



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de Transparencia,
Acceso a la Información Pública y
Protección de Datos Personales

“Decenio de la Igualdad de Oportunidades para mujeres y hombres”
“Año del Bicentenario del Perú: 200 años de Independencia”

OPINIÓN CONSULTIVA N° 014-2021-JUS/DGTAIPD

Asunto : Consulta sobre las obligaciones de los partidos políticos respecto a la Ley de Protección de Datos Personales y su reglamento.

Referencia: Hoja de Trámite N.º 49762-2020MSC

Fecha : Miraflores, 7 de abril de 2021

I. ANTECEDENTE

1. Mediante formulario de absolución de consulta sobre protección de datos personales, registrado con Hoja de Trámite N.º 49762-2020MSC, se consulta a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD), si los partidos políticos están en la obligación de cumplir con las disposiciones de la Ley de Protección de Datos Personales y su Reglamento; específicamente se consulta lo siguiente:

“¿En qué medida los partidos políticos están en la obligación de cumplir la Ley de Protección de Datos Personales y su Reglamento? En específico, si estos se encuentran en la obligación de inscribir las bases de datos de su titularidad y qué obligaciones (medidas de seguridad, etcétera) tienen estos respecto de los padrones electorales en su posesión que obtienen de la autoridad electoral en virtud del artículo 197 de la Ley Orgánica de Elecciones”.

II. MARCO NORMATIVO DE ACTUACIÓN

2. La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD), es la encargada de ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP)¹ y la Autoridad Nacional de Protección de Datos Personales (ANPD)².
3. Entre sus funciones se encuentra absolver las consultas que las entidades o las personas jurídicas o naturales le formulen respecto a la aplicación de las normas de transparencia, acceso a la información pública, así como de la normativa sobre protección de datos personales.

¹ 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 gestión de intereses (publicado el 07 de enero de 2017); Decreto Supremo N° 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos (publicado el 22 de junio de 2017); y Decreto Supremo N° 019-2017-JUS, que aprueba el Reglamento del Decreto Legislativo N° 1353 (publicado el 15 de setiembre de 2017).

² Ley N° 29733, Ley de Protección de Datos Personales, artículo 32.

“Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de Transparencia,
Acceso a la Información Pública y
Protección de Datos Personales

4. En esa medida, esta Dirección General emite la presente Opinión Consultiva en el ámbito de la interpretación en abstracto de las normas y no como mandato específico de conducta para un caso concreto.

III. ANÁLISIS

El ámbito de aplicación de la Ley N.º 29733, Ley de Protección de Datos Personales

5. La Ley N.º 29733, Ley de Protección de Datos Personales (en adelante la LPDP), tiene como objeto garantizar el derecho fundamental a la protección de datos personales, previsto en el artículo 2, numeral 6 de la Constitución Política del Perú.
6. De ese modo, el artículo 3 de la LPDP, señala que esta es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional.
7. Dicho artículo establece también que las disposiciones de la LPDP no son de aplicación a los siguientes datos personales:
 - “1. A los contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.
 2. A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por la ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito”.
8. Como es de verse, por regla general, todo tratamiento de datos personales, sean administrados por entidades públicas o privadas, están sujetos al ámbito de aplicación de la LPDP. La excepción a la regla son bancos de datos personales administrados por entidades públicas, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de sus competencias asignadas por ley, para la defensa nacional, seguridad pública y para el desarrollo de actividades en materia penal para la investigación y represión del delito, como por ejemplo los bancos de datos vinculados a la investigación y represión del delito del Ministerio Público o la Policía Nacional del Perú.
9. Sin embargo, debe precisarse que no todos los bancos de datos personales a cargo de las entidades públicas cuyas funciones están orientadas a la defensa nacional, seguridad pública y el desarrollo de actividades en materia penal para la investigación del delito se encuentran excluidos del alcance de la LPDP, toda vez que dichas entidades también administran otros tipos de bancos de datos personales que no son para los fines señalados anteriormente; como, por ejemplo, los bancos de datos personales de trabajadores, de videovigilancia, proveedores personas naturales, entre otros; los cuales sí se encuentran dentro del ámbito de aplicación de la LPDP.

“Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”

10. Por lo expuesto, se desprende que el ámbito de aplicación de la LPDP no se encuentra delimitado por el tipo de entidades públicas, sino por los fines de su tratamiento acorde a las competencias funcionales asignadas por ley.
11. Asimismo, dicha excepción al ámbito de aplicación de la LPDP no es absoluta, sino que debe leerse en concordancia la Constitución Política del Perú. Al respecto, es claro que LPDP contiene disposiciones que son manifestaciones de principios que tienen basamento constitucional, como es el caso del principio de interdicción de la arbitrariedad en el ejercicio del poder público, así como el de razonabilidad y proporcionalidad (artículo 200 de la Constitución)³.
12. En efecto, este sería el caso de las normas contenidas en los artículos 6, 7 o 9 de la LPDP. Normas que recogen principios como el de finalidad⁴, proporcionalidad⁵ o seguridad⁶ en el tratamiento de datos personales de ciudadanos, por citar unos ejemplos. Dado el basamento constitucional de estos, su fuerza normativa y eficacia irradia para todo tratamiento de datos personales, sea que este provenga de entidad pública o privada.
13. Así pues, para la ANPD, una agencia gubernamental dedicada a la defensa nacional o la seguridad pública, sólo puede exhibir finalidad legítima en el tratamiento de datos personales que realiza de los ciudadanos, si y sólo si, esa legitimidad comulga materialmente con los postulados constitucionales arriba reseñados.
14. Respecto a los partidos políticos, el segundo párrafo del artículo 1 de la Ley N.º 28094, Ley de Organizaciones Políticas, señala que *“los partidos políticos son asociaciones de ciudadanos que constituyen personas jurídicas de derecho privado cuyo objeto es participar por medios lícitos, democráticamente, en los asuntos públicos del país dentro del marco de la Constitución Política del Estado y de la presente ley”*.
15. En ese sentido, se aprecia que los partidos políticos no se encuentran dentro de las excepciones que señala el artículo 3 de la LPDP, por lo que se colige que los partidos políticos, de realizar tratamiento de datos personales, se encuentran sujetos al ámbito

³ Es basta la jurisprudencia constitucional que se ha ocupado de dar contenido a la arbitrariedad como cuestión interdicta. Aquí citamos la recaída en el Expediente N° 0090-2004-AA/TC (fundamento jurídico 12): “El concepto de arbitrario apareja tres acepciones igualmente proscritas por el derecho: a) lo arbitrario entendido como decisión caprichosa, vaga e infundada desde la perspectiva jurídica; b) lo arbitrario entendido como aquella decisión despótica, tiránica y carente de toda fuente de legitimidad; y c) lo arbitrario entendido como contrario a los principios de razonabilidad y proporcionalidad jurídica. De allí que, desde el principio del Estado de Derecho, surgiese el principio de interdicción de la arbitrariedad, el cual tiene un doble significado: a) En un sentido clásico y genérico, la arbitrariedad aparece como el reverso de la justicia y el derecho. b) En un sentido moderno y concreto, la arbitrariedad aparece como lo carente de fundamentación objetiva; como lo incongruente y contradictorio con la realidad que ha de servir de base a toda decisión. Es decir, como aquello desprendido o ajeno a toda razón de explicarlo. En consecuencia, lo arbitrario será todo aquello carente de vínculo natural con la realidad.”

⁴ **Artículo 6 de la LPDP. - Principio de finalidad**

“Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.”

⁵ **Artículo 7 de la LPDP. Principio de proporcionalidad**

“Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.”

⁶ Artículo 9 de la LPDP. 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.”

de aplicación de la LPDP y su reglamento, debiendo por tanto cumplir con todas las obligaciones y disposiciones que derivan de ellas, tales como la de inscribir los bancos de datos personales que sean de su titularidad.

El Padrón Electoral según la Ley N.º 26859, Ley Orgánica de Elecciones

16. El artículo 196 de la Ley N.º 26859, Ley Orgánica de Elecciones, establece que el Padrón Electoral es la relación de los ciudadanos hábiles para votar; se elabora sobre la base del registro único de identificación de las personas; se mantiene y actualiza por el Registro Nacional de Identificación y Estado Civil (RENIEC), según los cronogramas y coordinaciones de la Oficina Nacional de Procesos Electorales (ONPE).
17. Luego, el artículo 197 señala que el Padrón Electoral es público. Los partidos, agrupaciones independientes y alianzas pueden solicitar, en la forma que establezca el RENIEC, una copia del mismo. En párrafo aparte se indica que constituye excepción a la regla descrita en el párrafo anterior, los datos contenidos en el segundo párrafo del artículo 203⁷ de la presente Ley.
18. Por otro lado, el último párrafo del artículo 201 de la citada ley establece que el RENIEC y el JNE remiten a las organizaciones políticas, en formato digital, el padrón electoral preliminar y definitivo.
19. En ese orden de ideas, se tiene que los partidos políticos reciben una copia del Padrón Electoral, el cual es elaborado sobre la base del registro único de identificación de las personas, siendo el RENIEC quien lo mantiene y actualiza según los cronogramas y coordinaciones de la ONPE. Cabe mencionar que, la copia remitida a las agrupaciones políticas, de acuerdo a lo señalado en la Opinión Consultiva No. 12-2018-JUS/DGTAIPD, no debería incluir ni la huella dactilar ni el domicilio de cada elector⁸.
20. Llegado a este punto, es necesario precisar que el Padrón Electoral cuya elaboración es realizada en virtud a lo dispuesto por la Ley N.º 26859, Ley Orgánica de Elecciones, tiene como finalidad única y exclusiva su utilización en los diversos procesos electorales programados por la ONPE.
21. Por esa razón, es importante tener presente el principio de finalidad establecido en el artículo 6 de la LPDP, que señala que los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

