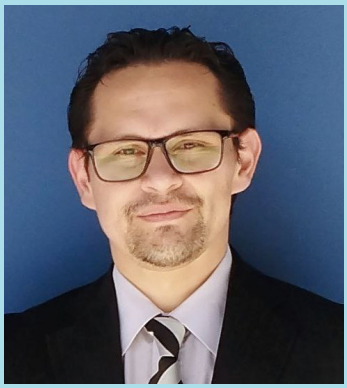
PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO ELECTORAL: ANÁLISIS DE LA LEGISLACIÓN ECUATORIANA

PROTECTION OF PERSONAL DATA IN THE ELECTORAL CONTEXT: ANALYSIS OF ECUADORIAN LEGISLATION



Darío Echeverría Muñoz

Abogado de los Tribunales y Juzgados de la República por la Universidad Central del Ecuador. Máster en Derecho Internacional de los Negocios por ESADE Law School, posee certificaciones como Delegado de Protección de Datos por la Universidad Andina Simón Bolívar y mediador por el Centro de Mediación "Jóvenes y Justicia". Es miembro activo de la Red Iberoamericana el Derecho Informático.

Actualmente, se desempeña como abogado en libre ejercicio, Director, Mediador y Docente en el Centro de Mediación "Jóvenes y Justicia", impartiendo la cátedra "Mediación y Tics" y la cátedra "Acceso a la Información y Protección de Datos" en el programa de Maestría en Derecho Digital mención Innovación Legal y Entorno Digital, también en el Programa de Legaltech y Protección de Datos de la Universidad de los Hemisferios. De igual modo, como maestrante en Derecho de la Economía Digital por la Universidad Andina Simón Bolívar del Ecuador.

Correo electrónico:
darioecmunoz@outlook.com
Sitio web: https://linktr.ee/darioecmunoz

- Fecha de recepción: 28/11/2023
- Fechas de revisión pares: 26/01/2024 - 09/02/2024
- Fecha de aceptación: 13/03/2024
- Fecha de publicación: 11/07/2024

RESUMEN

Este estudio ofrece un análisis crítico de cómo la legislación ecuatoriana protege los datos personales en el contexto electoral. Se centra en la Ley Orgánica de Protección de Datos Personales; y, la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia, examinando su impacto en la gestión de datos durante campañas y procesos electorales. Aborda la aplicación de principios de protección de datos, como minimización y consentimiento, y cómo afectan la confianza del electorado; así como las estrategias de campaña. Además, se efectúan comparaciones con regulaciones internacionales, identificando desafíos y oportunidades para mejorar la transparencia e integridad de los procesos electorales, concluyendo con recomendaciones para fortalecer la democracia en Ecuador.

PALABRAS CLAVE

Protección de datos personales, derechos de participación, democracia, privacidad, legislación política.

ABSTRACT

This study offers a critical analysis of how Ecuadorian legislation protects personal data in the electoral context. It focuses on the Organic Law on Personal Data Protection, Organic Law on Political and Electoral Organizations, Democracy Code, and examining their impact on data management during campaigns and electoral processes. It addresses the application of data protection principles, such as minimization and consent, and how they affect voter confidence and campaign strategies. In addition, comparisons are made with international regulations, identifying challenges and opportunities to improve the transparency and integrity of electoral processes. Finally, the article concludes with recommendations to strengthen the democracy in Ecuador.

KEYWORDS

Personal data protection, participation rights, democracy, privacy, political legislation.

Introducción

La expedición de la Ley Orgánica de Protección de Datos Personales en Ecuador, publicada en el Quinto Suplemento del Registro Oficial No. 459, el 26 de mayo de 2021, marca un hito fundamental en la regulación de la privacidad y la seguridad de la información personal, especialmente, en contextos sensibles como el electoral. Esta Ley responde a una creciente necesidad global de salvaguardar los datos personales frente a los desafíos impuestos por la digitalización y la era de la información. En este contexto, el presente estudio se enfoca en analizar cómo Ecuador, a través de su marco legal, aborda la protección de datos personales en el ámbito electoral, crucial para la integridad y transparencia de los procesos democráticos.

Específicamente, el trabajo se centra en la Ley Orgánica de Protección de Datos Personales, complementada por el

• ISSN 1390-8294 • e - ISSN 2960-8155

Código de la Democracia y el numeral 19, del artículo 66 de la Constitución de la República del Ecuador que reconoce el derecho a la protección de los datos de carácter personal; así como, la necesidad de autorización del titular para cualquier tipo de difusión, recolección o procesamiento. Estas normativas juntas forman un marco robusto para la protección de datos, asegurando la privacidad y la seguridad de la información de los ciudadanos en el entorno electoral. Más aún, la propia Constitución, en el mencionado artículo, establece un precedente claro para garantizar el derecho a la protección de datos personales, proporcionando un fundamento legal sólido para prevenir su mal uso en contextos electorales.

El artículo profundiza en cómo estas leyes se interrelacionan, examinando su aplicación práctica en la organización de elecciones, la gestión de campañas políticas y la participación ciudadana. Al desentrañar las complejidades de esta interacción legal, el objetivo es esclarecer el panorama actual de la protección de datos en Ecuador y proponer mejoras para reforzar la integridad y la transparencia de los procesos electorales. Este análisis busca contribuir a una comprensión más profunda de la importancia de la protección de datos en la democracia ecuatoriana, subrayando la relevancia de estas leyes en el fortalecimiento de un sistema electoral seguro y confiable.

1. Antecedentes de la protección de datos

El derecho a la protección de datos personales, actualmente, reconocido como un derecho autónomo, se origina en la protección de la libertad, el honor, la privacidad y la intimidad; principios arraigados en la historia del derecho. Este derecho encuentra sus cimientos en la Declaración de los Derechos del Hombre y del Ciudadano, emitida por la Asamblea Nacional Constituyente francesa en 1789, especialmente, en su artículo 1 que reconoce la libertad personal, así como los artículos 10 y 11 que enfatizan la libertad de opinión, bajo la condición de no perturbar el orden público. En ese sentido, se puede decir que el actual derecho a la protección de datos "corresponde a una parte de esa ejecución plena de las libertades otorgadas" (Villalba Fiallos, 2021), que fueron plasmadas en los primeros instrumentos que consagraban derechos fundamentales.

Con todo, el derecho a la protección de datos comienza a consolidarse -como tal- a finales del siglo XIX. En Estados Unidos, la noción del "derecho a estar solo" (traducido del inglés *"The right to be alone"*), fue conceptualizada por primera vez por Samuel D. Warren y Louis D. Brandeis en su artículo pionero "El derecho a la privacidad", publicado en el Harvard Law Review en 1890. Hay que tener en cuenta que esta noción, que sienta las bases del significado moderno de la privacidad, surge en un escenario en donde la fotografía, invención entonces

reciente y la difusión de información mediante los medios de comunicación, planteaba nuevos retos a este derecho (Huerta, 2023).

Por esta razón, el "derecho a ser dejado en paz" ha tenido una influencia significativa en la conformación del derecho a la protección de datos personales y se ha convertido en un pilar fundamental en el reconocimiento y protección de la privacidad personal como un derecho esencial, resaltando la importancia de proteger la vida privada de las personas frente a intrusiones no deseadas. En su esencia, este principio sostiene que cada individuo debe tener el derecho de controlar su información personal y cómo esta es utilizada o difundida.

Con el avance hacia la era digital, donde la información personal se genera, almacena y comparte a una escala sin precedentes, la relevancia de esta doctrina se ha magnificado. En un mundo interconectado, donde los datos personales pueden ser fácilmente accesibles y susceptibles de ser empleados de manera indebida, la necesidad de salvaguardar la privacidad se ha vuelto aún más crítica. Esto es, especialmente, pertinente en sectores sensibles como el electoral, donde la integridad de la información personal y la seguridad de los datos son esenciales para preservar la confianza en los procesos democráticos.

Así, el "derecho a estar solo" ha evolucionado desde su formulación original para abarcar la protección de datos personales en el contexto contemporáneo, subrayando la necesidad de legislaciones y políticas que protejan eficazmente la privacidad y seguridad de la información en la era digital. Esta doctrina ha influido en la creación de leyes y regulaciones tanto en Estados Unidos como en otros países, adaptándose y respondiendo a los desafíos emergentes de la tecnología y la sociedad moderna.

La importancia de este derecho se vio reforzada y ampliada en el contexto del siglo XX, tras las experiencias de la Segunda Guerra Mundial. Las atrocidades cometidas durante este conflicto, incluyendo el genocidio, evidenciaron la necesidad imperiosa de reafirmar y proteger los derechos humanos a nivel global. En este escenario, la Declaración Universal de Derechos Humanos (1948) emerge como un documento trascendental, jugando un papel crucial en la consolidación del derecho a la protección de datos personales.

Este documento, que fue aprobado por los que entonces eran los Estados miembros de la Organización de las Naciones Unidas (ONU), entre ellos Ecuador, prohíbe en su artículo 12 las injerencias arbitrarias en aspectos privados como la vida personal, la familia, el hogar o la correspondencia y protege contra ataques a la honra o reputación (1948). Este artículo es reconocido como un hito en el desarrollo y reconocimiento internacional del derecho a la protección de datos personales.

• ISSN 1390-8294 • e - ISSN 2960-8155

Este reconocimiento internacional del derecho a la privacidad sentó las bases para desarrollos legislativos más específicos y adaptados a las necesidades y contextos de diferentes regiones. En Estados Unidos, la doctrina del "derecho a estar solo" establecía un marco conceptual para la protección de la privacidad y los datos personales. Paralelamente, en Europa, se desarrollaron iniciativas legislativas que materializaban estos principios en leyes concretas.

La Ley de Protección de Datos de 1970 de Hesse en Alemania, redactada por el padre de la protección de datos Spiros Simitis, y legislaciones similares en otros países europeos, no solo siguieron la dirección marcada por la doctrina de Warren y Brandeis, sino que también aportaron elementos prácticos y específicos adaptados a sus propios contextos sociales y legales. Estas leyes europeas, enfocadas en los derechos de las personas sobre sus datos personales y en la implementación de medidas de protección, evidenciaron una evolución tangible de la teoría a la práctica en la protección de la privacidad y los datos personales.

Esta tendencia hacia un enfoque más estructurado y unificado en la protección de datos personales se refleja claramente en los desarrollos legislativos europeos y globales. El Convenio No.108 del Consejo de Europa de 1981 marcó un hito, al ser el primer instrumento jurídico vinculante a nivel internacional en esta materia, abordando aspectos transfronterizos cruciales del derecho a la protección de datos.

