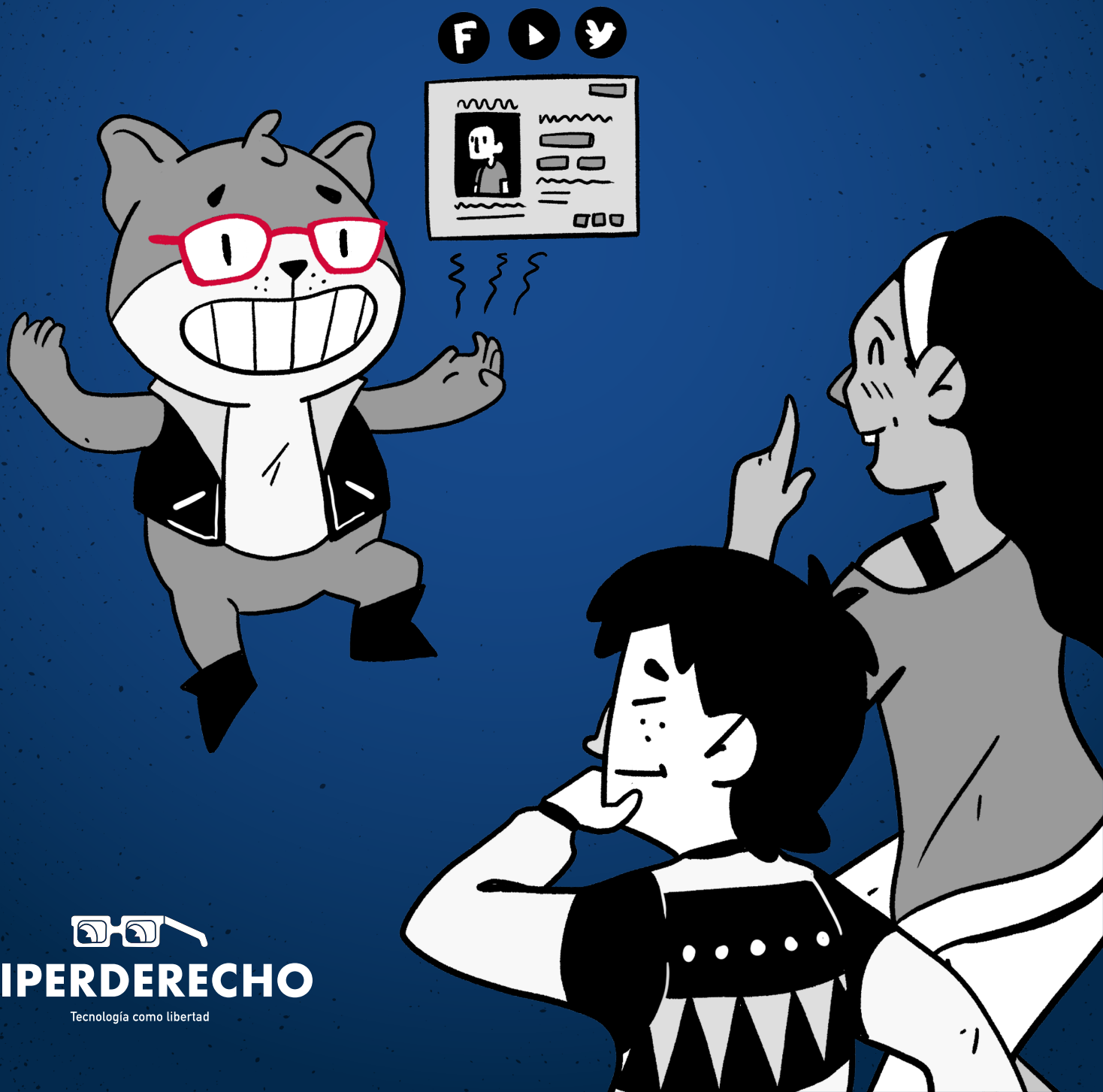
DATOS PERSONALES Y ELECCIONES



HIPERDERECHO

Tecnología como libertad

DATOS PERSONALES Y ELECCIONES

HIPERDERECHO

Asociación civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Investiga e interviene en debates de políticas públicas sobre libertad de expresión, derechos de autor, privacidad, ciberseguridad y violencia de género.

AUTOR

Dilmar Villena Fernández Baca

DIAGRAMACIÓN E ILUSTRACIONES

Gerald Espinoza *(El Chico Stan)*

Lima, marzo del 2021

Esta y otras publicaciones de Hiperderecho sobre tecnología e interés público pueden descargarse desde hiperderecho.org/publicaciones

Asociación Civil Hiperderecho

Av. Benavides 1944, oficina 901 Lima, Perú hola@hiperderecho.org

ÍNDICE

RESUMEN

En el presente informe se aborda la problemática del tratamiento de los datos personales en los procesos electorales. Se hace un análisis de la Ley de Protección de Datos Personales y cómo ésta obliga a los organismos electorales en el país y a las organizaciones políticas, determinando qué obligaciones deben cumplir respecto a los titulares de datos personales. A través de este informe, se podrá identificar qué información tienen o potencialmente podrían tener dichos organismos electorales y organizaciones políticas, lo cual ayudará a exigir el cumplimiento de las obligaciones en materia de protección de datos personales y de nuestros derechos.

INTRODUCCIÓN

Los procesos electorales trataron, desde un inicio, con cantidades bastante significativas de datos personales tanto de electores como de candidatos. Esto era necesario, principalmente, para poder llevarlos a cabo y preparar la logística detrás de la organización de un proceso electoral. En este sentido, existen bases de datos personales previas a la aprobación de la Ley de Protección de Datos Personales y de su caracterización como tales (por ejemplo, el Padrón Electoral) que hoy en día requieren especial atención para que su manejo se realice respetando nuestros derechos fundamentales.

