Resolución Directoral N° 2154 -2019-JUS/DGTAIPD-DPDP

Expediente N°
108-2018-JUS/DGTAIPD-PAS

Lima, 06 de agosto de 2019

VISTOS:

El Informe Nº 041-2019-JUS/DGTAIPD-DFI del 16 de abril de 2019[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), junto con los demás documentos que obran en el respectivo expediente; y,

CONSIDERANDO:

I. Antecedentes

1. Por medio del formulario ingresado el 17 de julio de 2018[2], el señor Miguel Enrique Morachimo Rodríguez (en adelante, el denunciante), presentó una denuncia contra la Oficina Nacional de Procesos Electorales - ONPE (en adelante, la administrada) por presuntas infracciones a le Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP), detallando lo siguiente:

- La administrada habría distribuido públicamente sus datos personales (nombres, apellidos, fecha de nacimiento, sexo y condición de mayoría de edad) a través de dos direcciones web alojadas en el sitio web www.hackathon.pe, a través de la cual se permite la descarga de cualquier ciudadano mayor de edad, así como la descarga masiva de números de DNI correlativos; lo cual descubrió el 8 de junio de 2018 al acceder a dicho sitio web
- Dicho acceso a datos personales se efectúa sin necesidad de vulnerar ninguna medida de seguridad y desde cualquier computadora, con el solo llenado del campo de información asignado al documento de identidad, que habilitaba el autocompletado de los otros campos (nombres, apellidos, sexo y condición de mayoría de edad), lo cual se debía a que el aplicativo web hacia una solicitud pública bajo el método "KEY" hacia un servidor de la administrada, que permitía que con consignar el DNI de cualquier persona, el visitante de dicho sitio web podía visualizar los datos personales del titular de dicho DNI.

Dirección de Protección de Datos Personales
M. GONZALEZ

[1] Folios 474 al 885
[2] Folios 1 al 47

- Dicho método de obtención estuvo activo entre el 8 y el 15 de junio de 2018, luego de lo cual se cambio al método "POST", el cual impedía que los datos fueran accesibles a simple vista.
- Según se aprecia en el video que adjuntó el denunciante, así como en la constatación notarial del 18 de junio de 2018, se podía acceder también a través de la web pública de dicho sitio web, en interfase HTML, modificando el componente del dominio (www.hackathon.pe/hackathon_ve/person/[DNI]) correspondiente al número de DNI, que arrojaba datos personales del titular del mismo, accediendo por este medio a la edad de este.
- Así también, tal como evidencia en el mencionado video y la constatación notarial mencionada, se aprecia la posibilidad de descargar los datos de una pluralidad de personas, a un archivo Excel.
- El 19 de julio de 2018 se remitió un reporte detallado al Jefe de la administrada, luego de lo cual, el 20 de junio de 2018, el formulario del sitio web señalado ya no efectuaba operaciones de llenado automático.
- Los datos personales también eran accesibles desde la página web de la "Hackathon 2017", página web que fue desactivada luego de haberse reportado tal situación.
- Tales hechos implicaban infracciones a los principios de Consentimiento, de Proporcionalidad y de Seguridad, al permitir la administrada el acceso a los datos personales contenidos en el Padrón Electoral sin el consentimiento de los titulares ni teniendo norma habilitante, sin que dicho tratamiento sea necesario ni proporcional para la inscripción en la "Hackathon 2018", y sin establecer medidas de seguridad que impidan el acceso no autorizado a los datos personales, suscitándose una situación de vulnerabilidad de los datos personales.
- Las medidas de seguridad no implementadas, se encuentran previstas en la Directiva de Seguridad aprobada por la Dirección General de Protección de Datos Personales, tratándose el caso de la administrada un banco de datos personales de nivel crítico, que requería la asignación de contraseñas a los usuarios del formulario.

2. El escrito de la denuncia adjuntó un CD con un vídeo en el cual se puede apreciar el proceso en el que el usuario de la mencionada página web puede acceder a datos personales ajenos, con solo el número del DNI de la persona (como en el caso de los datos del Presidente de la República, Martín Vizcarra Cornejo, así como de otras personas mayores de edad), así como, mediante el uso de la aplicación "Inspector Web" del navegador, se puede acceder a datos personales de múltiples personas, en interfaz HTML y con la posibilidad de obtener un listado con sus respectivos datos personales.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALES

3. Así también, el denunciante adjuntó a su escrito constataciones notariales del 18 de junio de 2018, de los procedimientos señalados[3].

4. Mediante la Orden de Visita de Fiscalización N° 85-2018-JUS/DGTAIPD-DFI[4], la DFI dispuso la realización de una visita de fiscalización a la administrada, en su domicilio del Jr. Washington N° 1894, Lima.

