceros. Asimismo, en caso de terminación de la relación laboral, esta obligación de confidencialidad se mantendrá vigente por un lapso de cinco (5) años computados a partir de la fecha de terminación de la relación laboral."

5.5.2. Literal v) del artículo 61 del RIT:

"v) No extraer directa o indirectamente, información de la empresa, ya sea en medios físicos como documentos originales, impresiones o fotocopias; o medios electrónicos como correos electrónicos, diskettes, discos compactos, discos duros extraíbles, discos virtuales y/o cualquier otro dispositivo electrónico; en especial si tienen carácter reservado, para usos ajenos a sus labores."

- 5.6. Que, el literal j) del artículo 62 del RIT establece como prohibición expresa a los trabajadores:



³ Folio 11

⁴ Folio 13

⁵ Folios 15 a 19

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

"Divulgar fuera o dentro del ámbito de la empresa a personas no autorizadas cualquier información o documentación de uso interno, especialmente la considerada como reservada, confidencial, estratégica y la considerada como secreto industrial o comercial."

- 5.7. Que, el Código de Ética (en adelante, el CE) hace varias referencias a la confidencialidad de la información:

"Mantener la confidencialidad de los antecedentes, datos y/o información de los clientes y resguardar la privacidad en las comunicaciones, en conformidad con las normas legales que rigen este mercado" (Página 12 del CE)

"Los colaboradores deben respetar también la confidencialidad de la información de nuestros clientes, colaboradores, proveedores, distribuidores, contratistas y socios de negocio, así como de cualquier dato personal que recaudemos y procesemos. En materia de uso y manejo de información, todos los colaboradores deberán conocer y dar cumplimiento a las normas legales reglamentarias, así como a todas las políticas y contratos de confidencialidad aplicables." (Página 19 del CE)



- 5.8. Que, se han efectuado capacitaciones a todos sus colaboradores sobre el CE, destacando que la información solo podrá entregarse al titular de la misma.
- 5.9. Que, ha enviado correos electrónicos a sus asesores recordándoles la importancia de la confidencialidad de la información de sus abonados, y que la misma no debe ser proporcionada a terceros.

6. Por medio del Informe de Fiscalización N° 160-2018-DFI-AARM del 9 de noviembre de 2018⁶, el Analista Legal de Fiscalización de la DFI concluye que se ha determinado con carácter preliminar que existen circunstancias que justifican la instauración del procedimiento administrativo sancionador contra la administrada.

7. Dicho Informe de Fiscalización fue notificado el 16 de noviembre de 2018 a la administrada mediante Oficio N° 719-2018-JUS/DGTAIPD-DFI⁷.

8. Por medio de la Resolución Directoral N° 095-2019-JUS/DGTAIPD-DFI del 31 de mayo de 2019⁸ (en adelante, la "RD de Inicio"), la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la presunta comisión del hecho infractor:

- La administrada habría realizado tratamiento de datos personales, incumpliendo la obligación de confidencialidad, establecida en el artículo 17 de la LPDP, al haber transferido los datos de la denunciante sin que ésta haya otorgado su consentimiento para dicho tratamiento.

9. Mediante el Oficio N°501-2019-JUS/DGTAIPD-DFI⁹, se notificó dicha Resolución Directoral a la administrada el día 25 de junio de 2019.

10. A través del escrito ingresado con Hoja de Trámite N°50255-2019 del 15 de julio de 2019¹⁰, la administrada solicitó una prórroga para presentar descargos. Asimismo, solicitó copia de los anexos del escrito que obra a fojas 6 a 7.

⁶ Folios 21 a 22

⁷ Folio 24

⁸ Folios 26 a 29

⁹ Folio 31

¹⁰ Folios 33 a 39

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

11. Mediante Proveído¹¹ de fecha 17 de julio de 2019 se dispuso la notificación de los folios 6 a 7, asimismo se concedió una prórroga de tres (3) días hábiles para la presentación de descargos. Dicho Proveído fue notificado a la administrada el 17 de julio de 2019, mediante Oficio N° 605-2019-JUS/DGTAIPD-DFI¹².