Por otro lado, las organizaciones políticas también acceden a estas bases de datos y también elaboran bases de datos propias para poder cumplir sus finalidades. El contexto actual, luego de las reformas políticas realizadas, donde se impulsará a que los partidos políticos dejen de lado los mecanismos tradicionales de publicidad electoral (pintas en muros, paneles, televisión, radio) y giren hacia mecanismos más segmentados y específicos de publicidad, también hará que estos accedan y elaboren mayores cantidades de datos personales que contengan más información.

Los distintos actores que participan en un proceso electoral (tanto públicos como privados) elaboran, acceden y generan bases de datos. En este informe se analizará cuáles son los actores públicos más relevantes y qué papel cumplen las organizaciones políticas, en particular, tomando en cuenta sus obligaciones respecto de la Ley de Protección de Datos Personales. Así, luego de analizar las bases de datos que puedan tener, elaborar o acceder por mandato legal, tendremos en cuenta qué obligaciones específicas tienen estos actores para que un proceso electoral se desarrolle con pleno respeto de nuestros derechos fundamentales.

1 Ley de Protección de Datos Personales: ámbito de aplicación

La normativa peruana en torno a la protección de datos personales data del año 2012. La Ley de Protección de Datos Personales (Ley N° 29733) es el marco regulatorio en Perú a través del cual se desarrolla el derecho fundamental a la protección de datos personales, se establecen los principios de su aplicación, las obligaciones de los titulares de bancos de datos, entre otros.

Son varios los actores (públicos y privados) que son partícipes de los procesos electorales en nuestro país. No obstante, para los fines del presente informe, identificamos como principales a los siguientes actores: partidos políticos (así como movimientos o alianzas electorales), de un lado, y organismos del Sistema Electoral (Jurado Nacional de Elecciones - JNE, Oficina Nacional de Procesos Electorales - ONPE y el Registro Nacional de Identificación y Estado Civil - RENIEC) del otro.

Ahora bien, antes de continuar con el análisis sobre qué obligaciones tendrían estos actores, resulta necesario realizar una primera definición de qué es un dato personal. La Ley de Protección de Datos Personales define al dato personal como "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados". En este sentido, son datos personales el nombre, la dirección de domicilio, el número de documento de identidad, la edad, etcétera: en suma, toda información que permita identificar o hacer identificable a alguien.

Dentro de este concepto de dato personal existe una categoría especial: el dato sensible. Estos son datos que, por su especial importancia y por su estrecha vinculación a la intimidad de la persona, requieren mayor tutela. Algunos datos sensibles son, por ejemplo, los datos biométricos, los datos relacionados a la vida sexual y salud de la persona y, en lo que a este informe concierne, los datos que se refieren a las opiniones o convicciones políticas, religiosas, filosóficas o morales.

En lo referido a un proceso electoral, existe un universo de datos personales cuyo tratamiento resulta relevante para que este se pueda realizar y para que los partidos políticos puedan cumplir con informar a los electores sobre sus propuestas. Entre estos datos podemos encontrar el nombre, la edad, el domicilio, el número de DNI, circunscripción electoral, entre otros. Además, dentro de este conjunto de datos contamos con algunos que, de acuerdo a ley, requieren especial protección: opinión política, convicciones ideológicas, afiliación política y/o sindical, etcétera.

Ahora bien, respecto del ámbito de aplicación de la Ley de Protección de Datos Personales, es decir, sobre quiénes se encuentran en obligación de cumplir sus disposiciones, el artículo 3 indica que

> *La presente Ley 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. Son objeto de especial protección los datos sensibles. Las disposiciones de esta Ley no son de aplicación a los siguientes datos personales:*
>
> *(...)*

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 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.*

Teniendo en cuenta este ámbito de aplicación, corresponde entonces analizar cómo los distintos actores del sistema electoral se encuentran en la obligación, o no, de cumplir la Ley de Protección de Datos Personales y en qué medida.

a. Organismos del Sistema Electoral

En Perú son tres los organismos parte del Sistema Electoral: 1) Jurado Nacional de Elecciones -JNE-, 2) Oficina Nacional de Procesos Electorales -ONPE-; y, 3) el Registro Nacional de Identificación y Estado Civil -RENIEC-. Estos organismos son constitucionalmente autónomos, lo que implica que su autonomía está garantizada y reconocida a nivel constitucional y que no existe relación de subordinación o jerarquía entre estos: su relación es de competencia y deben coordinar entre ellos para llevar a cabo sus finalidades constitucionales. Ahora bien, la Ley de Protección de Datos Personales reconoce que esta también se aplica a los bancos de datos personales de la Administración pública con la excepción de aquellos que sean necesario para cumplir sus competencia en materia de defensa nacional y seguridad pública.

I. Jurado Nacional de Elecciones:

De lo dispuesto en la Constitución peruana (artículo 178) y en la Ley Orgánica del Jurado Nacional de Elecciones podemos concluir que sus competencias son:

1. Fiscalizar la legalidad del ejercicio del sufragio y de la realización de los procesos electorales, del referéndum y de otras consultas populares.

2. Fiscalizar la legalidad de la elaboración de los padrones electorales, luego de su actualización y depuración final previa a cada proceso electoral. Asimismo, autoriza su uso para cada proceso electoral.

3. Mantener y custodiar el registro de organizaciones políticas.

4. Velar por el cumplimiento de las normas sobre organizaciones políticas y demás disposiciones referidas a materia electoral.

5. Administrar justicia en materia electoral.

6. Proclamar a los candidatos elegidos; el resultado del referéndum o el de otros tipos de consulta popular y expedir las credenciales correspondientes.