5. En la primera visita de fiscalización del 1 de agosto de 2018, según lo consignado en el Acta de Fiscalización N° 01-2018[5], se verificó que el sitio web www.hackathon.pe contenía un formulario para el registro de participantes en la página web www.hackathon.pe/hackathon_ve, el mismo que utilizó el servicio web de consulta proporcionado por el Registro Nacional de Identificación y Estado Civil (en adelante, Reniec), el cual contenía los registros de 28 405 444 personas; dicha página web fue

[3] Folios 23 al 33
[4] Folio 61
[5] Folios 62 al 67

cambiada el 20 de junio de 2018 debido a un aviso anónimo de vulnerabilidad, estando a la fecha inactiva.

6. Durante dicha visita se hizo entrega al personal fiscalizador de los formatos "Pase a Producción de un Producto Software" del 7 de junio de 2018[6] y del 20 de junio de 2018[7], en los cuales se detalla los cambios realizados al mencionado sitio web, así como la constancia de datos personales que retorna el servicio web de dicho sitio web, al momento del registro de cada participante[8].

7. Por medio del Oficio N° 501-2018-JUS/DGTAIPD-DFI[9], se informa que la segunda visita de fiscalización a la administrada se programa para el 14 de agosto de 2018.

8. Durante dicha visita de fiscalización, según lo consignado en el Acta de Fiscalización N° 02-2017[10], se verificó que la administrada recibe trimestralmente de Reniec una base de datos denominada "Padrón Trimestral", conteniendo datos personales de 949 361 personas, a fin de actualizar el padrón electoral, en mérito del artículo 214 de la Ley N° 26859, Ley Orgánica de Elecciones.

9. Se adjuntó a dicha acta la "Cartera de Proyectos" de la administrada, que es el resultado del histórico de proyectos emprendidos para el cumplimiento de sus planes operativos institucionales; así también, los informes concernientes a la entrega del "Padrón Trimestral".

10. Mediante el Informe N° 196-2018-DFI-VARS[11], el Analista de Fiscalización en Seguridad de la Información de la DFI señaló respecto de la administrada lo siguiente:

- Tiene debidamente documentados los procedimientos de gestión de accesos, gestión de privilegios y revisión periódica de privilegios asignados.
- No ha implementado las medidas de seguridad suficientes para el proceso de inscripción del evento "Hackathon 2018", permitiendo el acceso no autorizado al servicio de consulta web del Reniec que contiene información de 28 405 444 personas.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

11. Por medio del Informe de Fiscalización Nº 143-2018-JUS/DGTAIPD-DFI-AARM del 28 de septiembre de 2018[12], se puso en conocimiento de la DFI los resultados de la fiscalización adjuntando las actas de fiscalización, así como los demás anexos y documentos que conforman el respectivo expediente administrativo.

12. El 28 de enero de 2019, la DFI accedió al Registro Nacional de Protección de Datos Personales (en adelante RNPDP), verificando que la administrada tiene los siguientes bancos de datos personales inscritos:

- "Aportantes a Organizaciones Políticas, Candidatos y Parlamentarios de las Elecciones Generales 2011"
- "Personas Involucradas en Demandas Legales"
- "Electores que Figuras en los Padrones Electorales"
- "Personal"
- "Atención al Ciudadano"

[6] Folios 83 al 85
[7] Folio 90
[8] Folios 86 al 88
[9] Folio 103
[10] Folios 108 al 112
[11] Folios 169 al 171
[12] Folios 172 al 177

- "Videovigilancia"

13. Mediante la Resolución Directoral N° 014-2019-JUS/DGTAIPD-DFI del 31 de enero de 2019[13], la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la presunta comisión de las siguientes infracciones:

- Realizar el tratamiento de los datos personales del Padrón Electoral (DNI, nombres, apellidos, calidad de mayor de edad y sexo) proporcionado por el Reniec, para una finalidad distinta de aquella que motivó su recopilación, incumpliendo con la obligación establecida en los artículos 6, 7, 8 y el numeral 4 del artículo 28 de la LPDP, lo que configuraría la infracción grave tipificada en el literal e) del numeral 2 del artículo 132 del Reglamento de la LPDP, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, Reglamento de la LPDP), esto es, *"utilizar los datos personales obtenidos lícitamente para finalidades distintas de aquellas que motivaron su recopilación, salvo medie procedimiento de anonimización o disociación"*.
- No inscribir en el RNPDP el banco de datos personales de contactos de la entidad, incumpliendo con lo establecido en el artículo 78 del Reglamento de la LPDP, lo que configuraría la infracción leve tipificada en el literal e) del numeral 1 del artículo 132 del dicho reglamento, esto es, *"no inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*.
- No haber implementado las medidas de seguridad suficientes para el proceso de inscripción en el evento "Hackathon 2018" a través de su página web, permitiendo presumiblemente el acceso no autorizado al servicio de consulta web de datos personales que contiene un registro de 28405444 personas, incumpliendo con la obligación establecida en el artículo 16 de la LPDP; situación que configuraría la infracción leve tipificada en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es, *"realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"*.