12. Mediante escrito ingresado el 22 de julio de 2019, mediante Hoja de Trámite N°52310-2019, la administrada presentó descargos, solicitando archivar el procedimiento por los siguientes argumentos:

- 12.1. La notificación de cargos transgrede lo dispuesto por el TEO de la LPAG, en tanto existe una incongruencia en la imputación, siendo que por un lado al indicar que las conclusiones a las que arriba el órgano de fiscalización son que no existen circunstancias que justifican la Instauración de un procedimiento sancionador en su contra (numeral 5 de los Antecedentes de la Resolución de Inicio); en la notificación de cargos decide proseguir con el inicio del procedimiento en contra de la administrada (artículo primero de la parte resolutive de la Resolución de Inicio)
- 12.2. Dicha incongruencia contraviene el elemento imprescindible de precisión con el que debe contar toda notificación de cargos.
- 12.3. El inicio del procedimiento transgrede el principio de razonabilidad, en tanto, si bien los hechos imputados efectivamente acontecieron, la administrada ha acreditado la implementación de medidas para el tratamiento adecuado de los datos personales, conforme a la LPDP y su Reglamento, en el RIT y el CE.
- 12.4. El error aislado e involuntario de unos de sus asesores comerciales no debería constituir indicio suficiente para afirmar que la administrada no maneja de forma confidencial los datos de la totalidad de sus clientes.
- 12.5. Independientemente del proceso disciplinario iniciado al asesor comercial que incurrió en el incorrecto uso de los datos personales de la denunciante, la administrada procedió a remitir comunicaciones a sus trabajadores vía correo electrónico, recordando la importancia de la confidencialidad.
- 12.6. Incluso desde antes de la conducta imputada, la administrada ha tomado medidas para una correcta protección de datos personales de sus clientes. Adjuntó email con medidas de refuerzo en materia de protección de datos de fecha 21 de agosto de 2018.
- 12.7. La infracción imputada no puede imputarse a título de dolo o culpa. Existen supuestos en los cuales las personas jurídicas no deben responder por conductas cometidas por sus dependientes o representantes. Pese a que se han desplegado máximos esfuerzos, se ha incurrido en la infracción.

13. Por medio de la Resolución Directoral N°133-2019-JUS/DGTAIPD-DFI del 31 de julio de 2019¹³, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

14. Mediante Informe Final de Instrucción N° 084-2019-JUS/DGTAIPD-DFI del 31 de julio de 2019¹⁴, 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 lo siguiente:



M. GONZALEZ I...

¹¹ Folio 40

¹² Folio 42

¹³ Folios 66 a 68

¹⁴ Folios 69 a 73

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP



M. GONZALEZ

- Imponer sanción administrativa de multa ascendente a diecinueve unidades impositivas tributarias (19 UIT), por el cargo acotado en el hecho imputado N° 1 a la administrada, por la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP: "Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733."

15. Mediante Oficio N°642-2019-JUS/DGTAIPD-DFI, el 13 de agosto de 2019¹⁵, se notificó a la administrada la Resolución Directoral N° 133-2019-JUS/DGTAIPD-DFI y el Informe Final de Instrucción N° 084-2019-JUS/DGTAIPD-DFI.

16. A través del escrito ingresado con Hoja de Trámite N°59209-2019 del 19 de agosto de 2019¹⁶, la administrada solicitó una ampliación del plazo otorgado tanto para emitir sus descargos, así como para solicitar el informe oral respectivo.

17. Mediante Oficio N°2161-2019-JUS/DGTAIPD-DPDP, notificado a la administrada el día 3 de setiembre de 2019¹⁷, se le informó la programación del informe oral solicitado para 19 de setiembre de 2019 a las 10:00 horas.

18. La administrada no se presentó al informe oral programado.

II. Competencia

19. 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.