Posteriormente, en países como España, la legislación evolucionó con leyes como la Ley Orgánica 5/1992, conocida como LORTAD, que fue una de las primeras normativas específicas para la protección de datos personales, estableciendo reglas para el tratamiento automatizado de la información y sentando las bases para resguardar la privacidad, y los derechos individuales. Luego, la Ley Orgánica 15/1999 o LOPD, amplió y fortaleció estas disposiciones en línea con la Directiva 95/46/CE de la Unión Europea (UE) sobre protección de datos, asegurando así la compatibilidad de la legislación española con los estándares europeos y reforzando principios como el consentimiento del titular de los datos y el derecho a acceder, rectificar y cancelar datos personales.

Este proceso culminó con la adopción del Reglamento General de Protección de Datos (RGPD) por la UE en 2016, estableciendo un marco legal homogéneo para toda la región. La implementación de este reglamento en España y otros países miembros de la UE, a través de leyes como la Ley Orgánica 3/2018, demuestra un compromiso continuo con la protección de datos personales, reflejando una evolución hacia una legislación más robusta y coherente.

Este avance legislativo, a su vez, resalta la importancia creciente de adaptar las leyes a los desafíos tecnológicos y de garantizar la privacidad, además de la

seguridad de la información personal en diversos contextos, incluyendo el ámbito electoral.

2. Marco jurídico ecuatoriano de la protección de datos personales

En el contexto del marco jurídico ecuatoriano para la protección de datos personales, es fundamental clarificar ciertos conceptos clave. De acuerdo con (Enríquez Álvarez, 2018), se pueden distinguir varios términos relevantes en este ámbito:

- **Datos:** Se refiere a la información dispuesta de manera adecuada para su tratamiento por un ordenador. Esta definición subraya la naturaleza estructurada de los datos para su uso digital. Por tratamiento debe entenderse toda operación realizada en datos personales, mediante procedimientos automatizados o no, como la recopilación, registro, organización, conservación, transmisión, etc.

- **Metadatos:** Son datos acerca de los datos. Ejemplos comunes incluyen la fecha de creación o modificación de un archivo, el encabezado de un correo electrónico que detalla la ruta del mensaje o la dirección IP de origen.

- **Protección de Datos (Enfoque Técnico):** Implica salvaguardar la información para prevenir su pérdida o corrupción, resaltando la importancia de la seguridad informática.

- **Protección de Datos Personales (Enfoque Jurídico):** Es un mecanismo jurídico destinado para proteger el derecho a la vida privada. Refleja la transformación de toda actividad humana en datos digitales, enfatizando la importancia de resguardar esta información a nivel legal.

La evolución legislativa de la protección de datos personales en Ecuador tiene su origen en el reconocimiento del derecho a la privacidad, pero también en el derecho constitucional de inviolabilidad de correspondencia; posteriormente, se establece el *habeas data*, un mecanismo crucial incorporado en las reformas constitucionales del país. Este derecho posibilita a los individuos acceder a su información personal retenida por diversas instituciones, estableciendo una base legal esencial para la reclamación de datos personales. El *habeas data* no solo facilita el acceso a la información, sino que también resalta la importancia del consentimiento y el control sobre los datos personales. Este fundamento en la legislación ecuatoriana ha sido decisivo para sentar los cimientos de futuras regulaciones -más específicas- en el manejo y protección de los datos personales, marcando el comienzo de un enfoque integral hacia la privacidad y la seguridad de la información personal.

• ISSN 1390-8294 • e - ISSN 2960-8155

Avanzando en la evolución legislativa, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) marcó un avance importante al definir y regular la protección de datos personales, cuyo artículo 9 (actualmente derogado) prescribía:

> **Art. 9.- Protección de datos:** Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.
> La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.
>
> No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.
>
> El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

A pesar de ser una definición con alcance limitado, esta norma precisaba la necesidad del consentimiento expreso para la elaboración, transferencia o utilización de bases de datos, alineándose con los principios de privacidad, intimidad y confidencialidad garantizados por la Constitución.

Esto implicaba que las organizaciones debían contar con la autorización del titular de los datos antes de realizar cualquier tratamiento con los mismos. Sin embargo, su alcance era restringido, ya que únicamente regulaba la protección de datos personales en el contexto de la elaboración, transferencia o utilización de bases de datos derivadas del uso o transmisión de mensajes de datos, dejando de lado otros escenarios de recolección y tratamiento de datos personales.

De otra parte, la definición no contemplaba derechos de los titulares de los datos, como el derecho de acceso, rectificación, oposición o supresión ni obligaciones específicas para los responsables de su tratamiento, tampoco establecía un régimen sancionatorio claro ni mecanismos de control y supervisión para garantizar el cumplimiento de la norma.

Si bien la norma citada representaba un avance inicial, esta carecía de un marco regulatorio integral y detallado para la protección de datos personales, en comparación con las legislaciones más modernas y desarrolladas en esta materia. Aun así, sentó las bases para el reconocimiento de la necesidad del consentimiento y el respeto a los principios constitucionales de privacidad, intimidad y confidencialidad en el tratamiento de datos personales para asegurar un mayor respeto por su privacidad e intimidad en el entorno digital.

Siguiendo este progreso legislativo, la protección de datos personales alcanza un nuevo nivel con la Constitución de la República del Ecuador (2008), en la que se reconoce explícitamente el derecho a la protección de datos personales, como un derecho fundamental conforme lo determina el artículo 66, numeral 19:

> **Art. 66:** Se reconoce y garantizará a las personas:
>
> **19.** El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Este desarrollo es un cambio paradigmático que refuerza la necesidad de una regulación detallada y específica en este campo.

Posteriormente, con la Ley Orgánica de Protección de Datos Personales, publicada en el Quinto Suplemento del Registro Oficial No. 459, el 26 de mayo de 2021, se consolida el marco legal para la protección de datos personales en Ecuador, cuyo artículo 1 señala:

> **Art. 1.-Objeto y finalidad:** El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

Entre las ventajas y novedades que introduce esta Ley, se pueden destacar las siguientes:

- La ley consagra explícitamente la protección de datos personales como un derecho fundamental, tal y como lo establece la Constitución de la República del Ecuador. Este reconocimiento implica que las personas gocen de un mayor control sobre sus datos personales y pueden exigir su tutela frente a terceros.

- La ley implementa un marco legal completo y detallado para la protección de datos personales con la estipulación de principios, derechos,

• ISSN 1390-8294 • e - ISSN 2960-8155

obligaciones y mecanismos de tutela para garantizar un tratamiento adecuado de los datos personales por parte de las entidades públicas, privadas, nacionales y extranjeras.

– La ley requiere la autorización del titular o el mandato de la ley para la recolección, archivo, procesamiento, distribución o difusión de datos personales, lo que ayuda a proteger la privacidad de las personas.

– La ley exige a las entidades que traten datos personales que sean transparentes en sus actividades. Esto implica que deben informar a los titulares de datos sobre: finalidad del tratamiento, datos que se recopilan, destinatarios de los datos y derechos que les asisten.

– La ley establece obligaciones específicas para garantizar la seguridad de los datos personales, siendo obligación de las organizaciones la implementación de medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales frente a riesgos como la destrucción, pérdida, alteración, acceso no autorizado o divulgación indebida. En este sentido, la ley exige la implementación de un sistema de gestión de riesgos y la realización de evaluaciones de impacto cuando el tratamiento de datos personales pueda presentar un alto riesgo para los derechos y libertades de las personas.

– La ley dispone la creación de la Autoridad de Protección de Datos Personales, como un organismo independiente encargado de supervisar el cumplimiento de la ley y proteger los derechos de los titulares de datos, con la potestad para investigar denuncias, sancionar a las entidades que incumplan la ley y emitir dictámenes sobre la protección de datos personales.

Estas disposiciones tienen como objetivo proteger los derechos fundamentales de los ciudadanos ecuatorianos y garantizar que los datos personales se manejen de forma transparente y legal.

En el contexto del proceso electoral ecuatoriano, regulado por el Código de la Democracia, la protección de los datos personales de los votantes es un aspecto crucial. El referido Código, aunque no enfocado específicamente en la protección de datos, determina las bases para la organización y conducción de elecciones, implicando la necesidad de manejar con cuidado la información personal de los ciudadanos.

La Ley Orgánica de Protección de Datos Personales complementa este marco legal, asegurando que cualquier información personal recopilada, procesada y almacenada durante el proceso electoral se administre de acuerdo con los principios de seguridad, confidencialidad y respeto a la privacidad.

Por otro lado, el rol de las autoridades electorales en la implementación de estas leyes es esencial, deben asegurar que los sistemas utilizados para la inscripción de votantes, el conteo de votos y la publicación de resultados electorales estén protegidos contra accesos no autorizados, manipulación o pérdida de datos. La adecuada aplicación de la Ley Orgánica de Protección de Datos Personales y las disposiciones del Código de la Democracia aseguran un equilibrio entre la eficiencia administrativa de los procesos electorales y la protección de los derechos fundamentales de los ciudadanos en el ámbito de la privacidad y la seguridad de la información.

Regresando al contexto más amplio, en el Código de la Democracia ecuatoriano, se establecen normas que, aunque no se centren directamente en la protección de datos personales, tienen un impacto significativo en cómo estos se manejan durante los procesos electorales. Por ejemplo, las normas que rigen la inscripción de votantes son fundamentales, ya que determinan cómo se recopilan, almacenan y protegen los datos personales de los ciudadanos en el padrón electoral.

El artículo 78 del Código dispone que el Consejo Nacional Electoral (CNE) es responsable de organizar y elaborar el registro electoral, basándose en la información remitida por el Registro Civil o la entidad encargada de administrar el registro de personas. Este artículo también detalla cómo se estructuran los padrones electorales y las medidas para mantener la integridad y actualización de estos registros (2009). Dicha disposición resalta la importancia de mantener la integridad y actualización de los padrones electorales. Estos padrones, que forman la base para una gestión electoral precisa, deben ser administrados con rigurosos estándares de protección de datos. Este enfoque no solo asegura la precisión y relevancia de los registros electorales, sino el cumplimiento de las normativas de protección de datos, respetando la privacidad y los derechos individuales de los electores ecuatorianos.

Además, el artículo 78 subraya la inmutabilidad de los padrones entre las primeras y segundas vueltas electorales, reforzando así la estabilidad y la integridad del proceso electoral. Este mandato garantiza la coherencia y fiabilidad de los datos electorales, así como la protección de los derechos de los votantes al asegurar que su información personal no sea manipulada o alterada durante el período electoral. Por lo tanto, el artículo mencionado es clave en la gestión segura y transparente de los datos personales en el ámbito electoral, alineando las prácticas de registro y votación con los principios de protección de la información y la privacidad.

Con relación a los artículos 80, 82 y 83 del Código de la Democracia, es importante destacar que estas disposiciones, aunque enfocadas en aspectos técnicos y administrativos del proceso electoral, también tienen una relevancia directa en la protección de datos personales.