7. Recibir y admitir las credenciales de los personeros de las organizaciones políticas.

Como podemos apreciar, en la medida que sus competencias no están referidas a materias de defensa nacional o seguridad pública, al Jurado Nacional de Elecciones le es plenamente aplicable la Ley de Protección de Datos Personales. Por otro lado, de las funciones constitucionales previamen-

te desarrolladas, podemos apreciar que el Jurado Nacional de Elecciones tiene injerencia en los siguientes bancos de datos: del padrón electoral, de los candidatos a los distintos cargos públicos, el banco sobre los miembros de los Jurados Electorales Especiales, los bancos de datos personales que se encuentren en el registro de organizaciones políticas y del banco de datos referido a los personeros de las organizaciones políticas.
Justo es mencionar que, de acuerdo al artículo 14 de la Ley de Protección de Datos Personales, el Jurado Nacional de Elecciones no tiene la obligación de obtener el consentimiento de los titulares de estos datos en la medida que estos se recopilan para el ejercicio de sus funciones. No obstante, si bien no se encuentra en la obligación de recopilar el consentimiento, sí tiene la obligación de cumplir con otras disposiciones reconocidas en la Ley tales como cumplir con los principios de legalidad, finalidad, proporcionalidad, calidad, seguridad, disposición de recurso y nivel de protección adecuado, y las obligaciones que de estos principios se derivan.

En lo referido al cumplimiento de la Ley, es posible apreciar que el Jurado Nacional de Elecciones sí considera que la Ley les es aplicable puesto que dicha entidad ha inscrito en el Registro Nacional de Protección de Datos Personales las siguientes bases de datos: 1) Miembros de los Jurados Electorales Especiales, y 2) Antecedentes de posibles candidatos de las organizaciones políticas de un proceso electoral determinado.

De otro lado, un registro que se encuentra a cargo del Jurado Nacional de Elecciones es el Registro de Organizaciones Políticas. Según la Ley de Organizaciones Políticas, Ley N° 28094, este es un registro de carácter público (artículo 4) en el cual se almacenan los datos personales (nombre) de los fundadores, dirigentes, representantes legales, apoderados y personeros de las distintas organizaciones políticas. Además, en dicho Registro también se anota el padrón de afiliados, el cual también es público (artículo 7) y que, de acuerdo al Reglamento del Registro de Organizaciones Políticas, Resolución N° 0208-2015-JNE, contiene como mínimo los siguientes datos personales (artículo 98): los nombres y apellidos, DNI, firma y/o huella digital, fecha de afiliación, número de ficha y domicilio.

En la medida que tanto el Registro de Organizaciones Políticas y el Padrón de Afiliados son públicos, de acuerdo a ley, estos son accesibles a través de una página web del Jurado Nacional de Elecciones. Así, a través de Internet se puede consultar si determinada persona se encuentra afiliada o no a determinado partido político o si es fundadora o personera de uno.
Llegados a este punto, es importante volver a remarcar que estaríamos frente a datos sensibles. En efecto, los datos personales que revelan estos bancos de datos dan a conocer cuál es la orientación o filiación política de una persona. El artículo 13.6 de la Ley de Protección de Datos Personales dispone que se pueden tratar datos sensibles sin el consentimiento del titular con los siguientes requisitos: 1) autorización a través de una ley; y, 2) atender a motivos importantes de interés público.

El Jurado Nacional de Elecciones gestiona estos bancos de datos en virtud de un mandato legal (las disposiciones contenidas en la Ley de Organizaciones Políticas) y sí es posible sostener que la publicidad en torno a la fundación, filiación y militancia de organizaciones políticas responde a necesidades importantes de interés público. En efecto, el conocer esta información hace posible prever posibles situaciones de conflictos de interés, de nepotismo, de ausencia de meritocracia, entre otros.

No obstante, si bien no existe la obligación de recabar el consentimiento del titular, sí existen otras obligaciones que el Jurado Nacional de Elecciones debe cumplir cuando realiza el tratamiento de estos datos personales. Teniendo en cuenta que nos encontramos ante datos sensibles, es de especial importancia el cumplimiento del principio de seguridad, lo cual impone una serie de obligaciones al titular de estas bases de datos. Este punto será retomado más adelante (pag 15).

Finalmente, podemos apreciar que el JNE cuenta con un repositorio de resoluciones jurisdiccionales. De acuerdo al Reglamento de la Ley de Protección de Datos Personales, Decreto Supremo N° 003-2013-JUS, este repertorio debería estar anonimizado para que cumpla con los requisitos de fuente accesible al público. Sin embargo, es importante recalcar que las materias que resuelve el JNE son de alto interés público, en la medida que se discute la participación, las sanciones o el registro debido a cargos públicos. En este caso nos encontramos ante un supuesto en el que se debe ponderar el derecho a la protección de los datos personales de quienes aspiran a un cargo público y el interés detrás de conocer el contenido de resoluciones que determinan el devenir de un proceso electoral. En este punto nos inclinamos por la publicidad de las resoluciones y de los datos personales relevantes en ella: es decir, si la resolución gira en torno a si determinado candidato continúa o no en carrera electoral, la publicidad sobre la identificación del candidato resulta necesaria para que el proceso electoral tenga un normal desarrollo.

En resumen, el Jurado Nacional de Elecciones sí trata una serie de datos personales y tiene bajo su poder varios bancos de datos referidos al cumplimiento de sus fines constitucionales. Dicho organismo se encuentra en la obligación de cumplir la Ley de Protección de Datos Personales y, si bien no está obligado a recopilar el consentimiento para tratar los datos personales referidos al cumplimiento de sus finalidades públicas, sí debe cumplir con los demás principios reconocidos en la Ley.

II. Oficina Nacional de Procesos Electorales:

La Constitución establece que tiene como competencias el “organizar todos los procesos electorales, de referéndum y los de otros tipos de consulta popular, incluido su presupuesto, así como la elaboración y el diseño de la cédula de sufragio. Le corresponde asimismo la entrega de actas y demás material necesario para los escrutinios y la difusión de sus resultados. Brinda información permanente sobre el cómputo desde el inicio del escrutinio en las mesas de sufragio”. Su Ley Orgánica, Ley N° 26487, indica que tiene como función, además, el coordinar la elaboración de padrones electorales con el RENIEC, entre otros.