20. 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

21. Acerca de la responsabilidad de la administrada, se deberá tener en cuenta que el literal f) del numeral 1 del artículo 257 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General (en adelante, la "LPAG"), establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos¹⁸.

22. Asimismo, se debe atender a lo dispuesto en el artículo 126 del Reglamento de la LPDP, que considera como atenuantes la colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones conjuntamente con la adopción de medidas de enmienda; dichas atenuantes, de acuerdo con la oportunidad del

¹⁵ Folio 74

¹⁶ Folio 76

¹⁷ Folio 79

¹⁸ Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS

"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."

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

reconocimiento y las fórmulas de enmienda, pueden permitir la reducción motivada de la sanción por debajo del rango previsto en la LPDP¹⁹.

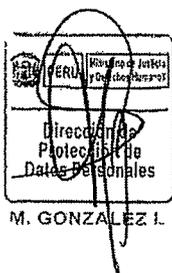
23. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG²⁰, que establece como condición atenuante el reconocimiento de la responsabilidad por parte del infractor de forma expresa y por escrito, debiendo reducir la multa a imponérsele hasta no menos de la mitad del monto de su importe; y por otro lado, las que se contemplen como atenuantes en las normas especiales.

IV. Cuestiones en discusión

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

24.1. Si la administrada es responsable por el siguiente hecho infractor:

- La administrada habría realizado tratamiento de datos personales, incumpliendo la obligación de confidencialidad, establecida en el artículo 17 de la LPDP, al haber transferido los datos de la denunciante sin que ésta haya otorgado su consentimiento para dicho tratamiento.



24.2. En el supuesto de resultar responsable, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, prevista en el literal f) del 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.

24.3. Determinar la multa que corresponde imponer, tomando en consideración los criterios de graduación contemplados en el numeral 3 del artículo 248 de la LPAG.

V. Análisis de las cuestiones en discusión

Sobre el presunto tratamiento de datos personales incumpliendo la obligación de confidencialidad establecida en el artículo 17 de la LPDP

25. La LPDP establece como uno de sus principios rectores, el consentimiento en el artículo 5 que señala que "Para el tratamiento de los datos personales debe mediar el consentimiento de su titular". Dicho consentimiento debe ser libre, expreso e informado de acuerdo a lo señalado en el numeral 5 de la LPDP. Sin embargo, es preciso tener en cuenta que la obligación de obtener el consentimiento tiene excepciones, las cuales se encuentran previstas en el artículo 14 de la LPDP, no

¹⁹ Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS
"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"

²⁰ Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS

"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."

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

2007-MTC (en adelante, el "TUO del Reglamento de la Ley de Telecomunicaciones") establece lo siguiente:

"Artículo 13.- Inviolabilidad y secreto de las telecomunicaciones

(...)

Los concesionarios de servicios públicos de telecomunicaciones están obligados a salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, adoptar las medidas y procedimientos razonables para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios, así como mantener la confidencialidad de la información personal relativa a sus usuarios que se obtenga en el curso de sus negocios, salvo consentimiento previo, expreso y por escrito de sus usuarios y demás partes involucradas o por mandato judicial.



Los titulares de servicios privados de telecomunicaciones deberán adoptar sus propias medidas de seguridad sobre inviolabilidad y secreto de las telecomunicaciones.

El Ministerio podrá emitir las disposiciones que sean necesarias para precisar los alcances del presente artículo." (El subrayado es nuestro)

31. Asimismo, es pertinente citar la "Norma que establece las medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales, y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones" aprobada mediante Resolución Ministerial N° 111-2009-MTC/03 (en adelante, la "Norma del Secreto de las Telecomunicaciones y Protección de Datos") que regula las medidas necesarias que deben adoptar las operadoras de estos servicios para que los datos personales de sus abonados o usuarios no sean obtenidos por terceros.

En este sentido, es pertinente citar los siguientes acápites de la referida Norma:

"6. ÁMBITO DE PROTECCIÓN

La protección del derecho a la inviolabilidad y al secreto de las telecomunicaciones y a la protección de datos personales, comprende, entre otros aspectos, los siguientes:

(...)