14. Dicha Resolución Directoral fue notificada a la administrada el 5 de febrero de 2019, a través del Oficio N° 99-2019-JUS/DGTAIPD-DFI[14].

15. A través de la comunicación ingresada con la Hoja de Trámite N° 13891-2019 del 26 de febrero de 2019[15], la administrada presentó sus descargos, alegando lo siguiente:

- En el marco de la implementación gradual del voto electrónico como parte de su política institucional y para el cumplimiento de su función vinculada a la organización de procesos electorales, realizó el "Hackathon 2018", dirigido a la búsqueda de nuevas tecnologías para el proceso electoral regional y municipal 2018 tal como se puede apreciar en las recomendaciones emitidas por su Gerencia de Informática y Tecnología Electoral, no siendo una actividad aislada o una simple capacitación.
- Por medio del sitio web no se consultó el Padrón Electoral, sino a un contenedor alterno, cuyo tratamiento se agotó con la vigencia de la inscripción al mencionado evento.
- La denuncia hace referencia a información en texto plano con datos que no corresponde a detalle y formato que recoge el Padrón Electoral ni al servicio web del Reniec.
- En el informe del analista de fiscalización en seguridad se menciona el supuesto uso de datos personales de 28 405 444 personas mayores de edad, sin haber indicado en el acta de fiscalización correspondiente el medio con el cual se determina el uso

[13] Folios 185 al 191
[14] Folio 193
[15] Folios 194 al 360

del servicio web del Reniec, siendo más bien que se declaró al personal fiscalizador que el servicio web de la "Hackathon 2018" es de la misma administrada.

- De forma previa al inicio del procedimiento sancionador, obtuvieron la inscripción del banco de datos personales "Participantes a la Hackathon ONPE 2018", habiéndose solicitado el 21 de diciembre de 2018.
- El servicio web no es un servicio implementado específicamente para la "Hackathon 2018", ni contiene los datos de 28 405 444 personas, sino que es una interfase intermedia que, por medio de un *token* y una clave de validación con los cuales el servicio web obtiene la autenticación con el método KEY, lo cual efectúa en cada petición que se realiza poniendo como requerimiento un número de DNI, para que luego el servicio revise las credenciales del mencionado token para garantizar el acceso válido al sistema, con lo cual arroja los datos necesarios para el registro.
- Para la interpretación del código HTML y su manipulación, se requiere un perfil técnico basado en programación para la capa de presentación hacia el usuario final.
- Al haber tomado conocimiento del reporte del denunciante, se modificó el método de autenticación al método POST, el cual no muestra la información del usuario, sino que permite continuar el proceso de inscripción una vez que verificó la validez del DNI y la mayoría de edad.
- El esquema de base de datos "HACKATHON-VE" no tiene privilegios de acceso a ninguna base de datos ni al Padrón Electoral; a través del servicio web solo se accedió a un contenedor con los siguientes datos de las personas mayores de edad: Apellido paterno, apellido materno, nombres, DNI, fecha de nacimiento y sexo, según se informó a través del Memorando N° 000454-2019-GITE/ONPE.
- Cuentan con equipos para la denegación de servicio, con lo que se evita los ataques masivos desde un solo origen, así como estadísticas en las que no se evidencia consultas masivas o indiscriminadas, ni un comportamiento anómalo consistente en más de 5000 concurrencias simultáneas.
- Entre otras medidas de seguridad, han implementado un equipamiento DoS (para denegatoria de servicio) contra consultas múltiples desde una dirección IP, protección contra ataques de código malicioso a través del equipamiento IPS y un equipo *Firewall*, los que permiten mitigar los riesgos informáticos, propios de los avances tecnológicos.
- En el Informe N° 000085-2019-SGIID-GITE/ONPE, se detallaron las pruebas funcionales y no funcionales realizadas para validar el funcionamiento, tales como las pruebas de integridad a los datos, de la interfaz de usuario, de regresión, de integración y de validaciones.
- El desarrollo de la "Hackathon 2018" trajo diversos beneficios tales como el incremento de la familiaridad en el uso de soluciones tecnológicas electorales, la promoción del voto electrónico presencial, el fomento de la transparencia respecto de dicho procedimiento que permitieron que se identifiquen sus debilidades, riesgos o mejoras.
- El acceso efectuado por el denunciante a través de la página web de la "Hackathon 2018" a la información, así como otras actividades de manipulación, no ha sido autorizado por ninguna autoridad, así como tampoco las pruebas realizadas.