• ISSN 1390-8294 • e - ISSN 2960-8155

Estos artículos remarcan los derechos de los ciudadanos a tener sus datos personales correctamente representados y actualizados en los registros electorales. Por ejemplo, el derecho a su rectificación y actualización se ve reflejado en la posibilidad de modificar el domicilio electoral o de incluirse en el registro para futuros procesos electorales, si se obtiene la cédula de identidad después del cierre del registro.

Los referidos derechos y su aplicación en la esfera electoral ecuatoriana serán explorados a profundidad en el siguiente subtítulo, donde se analizará la relevancia de la Ley Orgánica de Protección de Datos Personales con relación a los derechos individuales de acceso, rectificación, cancelación y oposición; así como, el consentimiento en el manejo de los datos personales. Este análisis destacará cómo la legislación ecuatoriana busca equilibrar la eficiencia y la integridad del proceso electoral con la protección de los derechos de privacidad de los ciudadanos en un entorno cada vez más digitalizado y centrado en los datos.

Dichas disposiciones tienen un papel crítico en garantizar que los datos personales se manejen de manera segura y confidencial, respetando los derechos de privacidad de los votantes. Estas normas son fundamentales para asegurar la protección de los datos personales de los ciudadanos. Estas disposiciones, establecidas en el Código de la Democracia y la Ley Orgánica de Protección de Datos Personales, comprenden un conjunto de normas y principios que regulan la recolección, almacenamiento, uso y divulgación de la información personal de los votantes.

Un aspecto clave de estas normas es la obligación del CNE de implementar medidas de seguridad adecuadas para proteger los datos personales de los votantes. Estas deben ser de carácter físico, técnico y administrativo, y estar orientadas a prevenir el acceso no autorizado, la divulgación indebida, la pérdida o alteración de la información.

Además, la ley establece que los datos personales de los votantes solo pueden ser utilizados para los fines específicos para los que fueron recolectados, es decir, para la organización, desarrollo y realización de procesos electorales. El CNE no puede utilizarlos para ningún otro propósito que la ley no haya establecido.

La gestión y divulgación de los resultados electorales, que incluyen datos personales, también está sujeta a estrictas normas de seguridad y confidencialidad. El CNE debe adoptar todas las medidas necesarias para garantizar que la información personal de los votantes no sea revelada de manera no autorizada.

La protección de datos personales en el ámbito electoral de Ecuador constituye un reto complejo que abarca múltiples facetas legales y prácticas. Es fundamental la coherencia entre el Código de la Democracia, que rige los derechos y obligaciones de participación

político-electoral, y la Ley Orgánica de Protección de Datos Personales, para lograr un equilibrio entre la eficiencia del proceso electoral, así como la protección de la privacidad y seguridad de los datos personales.

Esta intersección legislativa no solo asegura la salvaguarda de los datos personales durante los procesos electorales, sino también fomenta un entorno democrático transparente y seguro. La adecuada implementación de estas leyes es crucial para reforzar la confianza pública en el sistema electoral de Ecuador, subrayando el compromiso del país con la integridad democrática y el respeto a los derechos individuales.

3. Contexto electoral en el Ecuador para la aplicación del derecho de protección de datos personales

En el dinámico entorno de las elecciones en Ecuador, la aplicación de la Ley Orgánica de Protección de Datos Personales cobra una importancia crítica. Este escenario, caracterizado por el flujo intensivo y el manejo de información personal, plantea desafíos únicos y resalta la necesidad de un enfoque meticuloso en la protección de datos personales. Desde la creación de listas electorales hasta la ejecución de campañas políticas; el tratamiento de datos personales se encuentra en el corazón del proceso democrático.

En la esfera electoral, la Ley Orgánica de Protección de Datos Personales de Ecuador adquiere una relevancia particular. El artículo 2 establece el ámbito de aplicación material de la ley, incluyendo todos los datos personales, independientemente de su soporte. Esto implica que, en actividades electorales, donde se manejan grandes volúmenes de datos personales, tanto en formatos digitales como en papel, cada detalle debe ser tratado conforme a esta Ley. El ámbito de aplicación de la ley incluye el manejo de estos principios con relación a los datos personales de ciudadanos ecuatorianos dentro y fuera del país. Esto es especialmente relevante en un mundo cada vez más conectado, donde las campañas electorales pueden operar a través de fronteras nacionales.

Lo que significa que, en actividades electorales, donde se manejan grandes volúmenes de datos personales, cada detalle debe ser tratado de manera integral al tratamiento de datos personales en cualquier soporte, ya sea automatizado o no, y a cualquier modalidad de tratamiento posterior en el ámbito electoral. Por su parte, las excepciones mencionadas en este artículo delinean claramente los límites dentro de los cuales los datos personales no se aplican a ciertas situaciones específicas, como:

- **Actividades domésticas:** El tratamiento de datos personales no se aplica al ámbito familiar o doméstico. Esto significa que el tratamiento de datos dentro del hogar, entre familiares y amigos cercanos, no está sujeto a las regulaciones de la ley.

• ISSN 1390-8294 • e - ISSN 2960-8155

- **Personas fallecidas:** La ley no regula el tratamiento de datos de personas fallecidas; sin embargo, los titulares de derechos sucesorios o las personas o instituciones designadas por el fallecido pueden ejercer los derechos de acceso, rectificación, actualización y eliminación de los datos del fallecido ante el responsable del tratamiento, acreditando su comparecencia a través de los instrumentos legales reconocidos por el ordenamiento jurídico ecuatoriano.

- **Datos anonimizados:** El tratamiento de datos personales no se aplica a datos anonimizados, es decir, aquellos donde la identidad del titular no puede ser determinada. Sin embargo, si la anonimización se revierte, el tratamiento de los datos queda sujeto a la ley.

- **Actividades periodísticas y contenidos editoriales:** El tratamiento de datos personales en el contexto periodístico o editorial no está regulado por la ley.

- **Datos con normativa especializada:** La ley no se aplica a datos cuyo tratamiento esté regulado por normativa específica de igual o mayor jerarquía, como en materia de gestión de riesgos por desastres naturales, seguridad y defensa del Estado. En estos casos, se deben cumplir estándares internacionales de derechos humanos y principios de la Ley Orgánica de Protección de Datos Personales; además de criterios de legalidad, proporcionalidad y necesidad.

- **Datos para prevenir o investigar delitos:** La ley no regula el tratamiento de datos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales por parte de organismos estatales competentes. En estos casos, se deben cumplir estándares internacionales de derechos humanos, principios de la Ley Orgánica de Protección de Datos Personales y criterios de legalidad, proporcionalidad y necesidad.

- **Datos de personas jurídicas:** La ley no regula el tratamiento de datos que identifican o hacen identificable a personas jurídicas. Sin embargo, ciertos datos de profesionales, comerciantes, representantes, socios, accionistas y servidores públicos son accesibles al público y susceptibles de tratamiento, siempre que se refieran al ejercicio de su actividad. En el caso de servidores públicos, también se considera información de acceso público y susceptible de tratamiento, el historial y la remuneración actual de la declaración patrimonial; esto de acuerdo con los principios de transparencia y acceso a la información pública.

El concepto de consentimiento es esencial en la protección de datos

personales. Según el artículo 7 de la Ley Orgánica de Protección de Datos Personales de Ecuador (2021), el consentimiento se define como la manifestación de voluntad, libre, específica, informada e inequívoca, por la cual el titular de los datos acepta el tratamiento de sus datos personales. Esta definición es coherente con la del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que también enfatiza la importancia de un consentimiento libre, específico, informado e inequívoco.

La relevancia del consentimiento radica en su capacidad para empoderar a los individuos sobre el uso de sus datos personales. Al requerir consentimiento, se asegura que los individuos tienen control sobre cómo y cuándo se utilizan sus datos, lo cual es fundamental en la preservación de la privacidad y la autonomía personal. En el ámbito electoral, donde los datos personales son especialmente sensibles, el consentimiento garantiza que los ciudadanos estén conscientes y de acuerdo con la forma en que su información es utilizada en los procesos democráticos.

Existen situaciones excepcionales en las que la recopilación y el tratamiento de datos personales pueden realizarse sin el consentimiento del titular, particularmente, en el contexto electoral:

- **Interés público o ejercicio de poderes públicos:** Se refiere a situaciones donde el tratamiento y recopilación de datos personales es necesario para realizar tareas que benefician al público o que son parte de las funciones oficiales de una entidad gubernamental. Por ejemplo, la recopilación de datos personales de los votantes por parte de la autoridad electoral para garantizar elecciones libres y justas.

- **Cumplimiento de obligaciones legales:** Implica el tratamiento de datos personales necesario para cumplir con leyes y reglamentos aplicables. En la esfera electoral, permite crear y mantener registros electorales actualizados, lo cual es una obligación legal de las autoridades electorales.

- **Protección de intereses vitales:** Este término se refiere al tratamiento de datos personales que es fundamental para proteger los aspectos básicos de la vida de una persona natural. Esto, generalmente, se aplica en situaciones críticas donde la salud o la seguridad de alguien está en riesgo. Por ejemplo, si un votante sufre una emergencia médica en un centro de votación, los datos personales del votante, como su nombre y condiciones de salud, podrían ser compartidos con los servicios médicos para garantizar una atención rápida y adecuada.

- **Ejercicio o defensa de reclamaciones legales:** El tratamiento de datos personales es necesario para establecer, ejercer o defender reclamaciones

• ISSN 1390-8294 • e - ISSN 2960-8155

legales. Por ejemplo, utilizar datos personales en el marco de un litigio relacionado con disputas electorales.

– **Realización de actividades de interés público:** Se relaciona con el tratamiento de datos personales por autoridades para llevar a cabo actividades que benefician al público. En el ámbito electoral, el uso de datos personales por parte de las autoridades electorales para realizar análisis demográficos y asegurar la equidad en la distribución de lugares de votación.

Estas excepciones subrayan la importancia de un equilibrio entre la eficiencia del proceso electoral y la protección de los derechos individuales en el ámbito de la privacidad y seguridad de los datos. La integración de las disposiciones del Código de la Democracia y la Ley Orgánica de Protección de Datos Personales es fundamental para garantizar este equilibrio.

En el contexto electoral, el tratamiento de datos personales adquiere una dimensión particularmente significativa. En esta esfera, los datos personales no son solo un medio para un fin, sino un elemento crucial que impulsa todo el proceso democrático. La finalidad de este tratamiento va más allá de la mera gestión administrativa, tiene el objetivo de sostener la integridad y la transparencia del proceso electoral, asegurando que cada etapa, desde la inscripción de votantes hasta la publicación de resultados, se desarrolle con la mayor precisión y justicia posible.

Ahora bien, el tratamiento de datos personales en el campo electoral es un proceso fundamental que incluye la recopilación, almacenamiento, uso y divulgación de información personal de los votantes. Esta información se utiliza para una variedad de propósitos, desde la creación de registros electorales hasta la personalización de campañas políticas. Su objetivo es garantizar una administración eficiente y transparente del proceso electoral, asegurando la exactitud de los registros electorales y facilitando la comunicación efectiva entre candidatos, partidos políticos y votantes.

