# INFORME JURÍDICO N.° 020-2024-JUS/DGTAIPD

A : **Juan Enrique Alcántara Medrano**
Viceministro de Justicia

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

ASUNTO : Opinión sobre Proyecto de Ley que protege a los consumidores de servicios financieros del manejo indebido de su información personal que disponen las centrales privadas de riesgo y las billeteras digitales

REFERENCIA : a) Oficio PO N.º 320-2023-2024-CODECO/CR
b) Proyecto de Ley N.º 7919/2023-CR

FECHA : 28 de agosto de 2024

---

## I. ANTECEDENTES

1. Por medio del Oficio P.O N.º 320-2023-2024/CODECO-CR, el Presidente de la Comisión de Defensa del Consumidor y Organismos Reguladores de los Servicios Públicos del Congreso de la República solicitó al Ministerio de Justicia y Derechos Humanos (en adelante, MINJUSDH), la emisión de opinión técnica institucional del Proyecto de Ley N.º 7919/2023-CR, que propone regular el tratamiento de la información personal de la que disponen las centrales privadas de información de riesgo y los aplicativos móviles de billeteras digitales, con la finalidad de garantizar la protección de la mencionada información y preservar su privacidad (en adelante, el "Proyecto de Ley N.º 7919").

2. Con Proveído N° 5239-2024/JUS-VMJ el Despacho Viceministerial de Justicia del MINJUSDH derivó el Proyecto de Ley a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, DGTAIPD), para su atención de acuerdo con sus competencias.

## II. MARCO NORMATIVO DE ACTUACIÓN

3. En virtud de los artículos 70 y 71 del Reglamento de Organización y Funciones del MINJUSDH corresponde a la DGTAIPD ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP)[1] y la Autoridad Nacional

[1] Decreto Legislativo Nro. 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 gestión de intereses (publicado el 07 de enero de 2017; Decreto Supremo Nro. 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos (publicado

de Protección de Datos Personales (ANPD); por ende, en su calidad de tal, tiene entre sus funciones emitir opinión, a través del presente informe jurídico, respecto de los proyectos de normas que se refieran total o parcialmente a los ámbitos de su competencia.

4. Asimismo, el numeral 11 del artículo 33 de la Ley N.º 29733, Ley de Protección de Datos Personales (LPDP), establece como función de la ANPD, emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la cual es vinculante.

5. En esa medida, esta Dirección General emite el presente Informe Jurídico en el ámbito de la interpretación de las normas en materia de protección de datos personales, de acuerdo al contenido y alcances de la Autógrafa de Ley que propone proteger a los consumidores de servicios financieros del manejo indebido de la información personal de la que disponen las centrales privadas de riesgo y las billeteras digitales.

## III. ANÁLISIS

### *A. Sobre el Proyecto de Ley*

6. El Proyecto de Ley N.º 7919/2023-CR tiene como objeto regular el tratamiento de la información personal de la que disponen las centrales privadas de información de riesgo y la que brindan los aplicativos móviles de billeteras digitales con la finalidad de "garantizar el derecho de las personas a la protección de datos personales, así como, la implementación de medidas de seguridad técnicas y administrativas para evitar el acceso y disposición no autorizado y proteger la confidencialidad de esta información".

7. En ese marco, el artículo 4 de la propuesta señala que las CEPIRS deben incluir protocolos de protección de tratamiento de la información de riesgo, en coordinación con la Superintendencia de Banca, Seguros y AFP y con la ANPD.

8. Asimismo, el artículo 6 de la propuesta enfatiza en el resguardo de la información personal que utilizan los servicios de aplicativos móviles de billeteras digitales.

9. Finalmente, cabe resaltar que la Única Disposición Complementaria Modificatoria del Proyecto de Ley propone modificar la definición de datos sensibles establecida en el artículo 2, numeral 5, de la LPDP, incluyendo como parte de los datos sensibles al documento nacional de identidad, la dirección domiciliaria, el centro de labores, número de teléfono fijo o móvil.