16. Mediante el Oficio N° 195-2019-JUS/DGTAIPD-DFI, la DFI dio fecha para el informe oral solicitado por la administrada para hacer uso de la palabra, así como se le requirió documentos que evidencien la implementación de medidas de seguridad contra consultas múltiples, ataques maliciosos, así como evidencias de que para el uso de la página web del "Hackathon 2018", no hubo consultas al Padrón Electoral ni al servicio web del Reniec.

17. El mencionado informe oral tuvo lugar el 15 de marzo de 2019.

18. A través del escrito ingresado con la Hoja de Trámite N° 20305-2019 del 21 de marzo de 2019[16], la administrada remitió documentación solicitada por medio del Informe N° 195-2019-JUS/DGTAIPD-DFI, que incluye contratos de adquisición de diversos medios de seguridad para la página web del "Hackathon 2018".

19. En el Informe Técnico N° 053-2019-DFI-VARS[17], el Analista de Fiscalización en Seguridad de la Información de la DFI, concluyó que la administrada habría implementado medidas de seguridad necesarias para la página web del "Hackathon 2019".

20. Por medio de la Resolución Directoral N° 61-2019-JUS/DGTAIPD-DFI del 16 de abril de 2019[18], la DFI, siguiendo lo establecido en el artículo 122 del Reglamento de la LPDP, cerró la etapa instructiva del presente procedimiento administrativo sancionador.

21. A través del Informe N° 041-2019-JUS/DGTAIPD-DFI del 16 de abril de 2019[19], la DFI remitió a la DPDP el expediente del presente caso, recomendando archivar las tres imputaciones efectuadas por medio de la Resolución Directoral Nº 014-2019-JUS/DGTAIPD-DFI.

22. Mediante el escrito ingresado con la Hoja de Trámite N° 32848-2018 del 9 de mayo de 2019[20], la administrada manifestó su conformidad con las conclusiones del Informe N° 041-2019-JUS/DGTAIPD-DFI y reiteró los principales argumentos de sus descargos.

Perú Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

II. Competencia

23. 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.

24. 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. Primera cuestión previa: Sobre las normas relativas a la exención y atenuación de la responsabilidad administrativa

25. 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, aprobado por Decreto Supremo N° 004-2019-JUS (en adelante, 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 cargos[21].

---

[16] Folios 468 al 46
[17] Folios 468 al 469
[18] Folios 470 al 472
[19] Folios 474 al 484
[20] Folios 485 al 534
[21] **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."

26. Es conveniente delinear el concepto de la subsanación contemplado en dicha disposición de la LPAG, empezando por señalar que esta no elimina el carácter antijurídico de la conducta del infractor, sino que actúa sobre la responsabilidad derivada de la comisión del ilícito correspondiente, vale decir, de la obligación de dicho infractor consistente en responder por ello, asumiendo una consecuencia jurídica como es la sanción y la reparación del daño causado.

27. En tal sentido, la subsanación implica no solo efectuar una conducta que cese con el incumplimiento de una determinada norma u obligación impuesta, sino que, en los casos de incumplimientos donde se afecten los derechos de una persona o se crea una situación de inminente riesgo para estos, se pueda revertir tales efectos dañosos y resarcirlos, como señala Morón Urbina[22].

28. También es preciso reconocer que los hechos infractores en cada caso, por su naturaleza y circunstancias específicas, pueden significar un daño efectivo a los derechos de las personas o la puesta en riesgo de las mismas, variando por ello la posibilidad de su subsanabilidad, cuando incluso suprimiéndola no pueda revertirse la situación, al agotarse los efectos del comportamiento ilícito.

29. En estos supuestos, se debe atender a lo dispuesto en el artículo 126 del Reglamento de la LPDP[23], leído conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG[24], referentes a las acciones de enmienda, en virtud de las cuales se acogen 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.

30. La aplicación de los mencionados atenuantes se evaluará tomando en cuenta las fórmulas de enmienda, su oportunidad y la factibilidad de estas para eliminar las condiciones en las que se desarrolle las situaciones ilícitas (ya sean las de consumación instantánea y/o las de merca actividad riesgosa), conjuntamente con el reconocimiento expreso de la responsabilidad; factores con los que puede proceder la reducción motivada de la sanción por debajo del rango previsto en la LPDP.

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

31. 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] MORÓN URBINA, Juan Carlos: "Comentarios a la Ley del Procedimiento Administrativo General". Décimo segunda edición. Lima, Gaceta Jurídica, 2017, tomo II, p. 513.