Al igual que el JNE, la ONPE también considera que les es aplicable la Ley de Protección de Datos Personales pues también tiene una base de datos inscrita en el Registro Nacional de Protección

de Datos Personales: electores que figuran en los padrones electorales. Llegados a este punto es importante definir qué es el padrón electoral. El artículo 196 de la Ley Orgánica de Elecciones, Ley N° 26859, define al Padrón Electoral como "la relación de los ciudadanos hábiles para votar" la cual "se elabora sobre la base del registro único de identificación de las personas". El Padrón Electoral es público de acuerdo al artículo 197 de dicha Ley, y los datos personales que figuran en este son:

- Nombres
- Apellidos
- Código Único de Identificación
- Fotografía
- Firma digitalizada
- Distrito, provincia y departamento de la mesa de sufragio
- Número de la mesa de sufragio
- Declaración voluntaria de alguna discapacidad
- Domicilio
- Impresión dactilar

Ahora bien, es importante señalar que en la base de datos inscrita ante el Registro Nacional de Protección de Datos Personales se informa que la base de datos titulada "Electores que figuran en los padrones electorales" (Código RNPDP-EP N° 3242) cuenta con los siguientes datos personales:

- Nombres
- Apellidos
- N° DNI
- Dirección de domicilio
- Teléfono
- Dirección de correo electrónico
- Imagen
- Firma
- Firma electrónica
- Fecha de nacimiento
- Nacionalidad
- Sexo
- Profesión
- Edad
- Características físicas
- Información relativa a la salud física o mental
- Huella digital
- Convicciones políticas

Como podemos apreciar, la base de datos inscrita excede de lo autorizado a través de ley. En este sentido, si la base de datos contiene toda la información que indica en el registro, podríamos encontrarnos frente una afectación a los principios de legalidad, consentimiento, finalidad y proporcionalidad de la Ley de Protección de Datos Personales. Si bien existe una excepción para el principio de consentimiento, en la medida que existe autorización legal para tratar estos datos, estos solo aplican para los taxativamente recogidos en el artículo 197 de la Ley Orgánica de Elecciones. En este sentido, datos personales como el teléfono, la dirección de correo electrónico o la profesión quedan exentos del ámbito de aplicación de dicha excepción. Por ello, para su tratamiento, la entidad respectiva debería obtener el consentimiento del titular.

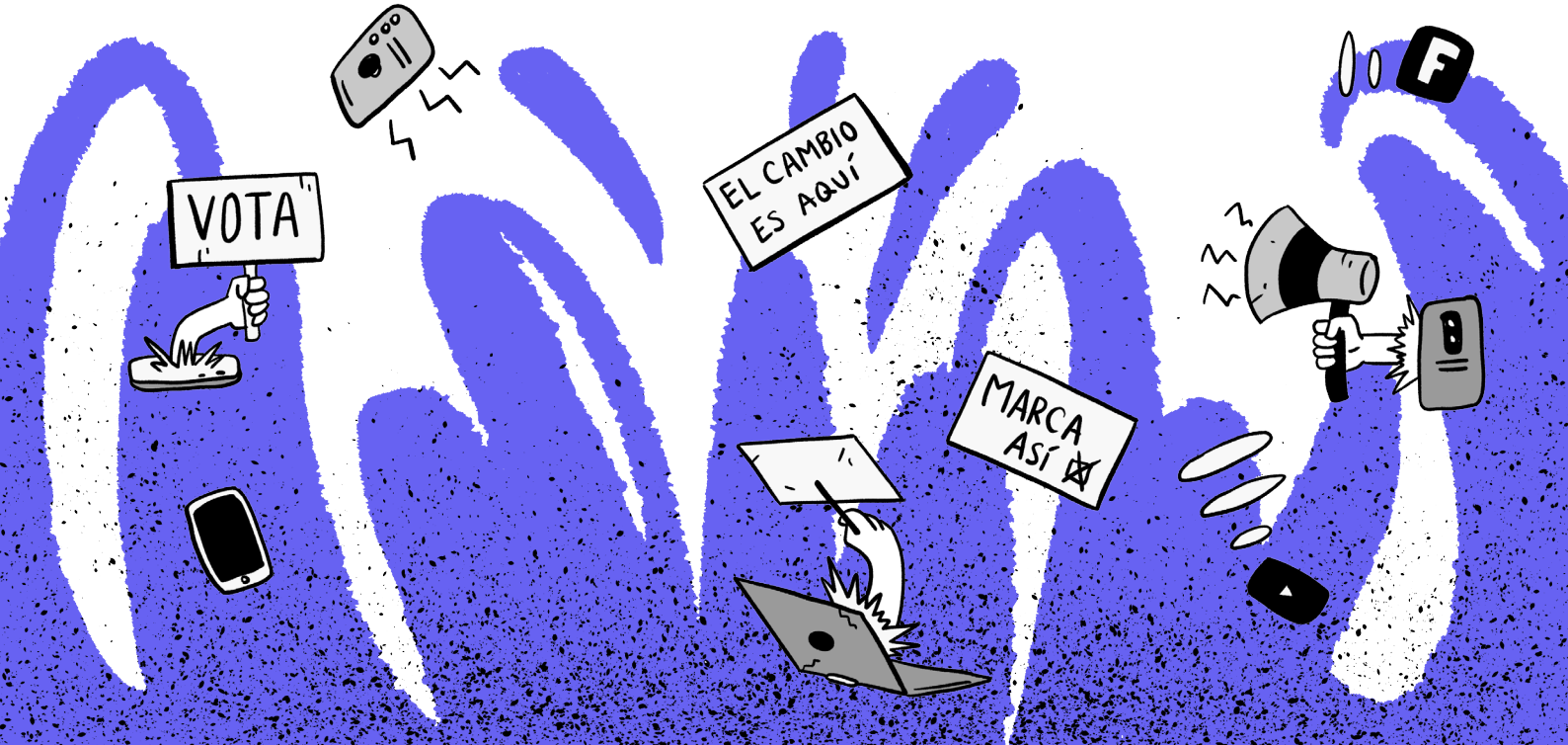
Más aún, teniendo en cuenta que el Padrón Electoral es una base de datos que, por mandato legal, es una lista de personas hábiles para votar y en base al cual se organiza el proceso electoral cabe preguntarnos sobre sí recopilar información sobre dirección de correo electrónico y profesión resultan esenciales para realizar el proceso electoral. En este sentido, se estaría también afectando el principio de proporcionalidad puesto que se estarían tratando datos personales que no resultan relevantes para la finalidad del Padrón Electoral.