⁷ Artículo 203 de la Ley 26859.-

En el padrón se consignan los nombres y apellidos, y el código único de identificación de los inscritos, la fotografía y firma digitalizadas de cada uno, los nombres del distrito, la provincia y el departamento y el número de mesa de sufragio. Asimismo, debe consignarse la declaración

El padrón también contendrá los datos del domicilio, así como la información de la impresión dactilar. Esta última será entregada en formato JPEG a una resolución de 500 píxeles por pulgada (dpi), la misma que será tratada y comprendida en soportes que garanticen su confidencialidad.

⁸ Ver: https://www.minjus.gob.pe/wp-content/uploads/2018/10/O-C-12_OCTUBRE.pdf

“Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”

22. De ese modo, si bien las agrupaciones políticas se encuentran autorizadas por ley para obtener una copia de los padrones electorales en el marco de los procesos electorales, también es importante que se tenga presente el principio de finalidad, a fin de garantizar que el tratamiento de los datos personales se limite a la finalidad para la cual les fue otorgada⁹.
23. De igual manera, es importante destacar que todo tratamiento de datos personales debe realizarse con especial responsabilidad y seguridad, por lo que las organizaciones políticas, al obtener copia de los padrones electorales, deben tener en cuenta el principio de seguridad establecido en el artículo 9 de la LPDP, que establece que “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.” De forma complementaria, el Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS, señala que *“en atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado”*.
24. Por consiguiente, se colige que los partidos políticos, al realizar tratamiento de datos personales a través de los padrones electorales, tienen la obligación de cumplir con las disposiciones que establece la LPDP y su reglamento a fin de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, mediante su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen, objeto que se encuentra establecido en el artículo 1 de la LPDP.
25. Respecto a la obligación de inscripción de los bancos de datos, de acuerdo al artículo 78 del Reglamento de la LPDP¹⁰, corresponde a los titulares de los bancos de datos personales su cumplimiento.¹¹
26. Al respecto, la LPDP, en el artículo 2, numeral 17, define al titular del banco de datos personales como la “persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.” En este caso, las organizaciones

⁹ **Artículo 19 del Reglamento de la LPDP.- Condiciones para la transferencia.**

Toda transferencia de datos personales requiere el consentimiento de su titular, salvo las excepciones previstas en el artículo 14 de la Ley y debe limitarse a la finalidad que la justifique. (subrayado nuestro).

¹⁰ Reglamento de la LPDP

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.



políticas no determinan el contenido del banco de datos personales del Padrón Electoral, por lo tanto no son titulares del mismo y no tienen la obligación de inscribirlo.

- 27. Sin embargo, si a partir de la copia recibida, generan un nuevo banco de datos, por ejemplo agregando nuevos datos, deberán inscribir ese nuevo banco de su titularidad ante el Registro Nacional de Protección de Datos Personales.

V. CONCLUSIONES

- 1. Los partidos políticos que realizan tratamiento de datos personales se encuentran sujetos al ámbito de aplicación de la LPDP y su reglamento, debiendo por tanto cumplir con todas las obligaciones y disposiciones que derivan de ellas, tales como la de inscribir los bancos de datos personales que sean de su titularidad.
- 2. El tratamiento de datos personales que realizan los partidos políticos, utilizando los padrones electorales, debe ser realizado con especial responsabilidad y seguridad, cumpliendo con las disposiciones que establece la LPDP y su reglamento, entre ellas el principio de finalidad y seguridad, a fin de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú.

Aprobado por:	Aprobado por:
<p>Eduardo Luna Cervantes Director General Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales</p>	<p>María Alejandra González Luna Directora (e) de la Dirección de Protección de Datos Personales</p>

“Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”