En este marco, es primordial reconocer los roles clave definidos en el artículo 4 Ley Orgánica de Protección de Datos Personales de Ecuador para la gestión y protección de datos personales:

– **Titular:** Se refiere a la persona natural cuyos datos personales son objeto de tratamiento.

– **Responsable de Datos:** Se refiere a la persona natural o jurídica, pública o privada, que determina los fines y medios del tratamiento de datos personales. Tiene la responsabilidad principal de garantizar que el manejo de los datos se realice conforme a la ley, asegurando la protección y privacidad de los datos personales.

– **Encargado de Tratamiento:** Es la persona o entidad que realiza el tratamiento de datos personales por cuenta del responsable. Aunque actúa bajo las instrucciones del responsable, debe asegurar que el tratamiento se adhiera a las normativas pertinentes y a las mejores prácticas de protección de datos.

La claridad en estos roles es vital para mantener la integridad y confianza en el proceso electoral, especialmente, en lo que respecta a la confidencialidad y seguridad de los datos personales de los votantes. Un manejo adecuado y claro de estas responsabilidades es esencial para asegurar la transparencia y eficacia en el tratamiento de datos personales, un pilar fundamental para la confianza pública en el sistema electoral.
En el ámbito electoral, el responsable juega un papel crucial, ya que es la autoridad que determina cómo y por qué se procesan los datos personales de los votantes. Esto incluye decisiones sobre la recopilación, almacenamiento y uso de información sensible, como las preferencias políticas y los datos de identificación de los votantes. La responsabilidad del responsable es asegurar que todas estas actividades se realicen de manera transparente, segura y conforme a la legislación vigente. Esto es, sustancialmente, importante durante las elecciones, donde la integridad de los datos personales es básica para la legitimidad del proceso electoral.

Por otro lado, el "encargado de tratamiento" es responsable de ejecutar las operaciones de procesamiento de datos de acuerdo con las instrucciones del responsable. En el contexto electoral, esto puede incluir la gestión de bases de datos electorales, la supervisión de la logística de las votaciones y la garantía de que la información personal de los votantes se maneje de manera confidencial y segura. El encargado también debe implementar medidas técnicas y organizativas adecuadas para proteger los datos contra el acceso no autorizado o el procesamiento ilegal, mitigando los riesgos asociados con la manipulación de datos en un entorno tan sensible como el electoral.

La eficacia en el desempeño de estos roles es imprescindible para asegurar la protección de la privacidad de los votantes; así como para fortalecer la confianza y la integridad en el sistema democrático de Ecuador. Una gestión efectiva y conforme a la ley de los datos personales durante los procesos electorales es, por tanto, un elemento esencial para el mantenimiento de una democracia saludable y transparente.

La Ley Orgánica de Protección de Datos Personales del Ecuador establece un marco sólido para el tratamiento adecuado y legítimo de los datos personales, enfatizando los derechos conocidos como Derechos ARCO. Estos derechos permiten a los titulares ejercer un control significativo sobre sus datos personales:

– **Derecho de información:** Consagrado en el artículo 12 de la Ley, permite

• ISSN 1390-8294 • e - ISSN 2960-8155

a los titulares estar plenamente informados sobre el tratamiento de sus datos personales. Esto incluye conocer los fines específicos para los cuales se tratan sus datos, quién es el responsable de su tratamiento y bajo qué fundamentos legales se justifica dicho tratamiento. En el ámbito electoral, este derecho asegura que los votantes estén conscientes de cómo y por qué los partidos políticos y las autoridades electorales manejan su información personal. Este marco de transparencia y lealtad es esencial para fomentar la confianza en los procesos electorales y asegurar que los ciudadanos puedan ejercer sus derechos de manera informada.

- **Derecho de acceso:** Este derecho establecido en el artículo 13 de la Ley, permite a los ciudadanos conocer qué datos personales suyos están siendo tratados, quién los está tratando y con qué finalidad. En el ámbito electoral, esto significa que los votantes pueden solicitar a los partidos políticos y autoridades electorales información sobre los datos personales que tienen de ellos, incluyendo cómo y por qué se utilizan en el proceso electoral.

- **Derecho de rectificación:** De acuerdo con el artículo 14 de la Ley, este derecho permite a los titulares corregir los datos personales que sean inexactos o incompletos. En el campo electoral es esencial para asegurar la precisión en los registros electorales y en la distribución de material de campaña, permitiendo a los votantes corregir errores en sus datos.

- **Derecho de eliminación:** También conocido como "derecho de supresión o de cancelación", según lo establecido en el artículo 15 de la Ley, este derecho posibilita a los titulares solicitar la eliminación de sus datos cuando ya no sean necesarios para los fines para los que fueron recogidos o si retiran su consentimiento para su tratamiento. Aplicado al contexto electoral, los votantes pueden solicitar que sus datos sean eliminados de las listas de contacto de campañas políticas.

- **Derecho de oposición:** Como lo dispone el artículo 16 de la Ley, este derecho permite a los titulares oponerse al tratamiento de sus datos personales, especialmente, para fines específicos como el marketing político. Dentro del campo electoral, los ciudadanos pueden oponerse al manejo de sus datos personales, sobre todo si se utilizan para fines de mercadotecnia política.

- **Derecho a la portabilidad de los datos:** Según lo dispuesto en el artículo 18 de la Ley, este derecho permite a los titulares recibir sus datos personales en un formato estructurado y transmitirlos a otro responsable del tratamiento. Además, facilita a los votantes la transferencia de sus datos personales entre distintas autoridades electorales o partidos políticos, asegurando el control sobre estos.

- **Derecho a la suspensión del tratamiento:** Conforme lo prescrito en el artículo 19 de la Ley, los titulares pueden solicitar que se suspenda el tratamiento de sus datos personales bajo ciertas condiciones. Este derecho permite a los votantes restringir cómo sus datos personales son utilizados en actividades electorales, por ejemplo, limitando su uso para determinadas campañas.

- **Derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles:** El artículo 20 de la Ley garantiza que los titulares no sean objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ellos o les afecte significativamente de modo similar. Asegurando que los votantes no sean sujetos a decisiones políticas o electorales basadas en el análisis automatizado de sus datos, como podría ser la selección de audiencias para publicidad política.

En campañas electorales, donde se recopilan y utilizan datos personales de votantes para una variedad de propósitos, desde la difusión de información hasta la organización de eventos, es imperativo que estas actividades se alineen con estos derechos. Las entidades responsables deben garantizar que los electores puedan ejercer su derecho a controlar cómo se emplean sus datos personales.

En el marco de la Ley Orgánica de Protección de Datos Personales de Ecuador, el artículo 4, que se refiere a los términos y definiciones, reconoce distintas clases de datos personales, cada una con sus propias implicaciones y requisitos de protección:

- **Dato Biométrico:** Dato personal único relacionado con características físicas, fisiológicas o conductas que permiten la identificación única de una persona, como imágenes faciales o datos dactiloscópicos.

- **Dato Genético:** Dato personal único vinculado a características genéticas que proporcionan información única sobre la fisiología o salud de un individuo.

- **Dato Personal:** Cualquier dato que identifica o hace identificable a una persona natural.

- **Datos Personales Crediticios:** Datos que reflejan el comportamiento económico de personas naturales para analizar su capacidad financiera.

- **Datos Relativos a la Salud:** Datos personales relacionados con la salud física o mental de una persona, incluyendo la prestación de servicios de atención sanitaria.

- **Datos Sensibles**: Incluyen datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial,

• ISSN 1390-8294 • e - ISSN 2960-8155

condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación o atentar contra los derechos y libertades fundamentales.

En comparación con el Reglamento General de Protección de Datos de la Unión Europea (RGPD), la Ley Orgánica de Protección de Datos Personales de Ecuador presenta un enfoque similar, pero más detallado en la clasificación de los datos sensibles. Mientras el RGPD en su artículo 9.1 se centra en prohibir el tratamiento de ciertos tipos de datos sensibles como el origen étnico, las opiniones políticas, las convicciones religiosas o filosóficas y los datos biométricos; el artículo 4 de la ley ecuatoriana citada, amplía esta categoría para incluir elementos como la identidad de género, la identidad cultural y el pasado judicial. Este enfoque refleja una comprensión más amplia de la diversidad de datos que pueden ser sensibles en diferentes contextos culturales y sociales.

En la esfera electoral, el manejo de datos sensibles, particularmente las preferencias políticas de los votantes, es un aspecto crítico que requiere un cuidado meticuloso. La privacidad individual es fundamental en este escenario, donde la información sobre las inclinaciones políticas puede ser especialmente delicada. Por ello, es esencial que el tratamiento de estos datos se realice con la máxima precaución, asegurando que se utilicen exclusivamente para los fines específicos para los que fueron recopilados, como podría ser la creación de registros electorales o la personalización de campañas políticas.

La personalización responsable de campañas políticas debe basarse en datos agregados y anonimizados, cumpliendo con estrictos requisitos de transparencia y consentimiento. Los votantes deben ser informados claramente sobre cómo se utilizarán sus datos y tener la posibilidad de negarse a que se recopilen o utilicen para este fin. Este enfoque permite mejorar la comunicación con los votantes, proporcionar información relevante sobre los candidatos y las propuestas, y fomentar la participación electoral, todo ello sin comprometer la privacidad individual.
Además, la integridad del proceso electoral depende de que estos datos se manejen de manera ética y segura, evitando cualquier riesgo de manipulación o uso indebido que podría influir en el resultado electoral o comprometer la confianza en el sistema democrático. Esto implica implementar medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados o filtraciones, así como asegurar que se respeten los principios de la ley en cada paso del tratamiento de estos datos sensibles.

La seguridad en el tratamiento de datos personales es un aspecto crítico para proteger la información contra accesos no autorizados, alteraciones o pérdidas. Para garantizar la integridad

y confidencialidad de los datos, se deben implementar medidas técnicas y organizativas adecuadas. Dentro de este marco, la ley en su artículo 39 establece dos conceptos fundamentales:

- **Protección de datos desde el diseño:** Este principio implica que la protección de datos debe ser una consideración integral desde la fase inicial de diseño de cualquier sistema o proceso que implique tratamiento de datos personales. En el ámbito electoral, resulta particularmente relevante, ya que las plataformas y herramientas utilizadas para gestionar datos electorales deben ser diseñadas con medidas de seguridad robustas desde el inicio. Esto garantiza que la protección de datos no es una adición posterior, sino una parte integral del diseño del sistema.