- La información personal que los Operadores de Telecomunicaciones obtengan de sus abonados y usuarios en el curso de sus operaciones comerciales y que se encuentre contenida en soportes físicos, informáticos o similares, tales como documentos privados y bases de datos, en tanto el usuario o abonado no haya autorizado su difusión o esté permitida por el marco legal vigente.

(...)"

"8. DE LA VULNERACIÓN A LA PROTECCIÓN DE DATOS PERSONALES

Se atenta contra la protección de la información personal relativa a los abonados o usuarios cuando ésta es entregada a terceros, salvo las excepciones previstas en la legislación vigente. La obligación de protección a que se refiere el párrafo precedente, no incluye la información que los Operadores de Telecomunicaciones deben incluir en las guías de abonados que publiquen, según corresponda.

Asimismo, no constituye vulneración a la protección de datos personales, la entrega de información personal de los usuarios o abonados a terceros que participen en la gestión comercial del servicio y respecto de la información estrictamente necesaria para dicho fin. Sin perjuicio de ello, la entrega y resguardo de esta información, deberá efectuarse de conformidad con lo dispuesto en la presente Norma."

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

encontrándose inmerso en ninguna de ellas la administrada en el caso materia de análisis.

26. El numeral 1 del artículo 13 de la LPDP establece que “*el tratamiento de datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta Ley les confiere. (...)*”

27. Es en este contexto, que una de las formas de materializar el resguardo y respeto de los datos personales sobre los cuales una entidad realiza tratamiento para la ejecución de la prestación de los servicios que ofrece a sus clientes, es a través del cumplimiento de la obligación de confidencialidad que se encuentra prevista en el artículo 17 de la LPDP:



“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. (El subrayado es nuestro)

28. Inclusive, para el caso del tratamiento de datos personales por parte de los operadores de servicios de comunicaciones o telecomunicaciones, el Reglamento de la LPDP, en sus artículos 31 y 32, ha puesto énfasis en la responsabilidad de velar por la confidencialidad, seguridad y uso adecuado de los datos personales de sus abonados y usuarios:

“Artículo 31.- Tratamiento de datos personales en el sector comunicaciones y telecomunicaciones.

Los operadores de los servicios de comunicaciones o telecomunicaciones tienen la responsabilidad de velar por la confidencialidad, seguridad, uso adecuado e integridad de los datos personales que obtengan de sus abonados y usuarios, en el curso de sus operaciones comerciales. En tal sentido, no podrán realizar un tratamiento de los citados datos personales para finalidades distintas a las autorizadas por su titular, salvo orden judicial o mandato legal expreso.

Artículo 32.- Confidencialidad y seguridad.

Los operadores de comunicaciones o telecomunicaciones deberán velar por la confidencialidad, seguridad y uso adecuado de cualquier dato personal obtenido como consecuencia de su actividad y adoptarán las medidas técnicas, legales y organizativas, conforme a lo establecido en la Ley y el presente reglamento, sin perjuicio de las medidas establecidas en las normas del sector de comunicaciones y telecomunicaciones que no se opongan a lo establecido en la Ley y el presente reglamento. (El subrayado es nuestro)

29. Justamente las normas del sector de telecomunicaciones establecen que los concesionarios de estos servicios públicos están obligados a salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, debiendo adoptar medidas para mantener la confidencialidad de los datos personales de los abonados o usuarios que se obtenga en la ejecución de sus relaciones comerciales con estos.

30. En este orden de ideas, el artículo 13 del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo N° 020-

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

"10. DE LAS OBLIGACIONES DE LOS OPERADORES DE TELECOMUNICACIONES RELATIVAS A LA INVIOABILIDAD Y AL SECRETO DE LAS TELECOMUNICACIONES Y LA PROTECCIÓN DE DATOS PERSONALES

(...)