---

el 22 de junio de 2017); y Decreto Supremo Nro. 019-2017-JUS, que aprueba el Reglamento del Decreto Legislativo Nro. 1353 (publicado el 15 de setiembre de 2017).

***B. Sobre las centrales de riesgo***

10. Es pertinente señalar que la Ley N.º 29733, Ley de Protección de Datos Personales (en adelante, LPDP), define a los datos personales en el artículo 2, numeral 4, como "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados".

11. Por su parte, el numeral 19 del citado artículo define al tratamiento de datos personales como "cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales".

12. La Ley N.º 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y Administradora de Fondos de Pensiones (SBS) y sus modificatorias define, en su artículo 158, a las centrales de riesgo como aquel registro financiero, crediticio, comercial y de seguros que tiene información consolidada y clasificada sobre los deudores de las empresas, las cuales, de acuerdo a lo dispuesto en el artículo 159 de la mencionada norma, deben de suministrar periódica y oportunamente la referida información para mantener actualizado el registro y, de contar con sistemas computarizados, proporcionar información diariamente.

13. Asimismo, el artículo 160 de la Ley N.º 26702 dispone que es libre la constitución de personas jurídicas que tengan por objeto proporcionar al público información sobre los antecedentes crediticios de los deudores de las empresas de los sistemas financiero y de seguros y sobre el uso indebido del cheque.

14. Por ello, mediante Ley N.º 27489 se regula las centrales privadas de información de riesgos y de protección al titular de la información (CEPIRS); las cuales, de acuerdo a los artículos 7 y 8 de la referida norma, podrán recolectar información de riesgos para sus bancos de datos, tanto directamente de sus titulares, como de fuentes públicas o privadas sin necesidad de contar con la autorización del titular de la información, entendiéndose que la base de datos se conformará con toda la información de riesgo.

15. En este sentido, la información que en razón de sus funciones poseen las Centrales de Riesgo, en tanto consiste en información real y actualizada de la situación crediticia de las personas que fueron reportadas como deudoras, constituyen datos personales, encontrándose dentro del ámbito de aplicación de la LPDP.

16. Atendiendo a lo anteriormente expuesto, es necesario resaltar que los reportes de información crediticia cumplen un fin constitucional legítimo, de conformidad a lo señalado por el Tribunal Constitucional. Así, en la sentencia recaída en el

Expediente N.º 03700-2010-PHD/TC[2] "(…) resulta legítimo y acorde con el derecho a la libertad de contratación, que exista un flujo continuo de información de riesgo crediticio en el mercado, pues sólo así se puede generar confianza en el sistema financiero para el otorgamiento de créditos y su consiguiente recuperación, en la medida que el tratamiento de este tipo de datos, permite, tanto a personas jurídicas como a personas naturales, conocer el comportamiento en el tiempo de los sujetos de crédito en general (historial crediticio: endeudamiento, capacidad de pago, voluntad de pago), para así tomar decisiones adecuadas en torno al ofrecimiento de créditos, lo cual repercute directamente en la economía nacional (requisitos para el acceso al crédito, tasas de interés, por ejemplo)".

17. En este orden de ideas, el tratamiento que realizan las centrales de riesgo responde a una finalidad constitucionalmente reconocida y, por ende, en sí mismo, no supone una vulneración al derecho fundamental de autodeterminación informativa o derecho de protección de datos, siempre que sea acorde con los principios establecidos en la LPDP.

18. El Proyecto de Ley N.º 7919/2023-CR propone en su artículo 4 que las centrales de riesgo tengan como obligación incluir protocolos de tratamiento de la información de riesgo en coordinación con la Superintendencia de Banca, Seguros y AFP y con la Autoridad Nacional de Protección de Datos Personales.

19. Es pertinente señalar que, estas entidades almacenan información referida al nivel de riesgo crediticio que la persona pudiera tener con el sistema financiero, con lo cual estos datos se encuentran relacionados a la conducta de su titular respecto al cumplimiento de alguna obligación o deuda con una empresa, incluyendo información sobre si los saldos de la deuda contraída se encuentran al día o si muestran algún nivel de morosidad.