En definitiva, podemos apreciar que ONPE, en la medida que tiene como finalidad constitucional el organizar los procesos electorales, trata datos personales y, dentro de ellos, la base de datos más relevante es la relativa al Padrón Electoral. Si bien existen ciertos datos en el Padrón cuyo tratamiento no requiere consentimiento en virtud de habilitación legal, existen otros que, de acuerdo al Registro, sí deberían de requerir consentimiento. Más aún, como señalamos previamente, que la recopilación de ciertos datos personales esté exento de requerir el consentimiento, no exime del cumplimiento de las otras obligaciones y principios contemplados en la Ley de Protección de Datos Personales.

III. Registro Nacional de Identificación y Estado Civil:

De acuerdo al artículo 183 de la Constitución, el Registro "tiene a su cargo la inscripción de los nacimientos, matrimonios, divorcios, defunciones, y otros actos que modifican el estado civil. (...) Prepara y mantiene actualizado el padrón electoral. Proporciona al Jurado Nacional de Elecciones y a la Oficina Nacional de Procesos Electorales la información necesaria para el cumplimiento de sus funciones. Mantiene el registro de identificación de los ciudadanos y emite los documentos que acreditan su identidad". Su Ley Orgánica, Ley N° 26497, indica (artículo 3) que esta entidad está "encargada de organizar y mantener el registro único de identificación de las personas naturales e inscribir los hechos y actos relativos a su capacidad y estado civil".
A diferencia de los anteriores organismos electorales, RENIEC no cuenta con bases de datos inscrita en el Registro. No obstante, la Ley de Protección de Datos Personales sí le es aplicable, tal como se indica en la Opinión Consultiva N° 36-2020-JUS/DGTAIP:

> *(...) el RENIEC administra bancos de datos personales relacionados con el registro de identificación de las personas naturales, así como sus hechos y actos relativos a su capacidad y estado civil (...) por lo que prima facie los bancos de datos personales que se encuentran bajo su administración, se encuentran bajo el ámbito de aplicación de la LPDP.*



Por lo tanto, RENIEC, entidad que es titular de los bancos de datos personales más grandes del Perú (los bancos de datos personales referidos al estado civil e identificación de las personas), debe cumplir con los principios y obligaciones de la Ley de Protección de Datos Personales. Entre ellas, podemos encontrar las obligaciones de "establecer un procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del titular de los datos personales; así como la obligación de adoptar las medidas técnicas, organizativas y legales que garanticen la seguridad del tratamiento de datos personales, evitando su alteración, pérdida, tratamiento o acceso no autorizado"[1].

Ahora bien, en lo referido al proceso electoral, resulta de especial importancia el rol que juega RENIEC en lo relacionado al Padrón Electoral. El artículo 196 de la Ley Orgánica de Elecciones indica que el RENIEC mantiene y actualiza el Padrón. Este es, pues, el encargado de su elaboración para su posterior aprobación del JNE y remisión a la ONPE (artículo 201). Es importante también anotar que el RENIEC es el encargado de dictaminar las formas y procedimientos a través de los cuales el Padrón, que es público, puede ser accesible por las organizaciones políticas (artículo 197).

Llegados a este punto cabe reflexionar, entonces, sobre qué datos personales contiene el Padrón Electoral que RENIEC remitirá a las respectivas organizaciones políticas. Una primera limitante a sobre qué información debería ser remitida a las organizaciones políticas es la que se contiene en el segundo párrafo del artículo 197 de la Ley Orgánica de Elecciones, donde se explicita que las organizaciones políticas no pueden solicitar la siguiente información contenida en el Padrón Electoral: domicilio e impresión dactilar. La Opinión Consultiva emitida a través de Oficio N° 140-2018-JUS/DGTAIPD también refrenda dicha afirmación pues indica que la remisión del Padrón Electoral hacia organizaciones políticas será acorde al principio de proporcionalidad solo cuando se comparte únicamente la información contenida en el primer párrafo del artículo 203 de la Ley Orgánica de Elecciones, vale decir: nombres y apellidos, código único de identificación de los inscritos, fotografía y firma digitalizadas, los nombres del distrito, la provincia y el departamento y el número de mesa de sufragio; y, declaración voluntaria de alguna discapacidad.

RENIEC, de su lado, afirma[2] que los datos personales contenidos en el Padrón Electoral que puede ser accesible por las organizaciones políticas son:

- Apellido paterno
- Apellido materno
- Nombres
- DNI
- Mesa (grupo de votación)
- Departamento, provincia y distrito

Asimismo, indica que la información que se ha de remitir a las organizaciones políticas no ha de contener los siguientes datos: fotografía, impresión dactilar, firma y domicilio. Ahora bien, llegados a este punto, parece ser que respecto del padrón electoral, los datos personales que este contiene varía en función de cuando es elaborado por el RENIEC, cuando este ha sido inscrito en el Registro Nacional de Datos Personales por ONPE y sobre qué datos pueden ser entregados a las organizaciones políticas cuando estas solicitan el Padrón. Este se puede clasificar de la siguiente manera:

[1]Opinión Consultiva N° 36-2020-JUS/DGTAIP, conclusión 4.
[2]CARTA N° 001162-2019/SGEN/OAD/RENIEC.