[23] **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"

[24] **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."

39. Por su parte, el artículo 8 de la LPDP contempla el principio de Calidad, con la siguiente redacción:

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

40. En virtud de dichos principios, la LPDP establece la siguiente obligación:

> **"Artículo 28. Obligaciones**
> El titular y el encargado de tratamiento de datos personales, según sea el caso, tienen las siguientes obligaciones:
> (...)
> 4. No utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación."

41. En tal sentido, el tratamiento adecuado de datos personales debe realizarse con el fin de alcanzar finalidades determinadas, explícitas y lícitas, debiendo guardar proporcionalidad y conservar la pertinencia y utilidad del tratamiento de los datos personales respecto de cada una de aquellas finalidades.

42. En el presente caso, se imputó a la administrada haber utilizado los datos personales que el Reniec le remite para su Padrón Electoral, en una finalidad distinta, como es el uso en la página web del "Hackathon 2018" para el registro de sus participantes.

43. En sus descargos, la administrada alegó que dicho evento se encuentra dentro del cumplimiento de sus funciones como entidad a cargo de los procesos de elecciones generales, estando prevista en su Plan Operativo Institucional la realización de mejoras para el prototipo de voto electrónico y recibir iniciativas de innovación tecnológica y transformación digital de dicho proceso.

44. Para este caso, es pertinente revisar las funciones de la administrada previstas en el artículo 5 de la Ley N° 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales (en adelante, LO-ONPE), transcrito a continuación:

> **"Artículo 5.-** Son funciones de la Oficina Nacional de Procesos Electorales:
> a) Organizar todos los procesos electorales, del referéndum y otras consultas populares.
> (...)
> q) Ejercer las demás atribuciones relacionadas con su competencia."

45. También resulta necesario el conocimiento del articulado de la Ley N° 26859, Ley Orgánica de Elecciones (en adelante, LOE), que tiene previsto lo siguiente:

> **"Artículo 37.-** La Oficina Nacional de Procesos Electorales tiene a su cargo la organización y la ejecución de los Procesos Electorales y consultas populares. Ejerce sus atribuciones y funciones con sujeción a la Constitución, la presente Ley y su Ley Orgánica.

> **Artículo 204.-** Se agregan al padrón electoral las inscripciones observando rigurosamente el ordenamiento por distritos, provincias y departamentos. Asimismo, se eliminan, en forma permanente, las inscripciones que sean canceladas o las excluidas temporalmente.
> El Registro Nacional de Identificación y Estado Civil remitirá trimestralmente, al Jurado Nacional de Elecciones y a la Oficina Nacional de Procesos Electorales, la relación de inscripciones agregadas o eliminadas del Padrón Electoral a nivel nacional, relación que deberá contener los mismos datos e imágenes que se consignan en el Padrón Electoral conforme al artículo 210 de la presente Ley."

46. De las normas precitadas, se tiene que las actividades de tratamiento de datos personales y de índole general que realiza la administrada, tienen relación con la función involucrada con el desarrollo de procesos electorales, abarcando el ámbito logístico de los mismos, lo cual implica el desarrollo de dispositivos con los cuales el ciudadano pueda ejercer su voto.

47. Se debe tener en cuenta que el artículo 5 de la LO-ONPE, contiene en su literal q) una cláusula que permite efectuar otras actividades que, indirectamente, permitan el cumplimiento de sus funciones, como la implementación, desarrollo o mejora de sistemas de votación.

48. Sobre el Padrón Electoral, sobre el cual también actúa la administrada, debe señalarse que sirve para el empadronamiento de los ciudadanos habilitados para participar en cada proceso electoral, lo cual delata el vínculo de su finalidad con el desarrollo de procesos electorales.

Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

49. En el presente caso, se aprecia que la administrada, con la finalidad de facilitar el registro de los participantes del "Hackathon 2018" a través de su página web, permitió el acceso al soporte anexo al Padrón Electoral ("servicio web", de titularidad propia) que contenía algunos de los datos incluidos en dicho padrón, suficientes para verificar la identidad y la mayoría de edad de los participantes.

50. Al respecto, esta dirección aprecia que el acceso a los datos personales contenidos en dicho soporte anexo fueron utilizados únicamente para la inscripción en el "Hackathon 2018", cuya finalidad es obtener mejoras y nuevos prototipos para el sistema de voto electrónico presencial para las Elecciones Regionales y Municipales 2018, lo cual es una actividad involucrada con el desarrollo de los procesos electorales, que es una de las funciones legalmente encomendadas a la administrada.