- **Protección de datos por defecto:** Paralelamente, el principio de protección por defecto asegura que solo se traten los datos necesarios para cada fin específico, minimizando así la exposición de datos personales. Este enfoque exige que, por defecto, los sistemas y procesos recojan, procesen y almacenen la mínima cantidad de datos necesarios para lograr su objetivo. En el campo electoral, esto significa que solo se recopilan los datos esenciales de los votantes, como nombre, dirección y datos de contacto, y se evita cualquier recolección innecesaria de información adicional.

En el escenario electoral, estas medidas se traducen en sistemas de votación electrónica y bases de datos de votantes diseñadas para maximizar la seguridad y minimizar el riesgo de acceso no autorizado. Por ejemplo, un sistema de votación electrónica puede incorporar encriptación avanzada y autenticación de votantes para proteger la integridad del voto. Paralelamente, las bases de datos de votantes pueden limitar el acceso a la información solo a personal autorizado, cumpliendo así con los requisitos de seguridad y privacidad.

En el contexto de la protección de datos personales, es fundamental comprender la distinción entre amenaza y vulnerabilidad:

- **Amenaza:** Se refiere a cualquier evento o acción que podría comprometer la seguridad y privacidad de los datos personales. Estas amenazas pueden ser intencionales (como un ataque cibernético) o no intencionales (como un error humano o un desastre natural). **Ejemplo:** Un hacker intenta robar datos personales de una base de datos de votantes.

- **Vulnerabilidad:** Es una debilidad o fallo en un sistema de tratamiento de datos personales que podría ser explotado por una amenaza para causar daño. Las vulnerabilidades pueden encontrarse en aspectos técnicos, organizativos o físicos del sistema. Ejemplo: La base de datos de votantes tiene una contraseña débil que el hacker puede adivinar.

• ISSN 1390-8294 • e - ISSN 2960-8155

Es importante destacar que la presencia de una vulnerabilidad no garantiza que se materialice una amenaza, pero sí aumenta la probabilidad de que ocurra un incidente de seguridad. Por lo tanto, la gestión de riesgos en el tratamiento de datos personales debe enfocarse en identificar, evaluar y mitigar tanto las amenazas como las vulnerabilidades.

Al comprender la distinción entre amenaza y vulnerabilidad, las autoridades electorales pueden implementar estrategias de seguridad más efectivas para proteger los datos personales de los votantes y asegurar la integridad de los procesos electorales.

La gestión de riesgos en el tratamiento de datos personales es primordial en el ámbito electoral. En este marco, un riesgo se refiere a cualquier posibilidad de evento o acción que podría comprometer la confidencialidad, disponibilidad e integridad de los datos personales, de acuerdo con lo dispuesto en el artículo 4 de la Ley.

Identificar, evaluar y mitigar estos riesgos es crucial para asegurar que los derechos de privacidad de los individuos se mantengan y que la integridad del proceso electoral se preserve. Dentro de esta categoría se dan los siguientes riesgos:

- **Riesgos Internos:** Son aquellos que surgen dentro de la organización o entorno operativo. Pueden incluir errores humanos, como el manejo inadecuado de datos por parte de los empleados o incluso acciones intencionadas, como la manipulación indebida de la información electoral por parte del personal interno. Estos riesgos pueden mitigarse mediante una formación adecuada, políticas claras y controles internos eficaces.

- **Riesgos Externos:** Se originan fuera de la organización y pueden incluir ciberataques destinados a manipular o robar datos electorales, así como otras formas de interferencia externa. La protección contra estos riesgos requiere una infraestructura de seguridad informática sólida y un monitoreo constante de las amenazas potenciales.

De conformidad con el artículo 40 de la Ley Orgánica de Protección de Datos Personales, para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras:

1) Las particularidades del tratamiento;
2) Las particularidades de las partes involucradas; y,
3) Las categorías y el volumen de datos personales objeto de tratamiento.

Además de lo anterior, es importante destacar que la Ley Orgánica de Protección de Datos Personales, en su artículo 42, establece la obligación de realizar una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de

que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.

Esta evaluación de impacto debe considerar, al menos, los siguientes aspectos:

- La naturaleza, el alcance, el contexto y los fines del tratamiento de datos personales.
- Los riesgos que el tratamiento presenta para los derechos y libertades de las personas físicas.
- Las medidas de seguridad y protección de datos personales que se implementarán para mitigar dichos riesgos.

Es importante mencionar que esta obligación de realizar una evaluación de impacto es concordante con lo establecido en el artículo 35 del RGPD, el cual dispone que el responsable del tratamiento deberá realizar una evaluación de impacto cuando sea probable que un tipo de tratamiento utilice nuevas tecnologías o que por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Los requisitos de la evaluación de impacto dispuestos en el RGPD son similares a los establecidos en la Ley Orgánica de Protección de Datos Personales. Sin embargo, el RGPD detalla algunos requisitos adicionales, como la consulta previa a la autoridad de control en determinados casos.

En el caso del tratamiento de datos personales en el ámbito electoral, es fundamental realizar una evaluación de impacto exhaustiva, ya que este tipo de tratamiento conlleva un alto riesgo para los derechos y libertades de los ciudadanos.

La evaluación de impacto, como se ha mencionado, es una herramienta fundamental para identificar y clasificar los riesgos potenciales asociados al tratamiento de datos personales. Esta información es esencial para desarrollar e implementar estrategias de gestión de riesgos efectivas que, en el contexto electoral implica una serie de acciones y estrategias específicas:

- **Evaluación Continua de Riesgos:** Las autoridades electorales deben realizar evaluaciones periódicas para identificar y clasificar los riesgos potenciales, tanto internos como externos.
- **Implementación de Medidas de Seguridad:** Esto incluye sistemas de seguridad informática avanzados, políticas de acceso a la información y mecanismos de autenticación robustos para prevenir accesos no autorizados y ataques cibernéticos.
- **Formación y Concienciación del Personal:** Capacitar al personal en buenas prácticas de seguridad de la

• ISSN 1390-8294 • e - ISSN 2960-8155

información y concienciar sobre los riesgos y cómo evitarlos.

– **Planes de Respuesta a Incidentes:** Desarrollar y mantener planes de acción para responder eficientemente, en caso de que se materialice un riesgo, minimizando el impacto.

– **Revisión y Mejora Continua:** Revisar regularmente las estrategias y prácticas de gestión de riesgos para mejorarlas y adaptarlas a nuevas amenazas o cambios en el entorno.

El conocimiento y la implementación efectiva de la gestión de riesgos son vitales para las organizaciones políticas. En este contexto, contar con un Delegado de Protección de Datos (DPO) se vuelve crucial. El DPO no solo asesora y supervisa el cumplimiento de la normativa, sino que también juega un papel clave en la evaluación de riesgos y en la implementación de medidas de seguridad; sus funciones incluyen asesoramiento, supervisión, evaluación y cooperación con la Autoridad de Protección de Datos Personales. Este profesional se convierte en un componente esencial para garantizar la seguridad de los datos en el ámbito electoral y más allá.

A partir del análisis realizado, se desprenden las siguientes implicaciones para el ámbito electoral:

– **Manejo responsable de datos:** Las autoridades electorales, partidos políticos y demás actores involucrados en procesos electorales deben manejar los datos personales de los votantes con responsabilidad y apego a la normativa vigente.

– **Medidas de seguridad:** Se deben implementar medidas de seguridad adecuadas para proteger los datos personales contra acceso no autorizado, divulgación indebida, pérdida, alteración o destrucción.

– **Transparencia:** Se debe brindar información clara y transparente sobre la finalidad del tratamiento de los datos y los derechos que asisten a los titulares.

– **Finalidad específica:** Los datos personales solo pueden ser utilizados para los fines específicos para los cuales fueron recabados, es decir, para la organización y realización de procesos electorales.

– **Prohibición de uso indebido:** El uso de datos personales para fines distintos a los electorales o para obtener beneficios políticos o económicos está expresamente prohibido.

– **Garantías para los votantes:** Los votantes tienen derecho a acceder a sus datos personales, solicitar su rectificación, supresión o limitación del tratamiento y a oponerse al mismo.

La Ley Orgánica de Protección de Datos Personales establece un marco legal

robusto para la protección de datos personales en el contexto electoral ecuatoriano. El cumplimiento efectivo de esta Ley por parte de todos los actores involucrados es fundamental para garantizar el derecho a la privacidad de los votantes y la integridad de los procesos electorales.

Es crucial que las autoridades electorales y demás actores relevantes adopten un enfoque proactivo en la protección de datos personales, implementando las medidas técnicas y organizativas necesarias para cumplir con la ley y garantizar la confianza de la ciudadanía en los procesos electorales.

4. Análisis comparativo de casos sancionados en la Protección de Datos Electorales

La protección de datos personales en el escenario electoral es un aspecto crucial, tanto en la Unión Europea como en América Latina. Analizando casos específicos de España, se puede apreciar el abordaje de estas infracciones como se mencionan a continuación.

4.1 Análisis del procedimiento sancionador PS/00341/2019 y el recurso de reposición Nº RR/00405/2020

4.1.1. Resumen del caso

El Partido Socialista de Cataluña (PSC-PSOE) fue objeto de una sanción por parte de la Agencia Española de Protección de Datos (AEPD) debido a la infracción del artículo 21 del Reglamento General de Protección de Datos (RGPD). La sanción se basó en el envío de propaganda electoral a personas que, expresamente, habían manifestado su oposición a recibirla, lo que constituía una clara vulneración del derecho de oposición al tratamiento de datos personales.

4.1.2. Resolución y apelación

La sanción inicial impuesta por la AEPD consistió en un apercibimiento, considerando las circunstancias específicas del caso y la necesidad de que el partido adoptara medidas para prevenir futuras infracciones. No obstante, el PSC-PSOE presentó un recurso de reposición, identificado como Nº RR/00405/2020, con el objetivo de apelar la decisión.

En el marco de este recurso, la AEPD ratificó la sanción impuesta y la convirtió en una multa de 5.000 euros. La multa se basó en la infracción del artículo 5.1.b) del RGPD, catalogada como una falta muy grave, según lo establecido en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. La infracción se relacionaba con el envío de cartas solicitando apoyo electoral, utilizando para ello datos personales obtenidos de manera indebida. Es importante destacar que el recurso de reposición presentado por el PSC-PSOE fue declarado inadmisible por extemporaneidad.

• ISSN 1390-8294 • e - ISSN 2960-8155

4.1.3. Implicaciones legales y contextuales

El caso del PSC-PSOE evidencia la importancia de respetar la voluntad de los electores y garantizar la protección de sus datos personales. La conducta del partido, al enviar propaganda electoral sin el consentimiento expreso de los destinatarios y utilizar datos personales de forma inapropiada, pone de relieve la responsabilidad que recae sobre los actores políticos de gestionar la información personal de manera ética y legal, especialmente en el contexto electoral.