Contenido del Padrón Electoral elaborado por el RENIEC	Contenido del Padrón Electoral elaborado ONPE	Contenido del Padrón Electoral que puede ser entregado a organizaciones políticas
Nombres	Nombres	Nombres
Apellidos	Apellidos	Apellidos
Código Único de Identificación	N° DNI	N° DNI
Fotografía	Imagen	-
Firma digitalizada	Firma Firma electrónica	-
Distrito, provincia y departamento de la mesa de sufragio	-	Distrito, provincia y departamento de la mesa de sufragio
Número de la mesa de sufragio	-	Número de la mesa de sufragio
Declaración voluntaria de alguna discapacidad	Información relativa a la salud física o mental	-
Domicilio	Domicilio	-
Impresión dactilar	Huella digital	-
-	Teléfono	-
-	Dirección de correo electrónico	-
-	Fecha de nacimiento	-
-	Nacionalidad	-
-	Sexo	-
-	Profesión	-
-	Edad	-
-	Características físicas	-
-	Características políticas	-

Como podemos apreciar, la información que registra ONPE abarca muchos datos personales adicionales a los que según Ley debería contener el Padrón Electoral. Sobre este punto nos remitimos a la problemática planteada en el punto II anterior. Ahora bien, también podemos observar que las organizaciones políticas no pueden acceder a todos los datos personales que contiene el registro, sino solo a unos mínimos y aquellos que estén estrictamente relacionados con publicidad del Padrón: saber qué ciudadanos pueden sufragar y dónde lo realizarán.

Finalmente, si bien el tratamiento de estos datos personales, por parte de RENIEC, está exento del consentimiento por mandato legal, dicha entidad sí debe cumplir con las demás obligaciones que se encuentran en la Ley de Protección de Datos Personales. Este punto será desarrollado posteriormente.

b. Organizaciones políticas

La Ley de Organizaciones Políticas define a los partidos políticos (artículo 1) como "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". En este sentido, y de acuerdo a lo que estipula la Ley de Protección de Datos Personales, los bancos de datos de los cuales las organizicaciones políticas sean titulares serán de administración privada. Asimismo, en la medida que el tratamiento de estos datos se darán en territorio nacional, la Ley de Protección de Datos Personales les será plenamente aplicable.

Ahora bien, teniendo en cuenta su naturaleza y las funciones que realizan, los partidos políticos tienen bajo su poder o tienen acceso básicamente las siguientes bases de datos:

a. Base de datos relativa a su padrón de afiliados.
b. El Padrón Electoral en caso sea solicitado.
c. Bases de datos que elaboren en virtud del desempeño regular de sus funciones y que puedan ser utilizados con fines de campaña electoral: bases de datos de aportantes, ciudadanos interesados, ciudadanos a los que remitir publicidad electoral, etcétera.

Respecto de la base de datos del padrón de afiliados, cabe mencionar que para su elaboración no se requiere consentimiento de los afiliados. Esto en virtud del artículo 14 numeral 7 de la Ley de Protección de Datos Personales:

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

(...)
7. *Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.*

Como podemos apreciar, las bases de datos sobre los afiliados a un partido político no requieren la autorización de los titulares de los datos; no obstante, para ser transferidos sí se requiere autorización. Sin embargo, en la medida que existe una ley que autoriza la transmisión de esta base de datos al Registro de Organizaciones Políticas administrado por el JNE, para realizar esta transferencia no

se requeriría tampoco el consentimiento de los titulares de los datos.

En lo relativo al Padrón Electoral, se puede apreciar que la Ley autoriza al RENIEC brindar su acceso a organizaciones políticas y que los datos remitidos deben ser estrictamente necesarios para su finalidad correspondiente. De acuerdo a lo establecido en la ley, las organizaciones políticas no podrán acceder a datos biométricos (huella dactilar) o sobre el domicilio de la persona. Para que el Padrón Electoral sea transferido a los partidos políticos no se requiere el consentimiento de los titulares de los datos en virtud de que existe una habilitación legal para ello y que estamos frente a una base de datos pública. Sin embargo, como podemos apreciar, ello no exime del cumplimiento de los principios de finalidad y proporcionalidad.

Finalmente, tenemos el caso de las bases de datos que las organizaciones políticas podrían elaborar en el desempeño de sus funciones. Un caso importante de análisis son las bases de datos que estos elaboran o adquieren con la finalidad de realizar publicidad electoral. Sobre este supuesto, es importante señalar que las organizaciones políticas deben requerir el consentimiento de los titulares para elaborar estas bases de datos y esto tiene que ser previo, expreso e informado. Asimismo, deben cumplir con los principios recogidos en la Ley de Protección de Datos Personales y con las obligaciones establecidas en ella.

2 Obligaciones que deben cumplir los actores en las elecciones en lo relativo a la protección de datos personales

El artículo 28 de la Ley de Protección de Datos Personales establece que los titulares de bancos de datos tienen las siguientes obligaciones:

1. **Efectuar el tratamiento de datos personales, solo previo consentimiento, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la presente Ley.**

   Como pudimos apreciar a lo largo del presente documento, son varias las bases de datos que pueden ser elaboradas y tratadas por mandato legal y que estarían exentas de cumplir esta obligación. Este es el caso del Padrón Electoral o del padrón de afiliados de partidos políticos.

2. **No recopilar datos personales por medios fraudulentos, desleales o ilícitos.**

   El cumplimiento de esta obligación tendría mayor nivel de injerencia en las organizaciones políticas. Estas, al momento de adquirir o elaborar bases de datos no pueden realizarlo fraudulentamente o de manera ilícita. Es decir, si van a elaborar una base de datos sobre determinada materia, deben informar a los titulares de estos que efectivamente van a recopilarlos y elaborar una base de datos y requerir la entrega voluntaria de estos datos. Esta obligación también prscribe la posibilidad de que las organizaciones políticas puedan acceder a bases de datos de manera ilícita, como podría ser la compra de estos en el mercado negro de bases de datos.

3. **Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.**

   Las organizaciones políticas, al momento de elaborar las bases de datos que estimen convenientes, deben recopilarlos de manera actualizada y deben ser los estrictamente necesarios para la finalidad que las bases de datos han sido creadas. Por ejemplo, si están elaborando una base de datos sobre personas a las cuales remitirle publicidad electoral, deberán recopilar los datos que permitan llevar a cabo dicha función: en ningún caso podrían recopilar información sobre orientación religiosa, estado económico, situación laboral, o cualquier otro no relacionado con ello.