51. Por tales motivos, se entiende que la utilización de los datos personales derivados del Padrón Electoral, son utilizados para una finalidad lícita, explícita y conocida, como es el desarrollo de los procesos electorales, función a cargo de la administrada; pues si bien tienen constituyen modalidades distintas al momento de realización de las inscripciones en la "Hackathon 2018" (almacenamiento, por un lado, y uso para inscripciones, por otro), ambas siguen la finalidad señalada como la principal, debiendo reconocer que una contribuye a ella de forma más directa que la otra actividad.

52. En tal sentido, la imputación por la presunta comisión de la infracción grave tipificada en el literal e) del numeral 2 del artículo 132 del Reglamento de la LPDP debe declararse infundada, procediendo con su archivo.

Sobre el deber de inscribir los bancos de datos personales ante el Registro Nacional de Protección de Datos Personales

53. El artículo 78 del Reglamento de la LPDP establece el carácter obligatorio de la inscripción en el mencionado registro de los bancos de datos personales que las entidades generen:

> **"Artículo 78.- Obligación de inscripción.**
> Las personas naturales o jurídicas del sector privado o entidades públicas que creen, modifiquen o cancelen bancos de datos personales están obligadas a tramitar la inscripción de estos actos ante el Registro Nacional de Protección de Datos Personales.
> (...)"

54. En el presente caso, se imputó como hecho infractor que la administrada no había cumplido con inscribir en el RNPDP el banco de datos personales de contactos de la entidad, derivado del tratamiento efectuado a través de la página web del "Hackathon 2018".

55. En sus descargos, la administrada señala que la información contenida en el soporte alterno ("servicio web") desde donde se extraían los datos para el registro en dicha página web, contenía datos de los electores que ya estaban almacenados en el Padrón Electoral.

56. Sobre ello, y de acuerdo con las constataciones efectuadas, esta dirección debe señalar que los datos a los que se accede a través de la página web, aún cuando no se accede directamente al Padrón Electoral, son los mismos presentes en dicho soporte principal, siendo el "servicio web" solo una copia de los mismos.

57. Debe señalarse también que, si bien es cierto que desde el 20 de junio de 2018, la administrada cambia el formulario de la página web de la "Hackathon 2018" del método de obtención de datos "KEY" (que implicaba el autocompletado del formulario) al método "POST" (que solo implica el cotejo del número del DNI para validar la identidad del usuario, dejando que este complete sus datos), tal situación no implicó la recopilación de datos diferentes a los que se encuentran en el Padrón Electoral.

58. Debe entenderse entonces que la administrada ya cuenta con un banco de datos personales inscrito para los contactos inscritos por medio de la página web del "Hackathon 2018", que es el de "Electores que Figuran en el Padrón Electoral", por lo que no corresponde exigir la inscripción de un banco de datos personales que cumple con la misma función.

59. En tal sentido, se halla que la imputación efectuada por este punto debe ser declarada infundada, debiendo proceder con su archivo.

Sobre el incumplimiento de las disposiciones reglamentarias referidas a las medidas de seguridad y la contravención al principio de Seguridad de la LPDP

60. El Título I de la LPDP establece los principios rectores para la protección de datos personales, entre ellos el principio de Seguridad, regulado en el artículo 9 de dicha ley:

> **"Artículo 9. Principio de seguridad**
> El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser

apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate."

61. Por su parte, el artículo 16 de la misma ley tiene los siguientes términos:

> **"Artículo 16. Seguridad del tratamiento de datos personales**
> Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
> Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.
> Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo."

62. Este artículo, que desarrolla las principales acciones a realizar a fin de cumplir con el principio de Seguridad, establece dos tipos de objetivos de la adopción de medidas técnicas, organizativas y legales de seguridad: El objetivo general, que es la garantía de la seguridad de los datos personales, y el objetivo específico, que son las acciones a través de las cuales se concreta tal garantía, consistentes en evitar la alteración, pérdida, tratamiento o acceso no autorizado a la información custodiada.

63. Debe entenderse entonces que la garantía de seguridad implica la implementación de medidas que prevengan los tratamientos de datos personales no deseados y otros incidentes que afecten la integridad, confidencialidad y disponibilidad de la información personal, vale decir, que el responsable del tratamiento de los datos esté en la posibilidad de evitar que tales hechos no sucedan.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

64. En tal sentido, el incumplimiento de la obligación contenida en el artículo transcrito puede implicar tanto la puesta en riesgo continua de la integridad, confidencialidad y disponibilidad de los datos personales en carencia de garantía para la seguridad (infracción continua), como la vulneración instantánea y concreta de la seguridad en un episodio específico (infracción instantánea).