La aplicación rigurosa de sanciones por infracciones electorales graves demuestra el firme compromiso con la protección de los derechos electorales y de privacidad. Esto, a su vez, contribuye a reforzar la confianza en el proceso democrático y en la protección efectiva de los datos personales en el ámbito político y electoral.

La atención cuidadosa y el cumplimiento estricto de estas normativas son pilares fundamentales para mantener la integridad y la confianza en los sistemas democráticos y electorales del país.

4.2 Análisis detallado del procedimiento sancionador PS/00449/2019

4.2.1. Resumen del caso

La Agencia Española de Protección de Datos (AEPD) impuso una sanción de 5.000 euros al Partit dels Socialistes de Catalunya (PSC-PSOE) por la infracción del artículo 5.1.b) del Reglamento General de Protección de Datos (RGPD). La sanción se basó en el uso indebido de datos personales para enviar cartas de propaganda electoral, utilizando datos facilitados por un médico sin el consentimiento expreso de los pacientes. La AEPD calificó esta infracción como muy grave, al considerar que contravenía los principios de limitación de la finalidad y responsabilidad proactiva del responsable del tratamiento de datos.

4.2.2. Resolución

La Agencia Española de Protección de Datos (AEPD) adoptó diversas medidas contra el PSC-PSOE. En primer lugar, impuso una multa de 5.000 euros al partido político. Además, el PSC-PSOE debía eliminar los datos personales que había utilizado de forma indebida. Por otro lado, se le exigió adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales en el futuro. Cabe mencionar que el PSC-PSOE tenía la posibilidad de recurrir la resolución ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

4.2.3. Implicaciones legales y contextuales

El caso del PSC-PSOE resalta las graves consecuencias de la utilización indebida de datos personales en el ámbito electoral, con implicaciones que van más allá del ámbito electoral y afectan a la protección de datos personales:

- **Impacto en el proceso electoral:** La utilización indebida de datos personales para propaganda electoral afecta la integridad del proceso democrático y la confianza pública en las instituciones.

- **Violación del derecho a la protección de datos:** El uso de datos personales sin consentimiento constituye una clara violación del derecho fundamental a la protección de datos personales.

- **Obligaciones del PSC-PSOE:** El PSC-PSOE, como responsable del tratamiento de datos, tenía la obligación de adoptar las medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales y cumplir con los principios establecidos en el RGPD.

- **Repercusiones potenciales:** La sanción impuesta por la AEPD es solo una de las posibles consecuencias de la infracción cometida por el PSC-PSOE. El partido también podría enfrentar demandas por parte de los afectados, así como un daño significativo a su imagen pública y reputación.

El caso del PSC-PSOE pone de manifiesto la importancia de respetar los principios democráticos y la protección de datos personales en el ámbito electoral. Las entidades políticas y cualquier actor que maneje datos personales deben actuar con responsabilidad y ética, garantizando el cumplimiento estricto de la normativa vigente.

4.3 Análisis detallado del Expediente EXP202104139 (2022)

4.3.1. Resumen del caso

La Agencia Española de Protección de Datos (AEPD) sancionó al partido político español Jaén Sentido y Común (JSC) con una multa de 2.000 euros por la infracción del Reglamento General de Protección de Datos (RGPD). La sanción se basó en el envío de un correo electrónico a 241 personas con sus direcciones de correo electrónico visibles, sin el consentimiento previo de los destinatarios ni del remitente. El remitente del correo electrónico, quien había colaborado con JSC en el pasado, no había autorizado el uso de su dirección de correo electrónico para recibir comunicaciones políticas.

4.3.2. Resolución

La AEPD impuso a JSC una multa total de 2.000 euros, dividida en dos partes:

- 500 euros por no garantizar un nivel de seguridad adecuado para los datos personales.

- 1.500 euros por no adoptar las medidas necesarias para proteger los datos personales contra el tratamiento no autorizado o ilícito.

4.3.3. Implicaciones legales y contextuales

La conducta de JSC, al revelar datos personales de manera insegura y sin

• ISSN 1390-8294 • e - ISSN 2960-8155

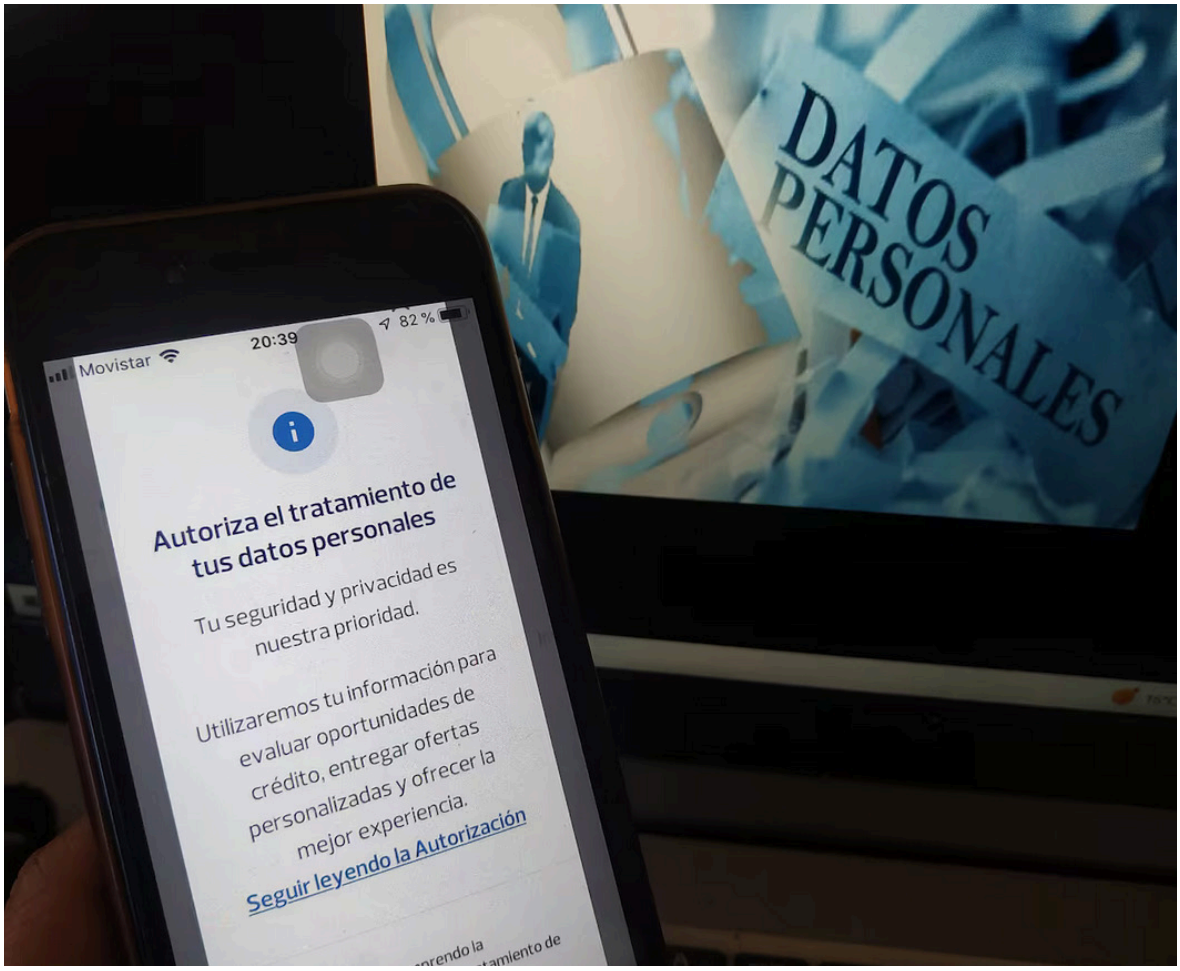


Foto: Archivo / El Universo / Patricia Sandoval.

consentimiento, pone de relieve la importancia crucial de la protección de datos en el entorno digital. Este caso subraya la necesidad de garantizar la seguridad y la confidencialidad de los datos personales, y resalta la existencia de sanciones para prevenir y castigar las infracciones que vulneran estos principios fundamentales.

El caso de JSC también ilustra la responsabilidad que recae sobre las entidades políticas y otras organizaciones de cumplir estrictamente con las normativas de protección de datos, especialmente en aquellas actividades que pueden afectar la opinión pública o la privacidad de los individuos. La divulgación insegura de direcciones de correo electrónico no solo representa un riesgo para la privacidad individual, sino que también puede socavar la confianza en las entidades que manejan estos datos.

La sanción impuesta por la AEPD es solo una de las posibles consecuencias de la infracción cometida por JSC. El partido también podría enfrentar demandas por parte de los afectados, así como un daño significativo a su imagen pública y reputación.

El caso de JSC sirve como un claro recordatorio de la importancia de la protección de datos en el ámbito político y en el entorno digital en general. Las entidades políticas y otras organizaciones deben actuar con responsabilidad y ética, garantizando el cumplimiento estricto de las normativas de protección de datos para preservar la privacidad de los individuos y la confianza pública.

4.4. Análisis desde la perspectiva de la Ley Orgánica de Protección de Datos Personales en el contexto electoral ecuatoriano

El ámbito electoral ecuatoriano ha enfrentado desafíos electorales de gran magnitud, entre los que destacan, desde la perspectiva de la protección de datos personales los siguientes: el caso de las firmas falsas y el escándalo del voto telemático en el exterior. Estos eventos han puesto en tela de juicio la transparencia y la legitimidad del sistema electoral, generando preocupación y desconfianza entre la ciudadanía.

Es importante subrayar que la Ley Orgánica de Protección de Datos Personales entró en vigencia el 26 de mayo de 2021 y la Autoridad de Protección de Datos Personales fue nombrada el 28 de marzo de 2024. Por lo tanto, estos escándalos electorales ocurrieron antes de la implementación completa de la normativa y la creación de la entidad encargada de su aplicación

Sin embargo, es posible examinar estos casos desde el enfoque de los principios y valores, incluso si la ley no se encontraba plenamente vigente en el momento de su ocurrencia.

4.4.1. Caso de las firmas falsas

En el año 2012, Ecuador se vio envuelto en un escándalo electoral de gran magnitud conocido como el caso de las firmas falsas. Este hecho marcó un precedente en la historia democrática del país y puso en tela de juicio la transparencia y la legitimidad del sistema electoral.

En el marco de las Elecciones Generales de 2013, varios movimientos y partidos políticos presentaron al Consejo Nacional Electoral (CNE) miles de firmas para obtener la inscripción legal y participar en los comicios. Sin embargo, se detectaron irregularidades en la autenticidad de estas firmas, lo que desató una investigación a fondo por parte de las autoridades.

Las investigaciones revelaron que miles de firmas habían sido falsificadas por organizaciones políticas con el objetivo de aumentar artificialmente su base de apoyo y obtener la inscripción en el CNE. Se identificaron diversas modalidades de falsificación, como la firma de personas fallecidas o inexistentes, la falsificación de firmas en actas de apoyo y la utilización de datos personales sin el consentimiento de los ciudadanos.