20. Así, que las centrales de riesgo elaboren protocolos de seguridad en el tratamiento de los datos personales, constituiría una medida adecuada, necesaria y proporcional atendiendo a sus fines.[3] Es adecuada, porque responde a criterios de responsabilidad proactiva, es decir, la existencia del protocolo anticipará escenarios de riesgo a la privacidad de la información crediticia desde el diseño y por defecto, así como la evaluación de impacto de los posibles riesgos. Además, es necesaria, porque este permitirá garantizar un tratamiento seguro de los datos personales al determinar de manera específica las medidas técnicas, legales y organizativas que las centrales de riesgo deberán implementar para la protección de la información personal; y, por último, resulta proporcional porque la existencia del protocolo sirve como medio para que las centrales de riesgo acrediten el cumplimiento de la normativa de protección de datos y, en consecuencia, evidencien la satisfacción o cumplimiento del objeto del derecho constitucional de autodeterminación informativa.

[2] Fundamento jurídico N° 6.
[3] Algo que, de por sí, se estima que ya ocurre porque la exigencia de adoptar medidas de seguridad en el tratamiento de datos personales deriva ya de la LPDP y su reglamento.

21. Por ello, este despacho considera positivo que se remarque legalmente la obligación de que las centrales de riesgo elaboren protocolos, específicamente de seguridad, para el tratamiento de datos personales; como ya genéricamente lo hace la LPDP (artículos 9, 16, 17) y su reglamento (artículos 39 y siguientes), además de la vigente Directiva de Seguridad para el Tratamiento de Datos Personales.[4]

22. Sin embargo, es pertinente advertir que la elaboración de protocolos de seguridad de la información personal depende de la organización que realiza el tratamiento de estos datos, en este caso de cada central de riesgo. Cada una de las CEPIRS debe atender a la magnitud de datos que tratan, a la categoría de los datos personales que reciben a partir de las empresas a las cuales dirigen sus servicios, entre otros criterios, que cada una de ellas maneja de forma particular. De esa forma, sus protocolos deben estar vinculados a los riesgos que representan para la disponibilidad, integridad y confidencialidad de los datos personales que se encuentran en su poder.

23. Por ende, lo que le corresponde a la ANPD no es participar en la elaboración de dichos protocolos, sino verificar, en virtud de las actuaciones fiscalizadoras, sancionadoras y de tutela propias de su competencia, que los titulares de bancos de datos o responsables del tratamiento adecúen el contenido de sus protocolos a la normativa de protección de datos personales. En este sentido, resulta inviable establecer que esta autoridad se aboque a coordinar con las centrales de riesgo, la elaboración de los mencionados protocolos.

24. Cabe mencionar que, de acuerdo al artículo 33 de la LPDP, la ANPD tiene entre sus funciones las siguientes:

    - Emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados. (numeral 12).
    - Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento. (numeral 16)
    - Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores. (numeral 17)
    - En el marco de un procedimiento administrativo en curso, solicitado por la parte afectada, obtener de los titulares de los bancos de datos personales la información que estime necesaria para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones. (numeral 18)
    - Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones

[4] Aprobada el 27 de diciembre de 2013. Disponible en: https://www.gob.pe/institucion/anpd/informes-publicaciones/1938516-directiva-de-seguridad-para-el-tratamiento-de-datos-personales

técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley. (numeral 19)

- Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento. (numeral 20)

25. Asimismo, de acuerdo a la Séptima Disposición Complementaria Final de la LPDP, la ANPD es competente para salvaguardar los derechos de los titulares de la información administrada por las Centrales Privadas de Información de Riesgos (Cepirs) o similares conforme a los términos establecidos en la citada norma.