65. En el presente caso, el denunciante señala que a través del sitio web de la "Hackathon 2018", cualquier usuario, escribiendo en el formulario un número de cualquier DNI, podía acceder a información de su titular en su interfaz principal, lo cual fue corregido el 20 de junio de 2018, así como, por medio de la interfaz HTML de la web pública de la búsqueda de cada titular de DNI (a través de la página web www.hackathon.pe/hackathon_ve/person) y a través de la aplicación "Inspector Web".

66. Como pudo sustentar el denunciante, con el mencionado sitio web, así como a través de su interfaz HTML, se tuvo una herramienta que, con solo el número de DNI, permitía que cada usuario que hiciera uso del formulario que incluía, pueda acceder a la información de cada titular de documento de identidad, situación que representa la consumación de la permisión del acceso no autorizado.

67. En el presente caso, se evidencia por un lado, el acto concreto de acceso no autorizado que afecta la confidencialidad de los datos personales de ciudadanos votantes; y por otro la carencia de medidas de seguridad, que permite se concrete la situación de daño mencionada, en el período del 8 al 20 de junio de 2018, durante el cual la administrada no garantiza la confidencialidad de los datos personales contenidos en el "servicio web" de forma general, suscitándose una situación de riesgo permanente para ellos.

68. En el primer supuesto, el acceso no autorizado se perfecciona con la exhibición de la información accedida que permitía el método "KEY", lo cual sucedía una vez que se remitía el DNI a través del formulario; dicha situación implica una configuración instantánea del daño consistente en el acceso no autorizado, permitido a través de la interfaz del sitio web, así como de su formato HTML desplegado, sobre el cual no hay posibilidad de reversión a un estado anterior al aludido daño.

69. No sucede lo mismo con el supuesto de falta continua de garantías de seguridad, pues el mantenimiento de dicha situación riesgosa, donde tiene lugar cada concreción del supuesto anterior, puede ser objeto de cese y reversión a un estado de inexistencia del riesgo, por medio de la implementación de las medidas de seguridad necesarias para el tratamiento, o el cese del mismo.

70. Para este segundo caso, la administrada procedió con la implementación de dispositivos de seguridad tales como la implementación de sistemas de prevención de intrusos y códigos maliciosos dentro del tráfico normal de red, *firewall* contra accesos no autorizados para direcciones IP específicas que hagan solicitudes múltiples y configure un límite para conexiones concurrentes externas.

71. Dichas implementaciones demuestran que la administrada habría cumplido con implementar medidas que garanticen la seguridad de los datos personales materia de tratamiento, sobretodo contra el acceso excesivo a su página web que exceda su funcionamiento y contra solicitudes múltiples a la misma que representen una amenaza para la confidencialidad de los datos personales.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

72. Posteriormente, la administrada, al finalizar el período de inscripción a la "Hackathon 2018", procedió con el cese del uso de la página web y con ello, con el uso del mencionado formulario y del plano HTML, en el cual también podía visualizarse los datos personales contenidos en el "servicio web".

73. En tal sentido, se tiene que, la situación de falta de garantías para la seguridad, que implica la situación de riesgo de acceso no autorizado terminó siendo enmendada con el cese del tratamiento, la cual no alcanza como enmienda del hecho dañoso constituido con el acceso no autorizado que se concretó.

74. Es preciso tener en cuenta que, al cesar la falta de garantías para la seguridad de la información, ya no existe el escenario para los accesos no autorizados, por lo que las acciones efectuadas por la administrada solo pueden considerarse como enmiendas o reversiones de la situación de carencia de dichas garantías.

75. Por ello, para la infracción imputada por el incumplimiento de la disposición del artículo 16 de la LPDP, tales medidas no conllevan a la subsanación de la misma, sino solo su enmienda, pues no corrigen los efectos del acceso no autorizado evidenciado, por lo que en su caso, debe calificarse el hecho como una acción de enmienda, aplicándose sobre la responsabilidad administrativa lo establecido en el artículo 126 del Reglamento de la LPDP.

76. En consecuencia, la administrada es responsable por la comisión de la infracción leve tipificada en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP, debiendo atenuarse su responsabilidad administrativa en mérito de las disposiciones del artículo 126 de dicho reglamento.

Sobre la determinación de la sanción

77. 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.

78. 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[25], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[26].

79. En el presente caso, se ha establecido la responsabilidad de la administrada por no haber implementado las medidas de seguridad suficientes para el proceso de inscripción en el evento "Hackathon 2018" a través de su página web, permitiendo presumiblemente el acceso no autorizado al servicio de consulta web de datos personales que contiene un registro de 28405444 personas, incumpliendo con la obligación establecida en el artículo 16 de la LPDP; situación que configuraría la infracción leve tipificada en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP sancionable con una multa de entre cero coma cinco (0,5) y cinco (5) unidades impositivas tributarias, de acuerdo con lo establecido en el artículo 39 de dicha ley.