El escándalo de las firmas falsas tuvo un impacto significativo en la política ecuatoriana, generando las siguientes consecuencias:

• ISSN 1390-8294 • e - ISSN 2960-8155

- Los movimientos y partidos políticos involucrados en la falsificación de firmas perdieron credibilidad y apoyo popular, lo que debilitó el sistema político en general.

- Los ciudadanos perdieron la confianza en las instituciones electorales y en los procesos democráticos, lo que generó apatía electoral y un clima de desconfianza hacia el sistema político.

- El escándalo manchó la imagen de Ecuador a nivel internacional, lo que afectó negativamente las relaciones diplomáticas y la inversión extranjera.

- La falsificación de firmas implica el uso indebido de datos personales sin el consentimiento de los ciudadanos, lo que constituye una clara violación a este derecho fundamental.

Si bien la Ley Orgánica de Protección de Datos Personales no estaba vigente en el momento del escándalo de las firmas falsas, sus principios y valores son aplicables a este caso, en el cual se violó el derecho de los ciudadanos a acceder a sus datos personales y conocer su uso, ya que estos fueron utilizados sin su consentimiento para fines políticos. Además, se vulneró el derecho a la rectificación, ya que las firmas falsificadas no correspondían a la voluntad real de los ciudadanos.

Entre las medidas para prevenir la repetición de este escándalo conforme a la Ley Orgánica de Protección de Datos Personales, se debe considerar:

- La Autoridad de Protección de Datos Personales debe fortalecer su capacidad para garantizar el cumplimiento de la Ley, investigando y sancionando las infracciones relacionadas con el uso indebido de datos personales en el ámbito electoral.

- El Consejo Nacional Electoral debe ser más transparente en sus procesos y brindar información clara y accesible al público sobre la inscripción de partidos y movimientos políticos, el financiamiento de campañas y el desarrollo de las elecciones.

- Es fundamental fomentar la educación cívica y la participación ciudadana para que los ciudadanos conozcan sus derechos y responsabilidades en el marco del proceso electoral, y puedan denunciar cualquier irregularidad relacionada con el uso de sus datos personales.

Es importante destacar que, si bien el escándalo de las firmas falsas no es un evento reciente, sigue siendo un referente para comprender los desafíos y las vulnerabilidades del sistema electoral ecuatoriano.

4.4.2. Escándalo del voto telemático en el exterior

El voto telemático en el exterior se realizó en las elecciones presidenciales de 2023, generando una gran expectativa entre los migrantes ecuatorianos. Sin embargo, la implementación del sistema estuvo plagada de problemas técnicos, fallas en la seguridad y denuncias de fraude.

Esto generó frustración, desconfianza y un alto porcentaje de votos nulos.

Si bien el voto electrónico no implica el uso directo de datos personales por parte del votante, sí involucra la gestión y transmisión de datos sensibles relacionados con la identidad y el sufragio de los ciudadanos. Las fallas en la seguridad del sistema de voto electrónico podrían haber expuesto estos datos a riesgos de filtraciones o manipulaciones, lo que representa una grave amenaza a la privacidad y la integridad del proceso electoral.

Para la ocurrencia de estos acontecimientos, la Ley Orgánica de Protección de Datos Personales ya estaba vigente, no así el nombramiento de la Autoridad de Protección de Datos Personales y más aún el organismo de control a su cargo; sin embargo, es posible analizar las consecuencias de este caso desde la perspectiva de los principios y valores establecidos en la ley:

- **Filtración de datos personales:** La falla en la seguridad del sistema de voto electrónico podría haber expuesto datos personales sensibles de los votantes, como nombres, direcciones, números de cédula y preferencias electorales, a riesgos de filtraciones o manipulaciones. Esto constituye una grave amenaza a la privacidad de los ciudadanos y una clara violación al derecho fundamental a la protección de datos personales, consagrado en el artículo 66, numeral 19 de la Constitución de la República del Ecuador y desarrollado en la Ley de la materia.

- **Propaganda electoral no autorizada:** Los votantes que se registraron en el sistema de voto electrónico recibieron en sus correos electrónicos propaganda electoral de movimientos políticos, algo ajeno a las funciones del CNE. Esta situación evidencia una grave falta de control y seguridad en el manejo de los datos personales, exponiendo a los votantes a mensajes políticos no solicitados y potencialmente manipuladores.

- **Falta de transparencia:** La falta de información clara y transparente sobre el manejo de los datos personales de los votantes por parte del CNE generó desconfianza en el sistema de voto electrónico. Los ciudadanos no fueron informados adecuadamente sobre cómo se recopilarían, almacenarían y utilizarían sus datos, lo que alimentó la percepción de que el proceso no era confiable ni seguro.

- **Daño a la reputación del CNE:** El escándalo del voto electrónico ha mermado aún más la credibilidad del CNE. La falta de garantías para la protección de datos personales y la aparente negligencia en el manejo de esta información han generado dudas sobre la capacidad del organismo para administrar procesos electorales confiables y seguros.

• ISSN 1390-8294 • e - ISSN 2960-8155

– **Privación del derecho al voto:** Los migrantes ecuatorianos que esperaban ejercer su derecho al voto a través del sistema electrónico se vieron privados de esta posibilidad debido a las fallas del sistema. Esto generó reclamos y denuncias por parte de la comunidad migrante, que vio transgredidos sus derechos políticos y electorales.

En este caso, se vulneró el derecho de los ciudadanos a acceder a sus datos personales y conocer su uso, pues no se brindó información clara y transparente sobre cómo se recopilarían, almacenarían y utilizarían. Además, se violó el derecho a la oposición al tratamiento, ya que los votantes no tuvieron la posibilidad de negarse a que sus datos fueran utilizados para el voto electrónico.

Para evitar que esta situación a futuro se repita y se eviten las sanciones establecidas en la Ley Orgánica de Protección de Datos Personales, es necesario:

– **Implementación efectiva de la normativa de protección de datos:** La Autoridad de Protección de Datos Personales debe fortalecer su capacidad para garantizar el cumplimiento de la Ley, investigando y sancionando las infracciones relacionadas con el uso indebido de datos personales en el ámbito electoral. Esto incluye la realización de auditorías regulares a los sistemas de gestión de datos electorales y la aplicación de sanciones ejemplares a los responsables de violaciones a la ley.

– **Evaluación exhaustiva del sistema de voto telemático:** Se debe realizar una evaluación exhaustiva del sistema de voto electrónico para identificar y corregir las fallas técnicas y de seguridad que puedan poner en riesgo la privacidad de los datos personales de los votantes. Esta evaluación debe incluir pruebas de penetración, análisis de vulnerabilidades y evaluaciones de seguridad independientes.

– **Implementación de medidas de seguridad robustas:** Se deben implementar medidas de seguridad robustas para proteger el sistema de posibles ataques cibernéticos y garantizar la integridad del proceso electoral. Estas incluyen encriptación de datos, controles de acceso estrictos y monitoreo constante del sistema.

– **Pruebas piloto y simulaciones:** Se deben realizar pruebas piloto y simulaciones para garantizar el correcto funcionamiento del sistema antes de implementarlo en las elecciones generales. Estas pruebas deben incluir escenarios de alta demanda y posibles ataques cibernéticos.

– **Comunicación transparente y efectiva:** El CNE debe mantener una comunicación transparente y efectiva con la ciudadanía, especialmente con los votantes que optan por el voto telemático, para informar sobre los avances, las dificultades y las medidas que se están tomando para proteger sus datos personales.

Esto incluye la publicación de informes de seguridad periódicos y la implementación de canales de comunicación claros para que los votantes puedan reportar cualquier problema o inquietud.

– **Educación cívica y participación ciudadana:** Es esencial fomentar la educación cívica y la participación ciudadana para que los ciudadanos conozcan sus derechos y responsabilidades en el marco del proceso electoral y puedan denunciar cualquier irregularidad relacionada con el uso de sus datos personales. Esto incluye la realización de campañas de información y la capacitación de observadores electorales independientes.

El análisis de estos casos desde la perspectiva de la Ley Orgánica de Protección de Datos Personales nos permite reflexionar sobre la importancia de la protección de datos personales en el contexto electoral.

La Ley Orgánica de Protección de Datos Personales de Ecuador establece un marco legal detallado para el tratamiento y la protección de datos personales, incluyendo una serie de sanciones para las infracciones, que se estructuran en función de su gravedad y pueden incluir multas monetarias significativas, que se calculan con base en un porcentaje del volumen de negocio del infractor.

Este marco legal también abarca la complejidad de las infracciones de protección de datos en el campo electoral. La resolución de estas infracciones comienza en la sede administrativa, donde las autoridades competentes, como la Autoridad de Protección de Datos, recientemente nombrada el 28 de marzo de 2024, tienen la responsabilidad inicial de tratar y resolver las disputas. Una vez agotada esta vía administrativa, los afectados pueden optar por la impugnación judicial si no se alcanza una resolución satisfactoria.

La elección del tribunal para la impugnación judicial depende de la naturaleza específica de la infracción. Mientras que el Tribunal Contencioso Electoral es competente para resolver disputas directamente relacionadas con el proceso electoral, el Tribunal Contencioso Administrativo es más adecuado para casos que implican infracciones de la Ley Orgánica de Protección de Datos Personales, enfocándose en el manejo indebido de datos personales en un contexto más amplio.

En este contexto, una solución viable sería que la Autoridad de Protección de Datos informe al Consejo Nacional Electoral sobre las infracciones relacionadas con el tema en el ámbito electoral. Esta acción permitiría reforzar la vía administrativa y proporcionaría una base sólida para la impugnación de decisiones ante el Tribunal Contencioso Electoral, de acuerdo con las competencias otorgadas por la Constitución y la ley. Esta colaboración interinstitucional garantizaría

• ISSN 1390-8294 • e - ISSN 2960-8155

un tratamiento más eficiente y coherente de las infracciones de protección de datos en el ámbito electoral.

Además, las vías judicial, civil y penal representan alternativas importantes para la reparación por daños o para abordar delitos vinculados al mal uso de datos personales. Estas vías ofrecen recursos adicionales más allá de la vía contenciosa administrativa, dependiendo de los detalles específicos de cada caso y los daños o perjuicios alegados.

En este escenario, la legislación ecuatoriana muestra una robustez en muchos aspectos de la protección de datos, pero aún puede mejorar en la adecuación y gestión de riesgos. La Ley Orgánica de Protección de Datos Personales adopta principios del RGPD de la Unión Europea, pero no profundiza en la gestión de riesgos. Esta omisión puede llevar a brechas en la seguridad y protección de datos personales, especialmente en procesos críticos como las elecciones.