10.3 Los Operadores de Telecomunicaciones tienen la obligación de respetar y salvaguardar el secreto de las telecomunicaciones y proteger los datos personales de sus abonados y/o usuarios, salvo las excepciones previstas en la legislación vigente. En ese sentido, las medidas mínimas que se detallan en los numerales siguientes, no deberán ser entendidas, como medidas únicas y/o excluyentes, encontrándose los Operadores de Telecomunicaciones obligados a implementar las medidas y procedimientos complementarios que resulten razonables para garantizar la inviolabilidad y el secreto de las telecomunicaciones y los datos personales de sus abonados y/o usuarios. Ello, en función a las redes y tecnologías que empleen y el personal propio o de terceros que tenga acceso a la red pública o a la información confidencial de sus abonados y/o usuarios.

(...)

10.7 Los Operadores de Telecomunicaciones establecerán las medidas pertinentes para proteger la información personal contenida en los contratos de abonado y en los contratos celebrados para la adquisición, arrendamiento u otra modalidad de provisión de equipos terminales. Para dicho efecto, se deberá:

10.7.1 Celebrar acuerdos de confidencialidad con su personal y con terceros que participen de la gestión comercial y/u operativa del servicio, y que tenga acceso a la planta interna, previendo en dichos acuerdos, la obligación de no divulgar cualquier información que pudiera facilitar o coadyuvar a la vulneración del secreto de las telecomunicaciones y la protección de datos, aún después de extinguido el vínculo laboral o contractual; así como las consecuencias civiles y penales derivadas de su incumplimiento.

En la celebración de sus acuerdos con terceros, los Operadores de Telecomunicaciones les exigirán a su vez, la suscripción de acuerdos de confidencialidad con el personal que éstos tuvieran a su cargo, que tenga acceso a la planta interna del citado Operador; debiendo verificar dicho cumplimiento.

(...)"

(El subrayado es nuestro)

32. De los extractos citados de la Norma del Secreto de las Telecomunicaciones y Protección de Datos, se aprecia pues que dicha normativa sectorial se adecúa perfectamente a las disposiciones de la LPDP y su Reglamento, complementándose ambas en beneficio de la protección de datos personales de los titulares abonados o usuarios de los servicios de telecomunicaciones. Tal es la magnitud de la relevancia que se le reconoce a la protección de los datos personales de los abonados y usuarios de servicios de telecomunicaciones que un trabajador e inclusive un tercero que sea trabajador de un proveedor de la operadora de servicios de telecomunicaciones debe suscribir acuerdos de confidencialidad en resguardo de los datos personales de tales abonados.
33. Con el objetivo de brindar mayor protección al derecho de la protección de datos personales en el sector telecomunicaciones se han establecido responsabilidades por incumplimiento de obligaciones, las mismas que pueden constituir infracción grave pasibles de multas y, dependiendo de la gravedad de la infracción puede hasta repercutir en una revocación temporal o definitiva de la concesión o autorización otorgada.

"Artículo 258 del TUO del Reglamento de la Ley de Telecomunicaciones.- Infracciones muy graves

Constituyen infracciones muy graves, además de las tipificadas en el artículo 87 de la Ley, las siguientes:

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP



"1. El incumplimiento de las obligaciones de los operadores de servicios públicos de telecomunicaciones para salvaguardar la inviolabilidad y el secreto de las telecomunicaciones, así como la protección de datos personales, conforme a la normativa que regulan estas obligaciones.

(...)"

"Artículo 90 del TUO de la Ley de Telecomunicaciones.- Las infracciones consideradas como muy graves serán sancionadas con multas entre treinta (30) y cincuenta (50) Unidades Impositivas Tributarias (UIT). Adicionalmente, en función de la gravedad, la autoridad administrativa puede ordenar el decomiso de los equipos y la revocación temporal o definitiva de la concesión o autorización.

(...)"