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.**

   Si los datos personales han sido obtenidos con la finalidad de realizar capacitaciones a la ciudadanía, las organizaciones políticas no pueden utilizar estos datos para realizar proselitismo político o para realizar estadísticas. Esto último solo está permitido en la medida que se anonimicen o disocien los datos.

5. **Almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.**

   Tanto las entidades del sistema electoral como las organizaciones políticas deben permitir la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición. Para esta finalidad, deben almacenar los datos personales de tal manera que permitan que la persona pueda acceder a sus datos o rectificarlos sin procedimientos más allá de los razonablemente esperados.

6. **Suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto.**

   Esta obligación hace referencia a que, en caso se tenga una base de datos incompleta o inexacta, los titulares están en la obligación de actualizar o eliminar estos datos cuando estos tengan conocimiento de ello. Por ejemplo, si se tiene conocimiento que una persona varió su domicilio, existe la obligación legal de actualizar esta información cuando se tenga conocimiento de ello.

7. **Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.**

   Esta disposición obliga, por ejemplo, a las organizaciones políticas a suprimir las bases de datos elaboradas para el proceso electoral general del 2021 una vez este haya concluído. En la medida que toda recopilación y tratamiento se realiza con una finalidad específica (por ejemplo: Base de datos para realizar publicidad electoral en la campaña política del 2021), una vez concluido el proceso electoral las organizaciones políticas deben eliminar dicha base de datos. Recordemos que todo tratamiento tiene que cumplir los principios de finalidad y proporcionalidad.

8. **Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información relativa al tratamiento de datos personales que esta le requiera y permitirle el acceso a los bancos de datos personales que administra, para el ejercicio de sus funciones, en el marco de un procedimiento administrativo en curso solicitado por la parte afectada.**

   Tanto el JNE, el RENIEC, la ONPE y las organizaciones políticas deben permitir el acceso a la Autoridad Nacional de Protección de Datos Personales y proporcionarle la información que esta requiera.

De otro lado, podemos también afirmar que existen dos grandes grupos de obligaciones que deben cumplir los actores de un proceso electoral:

(i) Establecer un procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del titular de los datos personales; y,

(ii) Adoptar las medidas técnicas, organizativas y legales que garanticen la seguridad del tratamiento de datos personales, evitando su alteración, pérdida, tratamiento o acceso no autorizado.

El primero hacer referencia a que, ya sea el JNE o un partido político o movimiento regional, todos estos actores deben generar procedimiento para permitir acceder a qué datos personales estos tienen almacenados, solicitar su rectificación o cancelarlos según sea conveniente. Esto significa, por ejemplo, que si recibimos publicidad electoral, los partidos políticos deben permitir el acceso a los datos nuestros que tengan almacenados y brindar información sobre cuál es el medio lícito de su obtención. Además, deben permitir que el titular pueda solicitar su eliminación de la base de datos que estos administren.

Respecto del segundo grupo de obligaciones, es importante para dicho caso traer a cuenta lo dispuesto en la Directiva de Seguridad de la Autoridad de Protección de Datos Personales. En el siguiente cuadro se podrá apreciar ello de mejor manera:

Base de datos	Obligado	Categorías en el tratamiento de acuerdo a la Directiva de Seguridad	Medidas de seguridad organizativas mínimas	Medidas de seguridad jurídicas mínimas	Medidas de seguridad técnicas mínimas			
					Relacionadas al acceso no autorizado	Relacionadas a la alteración no autorizada	Relacionadas a la pérdida del banco de datos personales	Relacionadas al tratamiento no autorizado del banco de datos personales.
Registro de organizaciones políticas	JNE	Complejo, crítico	- Llevar un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar al personal con acceso en determinado momento (Trazabilidad). - Desarrollar procedimientos documentados adecuados para el tratamiento de datos personales. - Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales. - Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales. - Desarrollar un procedimiento de asignación de privilegios de acceso al banco de datos personales y su correspondiente registro de acceso.	- Adecuación de los contratos del personal relacionado con el tratamiento de datos personales. - Adecuación de los contratos con terceros.	- Gestión y uso de contraseñas: Almacenar contraseñas de forma cifrada, contraseñas con un mínimo de 8 dígitos alfanuméricas. - Revisión, por lo menos semestral, de los privilegios de acceso y el registro de la revisión. - Proteger contra el acceso físico no autorizado: Ubicar el banco de datos personales en un ambiente aislado protegido por cerradura donde la responsabilidad del acceso recae en el titular del banco de datos o un responsable delegado por el titular. - La autorización de ingreso a la base de datos, por parte del titular, debe contener como mínimo: usuario, fecha y hora de asignación de autoriza-ción/retiro de autorización; y, usuario que autoriza. - Implementar un registro de accesos, que debe contener como mínimo: fecha y hora de acceso, persona que accede y motivo de acceso.	- El traslado de la base de datos debe contar con autorización del titular o quien este designe. - Si es físico, debe transportarse mediante contenedores que eviten su acceso y legibilidad. Si es informático deben ser previamente encriptados y luego asegurada su integridad. - Los procesos de copia o reproduc-ción de las bases de datos deben ser supervisadas y se debe registrar: a) Nombre de la persona que solicita la copia. b) Nombre de la persona autorizada a realizar copias. c) Descripción de los datos personales copiados. d) Número de copias. e) Motivo. f) Nombre de la persona que recibe la copia. g) Lugar de destino. h) Periodo de validez de la copia. - La asignación de privilegios de la base de datos, por parte del titular, debe contener como mínimo: usuario, fecha y hora, privilegio asignado; y, usuario que autoriza	- Realizar copias de respaldo. - La recuperación, desde la copia de respaldo, debe requerir autoriza-ción autorización. - Realizar pruebas de recuperación de las bases de datos.	- En bases de datos no automatizadas, se debe mantener los datos personales independizados de forma individual, de modo que pueda referirse unívoca-mente a un titular sin exponer información de otro. -El titular del banco de datos personales debe informar al titular de datos personales los incidentes que afecten significati-vamente sus derechos patrimoniales o morales. - Los equipos utilizados para el tratamiento de los datos personales deben recibir mantenimiento preventivo y correctivo. -Los equipos utilizados para el tratamiento de los datos personales deben contar con software actualizado de protección contra software malicioso. - Toda información electrónica que contiene datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad. - La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad. -Restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales salvo autorización del titular del banco de datos personales. -Realizar auditoría externa para la verificación del cumplimiento de la directiva de seguridad. - Resultados de la auditoría deben iniciar la implemen-tación de acciones correctivas.
Padrón de afiliados	Organizacines políticas, JNE	Crítico						
Padrón Electoral	RENIEC, JNE, ONPE, organizaciones políticas	Complejo, crítico						