26. Por lo tanto, no es viable que la ANPD participe en la elaboración de protocolos para cada una de las CEPIRS.

***C. Sobre las billeteras digitales***

27. El Banco Central de Reserva del Perú, en la Circular N.º 0024-2022-BCRP, de 6 de octubre de 2022, que aprueba el Reglamento de Interoperatividad de los Servicios de Pago provistos por los Proveedores, Acuerdos y Sistemas de Pagos, define a las billeteras digitales como aquella "aplicación móvil que permite iniciar una trasferencia electrónica de fondos a través de los instrumentos de pago vinculados a ella. En el caso de transacciones con Códigos QR, la billetera digital escanea la información del código presentado por el comercio, para que el consumidor ordene el pago".

28. Por su parte, el Proyecto de Ley N.º 7919/2023-CR, en el artículo 5, define a la billetera digital como aquel programa o aplicación a través del cual se puede almacenar, enviar y recibir dinero de manera electrónica, en la que se guarda información sobre fondos, saldos bancarios, y números de cuenta; y, con la que se puede realizar compras en línea, transferencias de dinero, pagos de servicio o realizar otras transacciones financieras sin necesidad de usar dinero físico. La billetera digital permite realizar las referidas operaciones financieras desde un teléfono móvil, de manera digital.

29. Atendiendo a este concepto, el inciso 6.1. del artículo 6 del mencionado proyecto propone prohibir que las entidades financieras que cuenten con el servicio de aplicativos móviles de billeteras digitales brinden información que afecte el tratamiento de información personal y datos sensibles de los consumidores de servicios financieros cuando estos realicen compras en línea, transferencia de dinero, pagos de servicio u otras transacciones financieras.

30. Al respecto, es pertinente advertir que de acuerdo a lo establecido en la LPDP, cualquier titular de banco de datos o responsable del tratamiento debe realizar aquellas operaciones que supongan el uso de datos personales velando porque no se produzca un tratamiento inadecuado de información personal y sensible, para tal efecto, los titulares de bancos de datos o responsables del tratamiento deberán

respetar los principios rectores del derecho de protección de datos personales, así como cuidar que el tratamiento de datos personales se realice con pleno respeto a los derechos fundamentales de sus titulares.

31. Uno de los principios rectores del derecho de protección de datos personales es el principio de proporcionalidad, regulado en el artículo 7 de la LPDP, el cual establece que "todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la cual fueron recopilados".

32. En ese marco, en el caso de las billeteras digitales, el tratamiento de datos personales de clientes o usuarios de este servicio debe limitarse a la información crediticia indispensable para realizar las compras en línea, transferencia de dinero, pagos de servicio u otras transacciones financieras, por lo que cualquier tratamiento de datos personales sensibles que no responda a estas finalidades se encuentra prohibido por la LPDP; con lo cual, lo propuesto en el inciso 6.1. del artículo 6 del Proyecto de Ley N.º 7919, si bien no genera una nueva obligación con respecto a lo regulado en la LPDP y su reglamento, es positivo en la medida que enfatiza dicha obligación ya existente.

33. Por su parte, el inciso 6.2. del artículo 6 del proyecto propone incluir en los protocolos de servicio y transacciones financieras que se realicen con las billeteras digitales códigos alfanuméricos, a fin de que no se vulneren los datos sensibles de los consumidores de servicios financieros.

34. Al respecto, se debe tener en cuenta que, como ya se ha señalado, los datos personales son toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

35. La LPDP reconoce una categoría especial de datos personales denominada "datos sensibles", dado que requieren mayor protección, debido a que su vulneración ocasiona daños con mayor gravedad.

36. De acuerdo a lo establecido en el artículo 2, numeral 5 de la LPDP, son datos sensibles, los datos personales constituidos por datos biométricos que por sí mismos pueden identificar al titular; los datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual de las personas.

37. En este sentido, las compras en línea, transferencia de dinero, pagos de servicio u otras transacciones financieras de una persona que se realicen a través de billeteras digitales pueden incluir información sensible, pues el seguimiento, a través de actividades de perfilamiento, puede dar cuenta de determinada información sensible, tales como ingresos económicos, o información de salud, dependiendo de las compras que se realicen (compras de medicamentos o pago de citas médicas, por ejemplo).