34. De la revisión del expediente materia de pronunciamiento, ha quedado evidenciado que hubo un tratamiento indebido de los datos personales de la denunciante mediante la transferencia de los mismos, sin su consentimiento, por parte de un trabajador de la administrada. Tal hecho se traduce en un resquebrajamiento del deber de confidencialidad contemplado en el artículo 17 de la LPDP, el mismo que se encuentra reforzado, para el caso particular-siendo que la administrada es una operadora de servicios de telecomunicaciones- por los artículos 31 y 32 del Reglamento de la LPDP.

35. Ahora bien, esta Dirección considera que dada la relevancia de un correcto tratamiento de datos personales reconocido normativamente en el sector telecomunicaciones (como se puede apreciar de los considerandos 29 a 33 de esta Resolución Directoral), imponiendo el cumplimiento del deber de confidencialidad a tal punto de castigar a nivel sectorial su inobservancia y contravención con hasta la revocación de la concesión y/o autorización a la operadora; es sensato amparar los argumentos de la administrada respecto a que contempla y da a conocer a sus trabajadores la importancia del deber de confidencialidad a través de su RIT, CE y su curso virtual de CE, por el sólo hecho que se encuentra obligada a hacerlo en observancia de las medidas complementarias que resulten razonables adoptar para garantizar la protección de los datos personales de sus abonados y/o usuarios, según lo exige la Norma del Secreto de las Telecomunicaciones y Protección de Datos.

36. Sin embargo, la Norma del Secreto de las Telecomunicaciones y Protección de Datos establece como obligación expresa, en su numeral 10.7.1, celebrar acuerdos de confidencialidad con su personal y con terceros que participen de la gestión comercial y/u operativa del servicio. Al respecto, cabe señalar que si bien en sus descargos del 23 de agosto de 2018 (conforme se describe en los considerandos 5.2 a 5.4 de esta Resolución Directoral), la administrada señala que ha colocado en sus contratos de trabajo una cláusula de confidencialidad, documento que estaría firmado por sus trabajadores, no ha adjuntado al documento de descargos prueba que lo acredite.

37. Respecto a las medidas de refuerzo llevadas a cabo por la administrada como las comunicaciones internas vía claqueta informativa en correo electrónico dirigido a sus trabajadores con fecha 21 de agosto de 2018, este Despacho considera que dicha acción será tomada en cuenta, así como la presentación de su RIT, CE y curso virtual de CE para efectos de graduar la responsabilidad de la administrada, en calidad de atenuantes.

38. Por otro lado, acerca de la incongruencia en la imputación de cargos alegada por la administrada en su escrito de descargos del 22 de julio de 2019 (descrita en los considerandos 12.1. y 12.2 de la presente Resolución Directoral), este Despacho desestima su procedencia, dado que de una revisión del Informe de Fiscalización N°

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

160-2018-DFI-AARM del 9 de noviembre de 2018, se concluyó que si se había determinado con carácter preliminar que existen circunstancias que justifican la instauración del procedimiento administrativo sancionador contra la administrada, habiéndose incurrido claramente en un error material de transcripción en artículo primero de la parte resolutive de la RD de Inicio. Al haber sido notificado correcta y oportunamente el referido Informe de Fiscalización, la administrada tuvo conocimiento pleno de la existencia de circunstancias que ameritaban el inicio de un procedimiento sancionador en su contra, con lo cual no puede manifestar que la RD de Inicio contraviene el elemento imprescindible de precisión con el que debe contar toda notificación de cargos, cuando ni siquiera el contenido esencial de la misma difería de las directrices plasmadas por el Informe de Fiscalización.

39. Sobre la referencia hecha por la administrada al principio de razonabilidad, este Despacho considera que si bien un hecho aislado no constituye indicio para afirmar que es una práctica recurrente el resquebrajamiento del deber de confidencialidad por parte de la administrada, sí constituye evidencia para afirmar que en el caso materia de denuncia no se trató los datos personales de la denunciante de forma confidencial.