80. 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 las conductas sancionables 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.

Ministerio de Justicia y Derechos Humanos PERÚ
Dirección de Protección de Datos Personales
M. GONZALEZ L.

81. 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.

---

[25] **Ley N° 29733, Ley de Proteccion 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)."

[26] **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."

b) La probabilidad de detección de la infracción:

La infracción pudo ser verificada a través de la visita de la página web correspondiente, así como con el uso de la herramienta "Inspector Web" con el que cuentan los programas de navegación en Internet.

Sin embargo, debe examinarse también que la implementación o no de las medidas de seguridad que impidan los accesos no autorizados implica un examen de los procedimientos técnicos al interior de la administrada, lo cual se realiza a través de las fiscalizaciones y requerimientos de información.

En tal sentido, la probabilidad de detección de la infracción es media.

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

Las infracciones detectadas afectan 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.

El incumplimiento de las disposiciones del artículo 16 de la LPDP en el presente caso, implicó tanto la generación de situación riesgosa que restó garantías para la confidencialidad de los datos personales tratados y posibilitó, en dicho entorno, la concreción de accesos no autorizados cuyo efecto dañoso tiene efecto no reversible.

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 las infracciones:

La administrada no fue sancionada anteriormente por la infracción.

f) Las circunstancias de la comisión de las infracciones:

En este punto, es preciso valorar el reducido lapso en el que la situación infractora pudo tener lugar, entre el 8 y el 20 de junio de 2018, así como la aplicación de medidas correctivas para detener la situación riesgosa a través del cambio del método de inscripción en la página web, debiendo considerar también la implementación de otros dispositivos lógicos que, si bien no se aplican directamente a las concretas permisiones de accesos no autorizados por las que se sanciona a la administrada, previenen otros incidentes o posibles vulneraciones.

En tal sentido, habiendo existido una situación de riesgo en la que se permitió el acceso no autorizado a los datos personales de todas las personas inscritas en el Padrón Electoral (al ser el "servicio web" un soporte que solo toma ciertos datos de todos sus registros), corresponde en este caso calificar la adopción de las medidas de seguridad como acciones de enmienda que atenúan la responsabilidad de la administrada, de acuerdo con el artículo 126 del Reglamento de la LPDP.

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

Si bien, por los numerosos registros de personas que se manejan a través del "servicio web" y del Padrón Electoral, es exigible a la administrada una diligencia aún mayor a la ordinaria, se aprecia que sí pudo adoptar mayores previsiones y

exámenes constantes de tales medidas, evidenciándose su intención conducente a evitar vulneraciones a la confidencialidad de los datos.

82. 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 en el considerando 81 de la presente resolución directoral.

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 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses aprobado por Decreto Supremo N° 019-2017-JUS;

SE RESUELVE:

Artículo 1.- Declarar infundada la imputación efectuada mediante la Resolución Directoral Nº 014-2019-JUS/DGTAIPD-DFI contra la Oficina Nacional de Procesos Electorales – ONPE, por la supuesta comisión de la infracción grave tipificada en el literal e) del numeral 2 del artículo 132 del Reglamento de la LPDP.

Artículo 2.- Declarar infundada la imputación efectuada mediante la Resolución Directoral Nº 014-2019-JUS/DGTAIPD-DFI contra la Oficina Nacional de Procesos Electorales – ONPE, por la supuesta comisión de la infracción grave tipificada en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

Artículo 3.- Sancionar a la Oficina Nacional de Procesos Electorales – ONPE con la multa ascendente a una unidad impositiva tributaria (1 UIT), por el incumplimiento de las disposiciones del artículo 16 de la LPDP, vulnerando el principio de Seguridad, al no garantizar la seguridad de los datos personales de los votantes, permitiendo el acceso no autorizado, infracción leve tipificada en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP.

Artículo 4.- Informar a Oficina Nacional de Procesos Electorales – ONPE 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 notificación[27].

Artículo 5.- Informar a Oficina Nacional de Procesos Electorales – ONPE 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 entiende que se cumple con pagar la multa impuesta, si antes de que venza el plazo establecido en el requerimiento de pago, se cancela el 60% de la multa impuesta, de conformidad con lo dispuesto en el artículo 128 del Reglamento de la LPDP[28].

---

[27] **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 a 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."

[28] **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

Artículo 6.- Notificar a Oficina Nacional de Procesos Electorales – ONPE la presente resolución directoral.

Artículo 7.- Notificar al señor Miguel Enrique Morachimo Rodríguez la presente resolución directoral.

Regístrese y comuníquese.

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

MAGL/rvr

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."