Como podemos apreciar, si bien los organismos del sistema electoral y los partidos políticos están exentos de requerir el consentimiento para tratar datos personales, sí deben cumplir con medidas organizativas, jurídicas y técnicas mínimas respecto de las bases de datos que están en su poder. Ello sumado a establecer los procedimientos para poder ejercer los derechos ARCO respectivos.

Finalmente, resulta importante compartir el documento elaborado por la Comisión Europea sobre protección de datos personales en contextos electorales. En lo referido a las organizaciones políticas se indica que, en la medida que controlan datos personales, se les realiza las siguientes recomendaciones:

- Cumplir con el principio de finalidad y proporcionalidad (tratamiento de datos posteriores solo compatibles con la finalidad respectiva).
- Elegir la base legal apropiada para tratar datos personales: consentimiento, autorización por ley, especiales previsiones para datos sensibles.
- Realizar evaluación de impacto de protección de datos personales.
- Informar a las personas sobre cada finalidad de tratamiento de datos personales, ya sea cuando ellos mismos la recolectan o cuando la reciban por parte de terceras partes.
- Asegurar la exactitud de datos personales, especialmente cuando los datos vienen de distintas fuentes y para datos inferidos.
- Verificar que los datos obtenidos por terceras partes sean obtenidos de manera lícita y con qué propósitos.
- Tomar en cuenta los riesgos de perfilación y adoptar las medidas de resguardo apropiadas.
- Identificar claramente quiénes acceden a los datos.
- Asegurar la seguridad del procesamiento cumpliendo con las medidas técnicas, legales y organizativas respectivas.
- Especificar obligaciones en contratos u otros documentos similares con procesadores de data o empresas de análisis de datos.
- Eliminar los datos cuando esta ya no sea necesaria para el propósito inicial que esta fue recopilada.

Cabe añadir que de la revisión del Registro Nacional de Datos Personales, no se ha podido encontrar ninguna base de datos inscrita por algún partido político. Ello nos da a entender que o no cuentan con bases de datos distintas a las que legalmente pueden ostentar (lo que no les quita la obligación de inscribir), o que cuentan con bases de datos y no están cumpliendo con la Ley de Protección de Datos Personales. Corresponde a la Autoridad de Protección de Datos revisar el cumplimiento de la normativa, fiscalizar y sancionar si considera que existen vulneraciones a la Ley y su Reglamento.

Conclusiones

- Los organismos del sistema electoral (JNE, ONPE y RENIEC) se encuentran bajo el ámbito de aplicación de la Ley de Protección de Datos personales.

- El JNE tiene bases de datos inscritas en el Registro Nacional de Datos Personales. Asimismo, se encarga de la administración del Registro de Organizaciones Políticas y el Padrón de afiliados de estos. Para su tratamiento no requiere consentimiento en virtud de la habilitación legal para ello. No obstante, ello no le exime del cumplimiento de obligaciones referidas a establecer un procedimiento para el ejercicio de derechos ARCO por parte de los titulares y de las medidas de seguridad respectivas.

- El JNE también es titular de un repertorio jurisprudencial. Este debería estar anonimizado, según lo dispuesto en el Reglamento de la Ley de Protección de Datos Personales. Sin embargo, en virtud del interés público detrás de este tipo de decisiones, esta obligación no debería ser exigible.

- ONPE también cuenta con bases de datos inscritas en el Registro Nacional de Datos Personales. La más relevante es la referida al Padrón Electoral. Si bien existen ciertos datos en el Padrón cuyo tratamiento no requiere consentimiento en virtud de habilitación legal, existen otros que, de acuerdo al Registro, sí deberían de requerir consentimiento y que resultan excesivos al tratamiento realizado. Más aún, que la recopilación de ciertos datos personales esté exenta de requerir el consentimiento, no exime del cumplimiento de las otras obligaciones y principios contemplados en la Ley de Protección de Datos Personales.

- RENIEC está encargado de la elaboración y actualización de una de las bases de datos más importante para un proceso electoral: el Padrón Electoral. No requieren autorización para su tratamiento y recopilación, en virtud de la Ley. Sin embargo, RENIEC debe cumplir con las medidas de seguridad correspondientes y habilitar un procedimiento para poder ejercer los derechos relativos a la protección de datos personales.

- No todos los datos que se encuentran en el Padrón Electoral son accesibles para las organizaciones políticas. Quedan exentos de su acceso datos biométricos (huella dactilar) y de domicilio.

- Las organizaciones políticas, al momento de recopilar y tratar datos personales, deben cumplir con las obligaciones establecidas en la Ley y su Reglamento. Entre estas, resaltamos las medidas de seguridad y los procedimientos necesarios para ejercer los derechos ARCO. Tomando en cuenta las recomendaciones de la Comisión Europea, estos deberían verificar que, si acceden a datos por terceros, estos sean obtenidos de manera lícita. Además, el tratamiento debe ser específico para la finalidad que fueron recopilados y, una vez estos ya no sean necesarios, eliminarlos.

Elecciones, datos personales y tecnologías

HIPERDERECHO

Tecnología como libertad