38. Por ello, la implementación de medidas de seguridad de datos personales en billeteras digitales debe estar encaminada a garantizar que las transacciones aseguren la identidad de quienes las utilicen y, de esta forma, evitar usos fraudulentos.

***D. Sobre la modificación del numeral 5 del artículo 2 de la LPDP***

39. El Proyecto de Ley N.º 7919 propone modificar el numeral 5 del artículo 2 de la Ley N.º 29733, de Protección de Datos Personales en los siguientes términos:

| Texto vigente | Propuestas de modificación (resaltado en negrita) |
|---|---|
| "**Artículo 2.- Definiciones.**<br>Para todos los efectos de las presente Ley, se entiende por:<br>(…)<br>**5. Datos sensibles:** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; filiación sindical; e información relacionada a la salud o a la vida sexual". | "**Artículo 2.- Definiciones.**<br>Para todos los efectos de las presente Ley, se entiende por:<br>(…)<br>**5. Datos sensibles:** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; **documento nacional de identidad, dirección domiciliaria, centro de labores, número de teléfono fijo o móvil**, datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.<br>(…)" |

40. Los datos sensibles son aquellos datos personales cuyo tratamiento requiere de una protección reforzada, debido a su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona.

41. Lo que diferencia a los datos sensibles del resto de datos personales reconocidos por la LPDP reside en el impacto que los primeros pueden tener sobre la vida de las personas, ya que esta información se refiere a la esfera privada y, su conocimiento por terceros no legitimados para su tratamiento puede conducir, en determinadas circunstancias, a que se produzca discriminación o estigmatización de la persona.

42. En el Perú, esa protección reforzada a los datos sensibles viene determinada por la forma en que los titulares de los bancos de datos personales y responsables del tratamiento deben recabar el consentimiento de los titulares de los datos personales, dado que, en el caso de tratamiento de datos sensibles, el consentimiento de los titulares de los datos debe ser otorgado siembre por escrito, de acuerdo a lo señalado en el artículo 13, inciso 13.6; a diferencia del consentimiento para el tratamiento de los demás datos personales que puede darse tanto de forma verbal como por escrito, conforme el inciso 13.5 del citado artículo.

43. Asimismo, el artículo 132 del Reglamento hace una clara distinción en la gravedad de infringir determinadas disposiciones de la LPDP y su reglamento cuando se realiza tratamiento de datos sensibles:

| Infracciones leves | Infracciones graves |
|---|---|
| • Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.<br><br>• Recopilar datos personales que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. | • Realizar tratamiento de **datos personales sensibles** incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.<br><br>• Recopilar **datos personales sensibles q**ue no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos. |

44. Es necesario enfatizar que, el tratamiento de datos personales sensibles como los no sensibles debe ser acorde a lo establecido en la LPDP y su reglamento. Es decir, el hecho que se realice tratamiento de datos no sensibles no quiere decir que no se deban aplicar los principios y disposiciones de la LPDP, tales como el principio de seguridad[5] y el deber de confidencialidad[6].

45. Atendiendo a lo anteriormente expuesto, es necesario analizar si las modificatorias propuestas al artículo 2, numeral 5, de la LPDP por el Proyecto de Ley N.º 7919 responden a la naturaleza de datos sensibles y, por lo tanto, si es o no viable en este punto.

46. En relación a los datos sobre dirección domiciliaria, centro de labores, número de teléfono fijo o móvil, si bien pueden ser considerados datos personales, dado que permiten hacer identificable a una persona, lo cierto es que, atendiendo a la naturaleza de los datos sensibles, esta información, por su solo conocimiento, no

---

[5] LPDP
**"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."

[6] 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.
(…)"

supone una intromisión en la esfera íntima de las personas, ni su tratamiento puede conducir, en determinadas circunstancias, a que se produzca discriminación o estigmatización. Así, el conocer el domicilio, el centro de labores o el número de teléfono fijo o móvil de una persona, no implica tener acceso al ámbito personalísimo de sus pensamientos o creencias, al estado de su salud física o mental o a su vida sexual, con lo cual, el solo tratamiento de los datos que propone el proyecto, no pueden, por sí mismos, dar origen a actos de discriminación por parte de aquel que conozca o trate esta información sin su consentimiento; y, por ello, no pueden ser calificados como datos sensibles.