40. Finalmente, la administrada considera que no se le debe interponer sanción alguna en aplicación del principio de culpabilidad reconocido en el artículo 248 del TUO de la LPAG, ya que para ello no basta con demostrar que se ha producido una conducta típica, sino que ésta es atribuible a título de dolo o culpa. Al respecto, este Despacho concuerda con lo señalado por la DFI en el Informe Final de Instrucción, toda vez que en materia de protección de datos personales, existe una ley especial que recoge la aplicación de responsabilidad objetiva (siendo que el análisis debe restringirse a acreditar la existencia de la conducta típica).



“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° 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros.

Sin perjuicio de las sanciones que en el marco de su competencia imponga la autoridad competente, 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.

Los administrados son responsables objetivamente por el incumplimiento de obligaciones derivadas de las normas sobre protección de datos personales”. (El subrayado es nuestro)

41. En el caso materia de denuncia se observa que un trabajador de Entel le habría proporcionado al titular del número telefónico asignado a la denunciante los datos de la denunciante, por lo que esta Dirección considera necesario que se verifique si la administrada cuenta con las medidas de seguridad, conforme lo señalado en los artículos 9 y 16 de la LPDP, especialmente aquellas medidas relacionadas al acceso y privilegios a los bancos de datos de clientes.

Sobre las sanciones a aplicar a los hechos analizados

42. 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.

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

43. 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 tributarias²¹, sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP²².

44. En el presente caso, se ha establecido la responsabilidad de la administrada por lo siguiente:



- La administrada habría realizado tratamiento de datos personales, incumpliendo la obligación de confidencialidad, establecida en el artículo 17 de la LPDP, al haber transferido los datos de la denunciante sin que ésta haya otorgado su consentimiento para dicho tratamiento; con lo cual se configuraría una infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP, infracción sancionable con una multa desde más de cinco (5) hasta cincuenta (50) unidades impositivas tributarias.

45. Cabe señalar que esta Dirección determina el monto de la multa a ser impuesta tomando en cuenta para su graduación los criterios establecidos en el numeral 3 del artículo 248 de la LPAG. En tal sentido, debe prever que la comisión de la conducta sancionable no resulte más ventajosa para el infractor que cumplir las normas infringidas o asumir la sanción administrativa, por lo que la sanción deberá ser proporcional al incumplimiento calificado como infracción, observando para ello los criterios que dicha disposición señala para su graduación.

46. En el presente caso, se considera como criterios relevantes para graduar las sanciones, los siguientes:

- a) El beneficio ilícito resultante por la comisión de la infracción:

No se ha evidenciado beneficio ilícito alguno resultante de la comisión de la infracción a sancionar.

- b) La probabilidad de detección de las infracciones:

Sobre la verificación del incumplimiento de la obligación de confidencialidad, la probabilidad de detección de esta infracción es baja, toda vez que pudo tenerse

²¹ 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)."

²² Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS

"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 N° 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."

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

conocimiento de este quebrantamiento a raíz de la denuncia de parte interpuesta contra la administrada.

c) La gravedad del daño al interés público y/o bien jurídico protegido:

La infracción detectada afecta el derecho fundamental a la protección de datos personales, el cual se encuentra reconocido en el artículo 2, numeral 6, de la Constitución Política del Perú, siendo desarrollado por la LPDP y su reglamento.

Este Despacho considera que si bien no se ha tratado de un nivel de daño masivo que hubiese perjudicado a más abonados de la administrada, considera importante pronunciarse por el hecho acontecido, a efectos de prevenir que situaciones como la denunciada vuelvan a ocurrir y por el grado de vulnerabilidad que implica que los trabajadores de una operadora de servicios públicos de telecomunicaciones transgredan dicho deber de confidencialidad por falta de compromiso y concientización, los mismos que deben ser promovidos por la administrada. Consecuentemente, este Despacho considera razonable imponer una sanción proporcional al hecho materia de la denuncia, por el quebrantamiento, a través de uno de sus trabajadores, al deber de confidencialidad que debe imperar para la protección de los datos personales de sus abonados y usuarios.