47. En lo que respecta al Documento Nacional de Identidad (DNI), el artículo 2 de la Ley N.º 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil (en adelante, Ley RENIEC) señala que el Documento Nacional de Identidad (en adelante, DNI) es un documento público, personal e intransferible que constituye la única cédula de Identidad Personal para todos los actos civiles, comerciales, administrativos, judiciales y, en general, para todos aquellos casos en que, por mandato legal, deba ser presentado.

48. Asimismo, de acuerdo con el artículo 32 de la Ley RENIEC, el DNI, como mínimo, deberá contener la fotografía del titular de frente, la impresión de la huella dactilar del índice de la mano derecha del titular o de la mano izquierda a falta de éste, además de datos como el código único de identificación que se le ha asignado a la persona; los nombres y apellidos del titular; el lugar y fecha de nacimiento del titular; la firma del titular; la fecha de emisión del documento; la dirección domiciliaria que corresponde a la residencia habitual del titular; entre otros datos.

49. El DNI, por lo tanto, contiene diversos datos personales que no necesariamente son sensibles, pero que, sin embargo, de proporcionarse a terceros, podrían vulnerar la confidencialidad y seguridad del titular de los datos personales.

50. Así tenemos que, a través de datos como la fecha de emisión del DNI, se permite la realización de algunos trámites a los que únicamente el titular del DNI tiene acceso; asimismo, al darse a conocer la totalidad de datos del DNI se puede ocasionar que una tercera persona se apropie de la identidad del titular para hacerse pasar por este, obteniendo beneficios y, en algunos casos, recursos que no le corresponden.

51. Atendiendo a lo anteriormente expuesto, cuando algún titular de banco de datos personales o responsable del tratamiento considere utilizar la información que aparece en el DNI debe limitarse al uso de los datos personales que resulten estrictamente necesarios para los fines específicos del tratamiento que pretende realizar y a la base jurídica o motivo legítimo que justificó su recogida, en estricto respeto al principio de proporcionalidad, regulado en el artículo 7 de la LPDP.

52. En este orden de ideas, dado que el DNI contiene información personal, tanto sensible (huella dactilar) como no sensible, no se puede considerar el documento en sí mismo como un dato sensible.

## IV. CONCLUSIONES

1. El Proyecto de Ley N.º 7919-2023-CR tiene por objeto regular el tratamiento de la información personal de la que disponen las centrales privadas de información de riesgos y protección al titular de la información, y la que brindan los aplicativos móviles de billeteras digitales, para garantizar la protección de la información personal y preservar su privacidad.

2. Este despacho, si bien valora como positivo que las centrales de riesgo tengan como obligación incluir protocolos para el adecuado tratamiento de datos personales, como prevé el Proyecto de Ley, considera a la vez que resulta inviable que la Autoridad Nacional de Protección de Datos Personales tenga que coordinar con cada central de riesgo la elaboración de los referidos protocolos, dado que corresponde a estas determinar el alcances y medidas de seguridad que establecerá en los mismos, atendiendo a sus propias características y usuarios.

3. En relación a la modificación del numeral 5 del artículo 2 de la LPDP, los datos dirección domiciliaria, centro de labores, número de teléfono fijo o móvil, no pueden ser calificados como datos sensibles, dado que estos no constituyen información que, por sí misma, pueda afectar a la vida íntima o personalísima de las personas u origine discriminación.

4. Con respecto a la incorporación del DNI como dato sensible, esta dirección aclara que este documento contiene tanto datos personales sensibles como no sensibles y, en este sentido, no resulta viable calificar al DNI en su integridad como dato sensible.

5. En conclusión, expuestas y valoradas en conjunto las consideraciones precedentes, el Proyecto de Ley N.º 7919/2023-CR resulta inviable.

Atentamente,

PERÚ MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Firmado digitalmente por LUNA CERVANTES Eduardo Javier FAU 20131371617 soft

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