Se debe tener en cuenta que los datos de la denunciante transferidos por la administrada son el nombre, dirección, rango de cuenta, número de solicitud, giro de negocio. Por lo tanto, no se transfirieron datos personales sensibles.

d) El perjuicio económico causado:

No se evidencia un perjuicio económico resultante de la comisión de la infracción.

e) La reincidencia en la comisión de la infracción:

La administrada no fue sancionada anteriormente por la infracción.

f) Las circunstancias de la comisión de la infracción:

Respecto del incumplimiento del artículo 17 de la LPDP debe señalarse que la administrada tiene una iniciativa de difusión del cumplimiento del deber de confidencialidad a nivel interno, sin embargo, a pesar de sus esfuerzos pueden acontecer sucesos como el denunciado, para lo cual reviste de suma importancia haga firmar acuerdos de confidencialidad asegurando con ello que el trabajador haya leído y comprendido las consecuencias graves que puede traer a la compañía, y las responsabilidades civiles y penales que puede repercutir en su contra.

Al respecto, una buena práctica consistiría en la elaboración de protocolos dirigidos al personal que tiene acceso a datos personales.

g) La existencia o no de intencionalidad en la conducta del infractor:

Se ha evidenciado la responsabilidad objetiva de la administrada en la comisión de la infracción del deber de confidencialidad, respecto a los datos personales de la denunciante.

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-DPDP

46. Es pertinente indicar que para imponer la sanción se tendrá en cuenta la suma de todos los criterios que permiten graduar la sanción conforme a los argumentos desarrollados a lo largo de la presente Resolución Directoral.

SE RESUELVE:

Artículo 1.- Sancionar a ENTEL PERÚ S.A con la multa ascendente a quince unidades impositivas tributarias (15 UIT) por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP: "Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N°29733"

Artículo 2.- Imponer como medidas correctivas a ENTEL PERÚ S.A acreditar que cumple con celebrar acuerdos de confidencialidad con sus trabajadores, sea de forma independiente o a través de una cláusula de confidencialidad en el contrato de trabajo y/o renovación de contrato de trabajo, para la protección de los datos personales de sus abonados y/o usuarios.



Para el cumplimiento de tal medida correctiva, se otorga el plazo de treinta (30) días hábiles contados a partir de la notificación que declare consentida o firme la presente resolución directoral, debiendo remitir la documentación sustentatoria de su implementación.

Artículo 3.- Informar a ENTEL PERÚ S.A que el incumplimiento de la medida correctiva constituye la comisión de la infracción tipificada como muy grave en el literal d) del numeral 3 del artículo 132 del Reglamento de la LPDP²³.

Artículo 4.- Informar a ENTEL PERÚ S.A, que contra la presente Resolución, 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 notificación²⁴.

Artículo 5.- Informar a ENTEL PERÚ S.A que el pago de la multa será requerido una vez que la resolución que impone la sanción quede firme. En el requerimiento de pago se le otorgará diez (10) días hábiles para realizarlo y se entenderá que cumplió con pagar la multa impuesta, si antes de que venza el plazo mencionado, cancela el

²³ Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS "TÍTULO VI INFRACCIONES Y SANCIONES

CAPÍTULO IV
INFRACCIONES

Artículo 132.- Infracciones

Las infracciones a la Ley N° 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.

(...)

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."

²⁴ Texto Único Ordenado de la Ley N° 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."

Resolución Directoral N° 708 -2020-JUS/DGTAIPD-PPDP

sesenta por ciento (60%) de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP²⁵.

Artículo 6. Remitir el expediente N° 121-2018-JUS-DGTAIPD-PAS para el inicio de las actuaciones de fiscalización referidas a las medidas de seguridad implementadas por la administrada para la protección de los datos personales de sus clientes a la Dirección de Fiscalización e Instrucción

Artículo 7- Notificar a ENTEL PERÚ S.A la presente Resolución Directoral.

Regístrese y comuníquese.



.....
MARIA ALEJANDRA GONZÁLEZ LUNA
Directora (e) de la Dirección de Protección de
Datos Personales
Ministerio de Justicia y Derechos Humanos

²⁵ Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS
"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."