La necesidad de fortalecer el enfoque en la gestión de riesgos dentro del marco de protección de datos en Ecuador y de definir de manera más precisa el papel del DPO es fundamental. Este enfoque mejorado aseguraría una mayor alineación con las mejores prácticas internacionales y proporcionaría una protección de datos más efectiva y adecuada a las realidades del país. La protección de datos personales es un elemento clave para la integridad y la confianza en los sistemas democráticos, y Ecuador tiene la oportunidad de avanzar en esta dirección para garantizar los derechos y la privacidad de sus ciudadanos.

Finalmente, es importante fomentar una cultura de protección de datos entre todos los actores involucrados en los procesos electorales. Esto implica:

- **Capacitación y sensibilización:** Brindar capacitación continua a funcionarios electorales, personal de partidos políticos y demás actores relevantes sobre la Ley Orgánica de Protección de Datos Personales, sus principios y la importancia de la protección de datos personales en la esfera electoral.

- **Comunicación efectiva:** Establecer canales de comunicación claros y transparentes para informar a los votantes sobre el tratamiento de sus datos personales, sus derechos y cómo ejercerlos.

- **Enfoque preventivo:** Implementar medidas preventivas para minimizar los riesgos de filtraciones, accesos no autorizados o uso indebido de datos personales.

- **Rendición de cuentas:** Establecer mecanismos de rendición de cuentas para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales y la protección efectiva de los datos personales de los votantes.

- **Fomentar una cultura de responsabilidad compartida:** Todos los actores involucrados en los procesos electorales, desde las autoridades electorales hasta los votantes, deben asumir la responsabilidad de proteger los datos personales.

- **Cultura de privacidad desde el diseño:** Incorporar principios de privacidad desde el diseño y desarrollo de los sistemas y procesos electorales, asegurando la protección de datos desde las primeras etapas.

- **Evaluación y mejora continua:** Implementar mecanismos para evaluar periódicamente el cumplimiento de la Ley Orgánica de Protección de Datos Personales y la eficacia de las medidas de protección de datos, identificando áreas de mejora y realizando las correcciones necesarias.

Al fomentar una cultura de protección de datos entre todos los actores electorales, se puede fortalecer la confianza de la ciudadanía en los procesos electorales y garantizar el ejercicio efectivo del derecho a la privacidad de los votantes.

5. Conclusiones

Del análisis realizado, se derivan las siguientes conclusiones:

1. La expedición de la Ley Orgánica de Protección de Datos Personales en Ecuador es un hito que responde a la necesidad global de proteger la privacidad en la era de la información. Su integración con el Código de la Democracia y la Constitución de la República del Ecuador conforma un marco legal integral, reforzando la seguridad de la información personal, especialmente, en el ámbito electoral.

2. La Ley Orgánica de Protección de Datos Personales de Ecuador, en sinergia con normativas existentes, juega un papel crucial en la organización de elecciones, la gestión de campañas políticas y la participación ciudadana. Este entrelazamiento legal asegura la integridad y la transparencia de los procesos democráticos, subrayando la relevancia de estas leyes en el fortalecimiento de un sistema electoral confiable.

3. El estudio resalta la necesidad de proteger los datos personales dentro del marco democrático ecuatoriano. La adecuada implementación de las leyes pertinentes se erige como un pilar clave para consolidar la confianza pública en el sistema electoral y, por ende, en la democracia del país.

• ISSN 1390-8294 • e - ISSN 2960-8155

4. Este estudio ilustra la complejidad y la relevancia de la protección de datos personales en Ecuador, enfatizando la necesidad de un enfoque legislativo y práctico que salvaguarde eficazmente los derechos fundamentales en un mundo interconectado. La Ley Orgánica de Protección de Datos Personales se presenta como una herramienta fundamental para garantizar la privacidad y la seguridad de la información personal; así como, para reafirmar los principios democráticos en el país.

5. Es primordial que el gobierno y otras entidades mejoren la educación pública sobre los derechos de protección de datos y su relevancia en el ámbito electoral. La implementación de campañas de concienciación podría desempeñar un papel crucial en la sensibilización sobre cómo los datos personales son utilizados en las elecciones y en la promoción de prácticas de protección de datos entre los ciudadanos.

6. Es vital fomentar la participación y la conciencia de los ciudadanos en la protección de sus datos personales. Se recomienda implementar estrategias para incrementar esta conciencia y participación, que pueden incluir la educación sobre derechos de privacidad, talleres sobre seguridad de datos y la promoción de canales para reportar malas prácticas en el manejo de datos personales durante procesos electorales.

Referencias bibliográficas

Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa. (2018). *Manual de legislación europea en materia de protección de datos*.

Agencia Española de Protección de Datos - AEPD. (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Agencia Española de Protección de Datos (AEPD). (06 de octubre de 2020).Recurso de Reposición Nº RR/00405/2020, Procedimiento nº.: PS/00449/2019. https://www.aepd.es/documento/reposicion-ps-00449-2019.pdf

Agencia Española de Protección de Datos (AEPD). (17 de agosto de 2020). Resolución de Procedimiento Sancionador, Procedimiento Nº: PS/00449/2019. https://www.aepd.es/documento/ps-00449-2019.pdf

Agencia Española de Protección de Datos (AEPD). (18 de febrero de 2020). Resolución de Procedimiento Sancionador, Procedimiento Nº: PS/00341/2019. https://www.aepd.es/documento/ps-00341-2019.pdf

Agencia Española de Protección de Datos (AEPD). (04 de agosto de 2022). Resolución de Procedmiento Sancionador, Expediente N.º: EXP202104139. https://www.aepd.es/documento/ps-00622-2021.pdf

Almoguera, P. (2022, agosto 27). Multan a un partido político de Jaén por enviar correos masivos sin copia oculta. *El Confidencial*. https://www.elconfidencial.com/espana/andalucia/2022-08-27/proteccion-datos-correos-electronicos-jaen_3480825/https://protecciondata.es/wp-content/uploads/2019/10/aqui-1.pdf

Asamblea Nacional Francesa. (1789). *Declaración de los Derechos del Hombre y del Ciudadano*. https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/espagnol/es_ddhc.pdf

Celi, E. (2019, agosto 22). El CNE arrastra un sistema de verificación de firmas lleno de fallas. *Primicias*. https://www.primicias.ec/noticias/politica/cne-verificacion-firmas-fallas/

Celi, E. (2022, septiembre 27). Firmas fraudulentas aún complican a partidos y movimientos. *Primicias*. https://www.primicias.ec/noticias/politica/firmas-afiliados-partidos-movimientos/

Echeverría Muñoz, D. (2023). Delegado de Protección de Datos (DPO) en Ecuador. *Revista Judicial del Diario La Hora - DerechoEcuador.com*. https://derechoecuador.com/delegado-de-proteccion-de-datos-dpo-en-ecuador/

Enríquez Álvarez, L. (2018). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Foro: Revista de Derecho* (27), 43 - 61. https://revistas.uasb.edu.ec/index.php/foro/article/view/500

Granja Medranda, C. (2023, agosto 25). Consejo Nacional Electoral define nulidad de las elecciones en las tres circunscripciones en el exterior. *El Universo*. https://www.eluniverso.com/noticias/politica/elecciones-presidenciales-2023-consejo-nacional-electoral-voto-en-el-exterior-nulidad-revolucion-ciudadana-nota/

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002, 17 de abril) Registro Oficial Suplemento No. 557. https://vlex.ec/vid/ley-67-ley-comercio-643461577

Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador. (2009, 07 de abril). Registro Oficial Suplemento 578. https://vlex.ec/vid/ley-2-ley-organica-643461725

Ley Orgánica de Protección de Datos Personales. (2021, 26 de mayo). Registro Oficial Suplemento No. 459. https://derechoecuador.com/wp-content/uploads/2022/01/LEY-ORGA%CC%81NICA-DE-PROTECCIO%CC%81N-DE-DATOS-PERSONALES.pdf

Loaiza, Y. (2023, agosto 20). *El Consejo Electoral de Ecuador confirmó un ataque cibernético en su sistema de voto en el extranjero. InfoBae*. https://www.infobae.com/america/america-latina/2023/08/20/el-consejo-electoral-de-ecuador-confirmo-un-ataque-cibernetico-en-su-sistema-de-voto-en-el-extranjero/

Naciones Unidas. (1948). *La Declaración Universal de los Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Nohlen, D., Zovatto, D., Orozco, J., & Thompson, J. (2007). *Tratado de derecho electoral comparado de América Latina*. Fondo de Cultura Económica. https://www.iidh.ed.cr/en/component/content/article/tratado-de-derecho-electoral-comparado-de-america-latina?catid=28:democracias-autenticas-funcionales-e-incluyentes&Itemid=101

Parlamento Europeo (21 de marzo de 2019). *Sanciones por el mal uso de los datos personales en las campañas políticas europeas*. https://www.europarl.europa.eu/news/es/headlines/eu-affairs/20190227STO28983/sanciones-por-el-mal-uso-de-los-datos-en-las-campanas-politicas-europeas

Redacción. (2023, agosto 28). El voto telemático pone al CNE en el 'ojo del huracán' . *Ecuador Chequea*. https://ecuadorchequea.com/el-voto-telematico-pone-al-cne-en-el-ojo-del-huracan/

Redacción Diario Expresso. (2016, septiembre 18). *Cuatro anos despues, el caso de las firmas falsas sin resultados*. *Expresso*. https://www.expreso.ec/actualidad/cuatro-anos-despues-caso-firmas-falsas-resultados-70146.html

• ISSN 1390-8294 • e - ISSN 2960-8155

Redacción Plan V. (2022, agosto 23). Firmas falsas: delincuencia política organizada y el fraude a la democracia y a los ciudadanos. *Plan V*. https://www.planv.com.ec/historias/politica/firmas-falsas-delincuencia-politica-organizada-y-el-fraude-la-democracia-y

Redacción Primicias. (2023, agosto 30). Frente a Frente Resultados Noticias Candidatos A la Asamblea Diario de Campaña Consulta Popular Análisis Data Elecciones Presidenciales 2023 Migrantes vivieron un "proceso estresante" con el fallido voto telemático. *Primicias*. https://www.primicias.ec/noticias/elecciones-presidenciales-2023/migrantes-proceso-estresante-voto-telematico/

Redacción Primicias. (2023, agosto 25). El CNE apunta la responsabilidad a la empresa que ejecutó el voto telemático. *Primicias*. https://www.primicias.ec/noticias/elecciones-presidenciales-2023/voto-telematico-exterior-cne-resultados-asambleistas/

Reglamento General de la Ley Orgánica de Protección de Datos Personales. (2023, 11 de noviembre). *Decreto Ejecutivo No. 904*. Registro Oficial Suplemento No. 435.

Unión Europea. (27 de abril de 2016). Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679

Warren, S. D., & Brandeis, L. D. (15 de diciembre de 1890). *The right to privacy*. Harvard Law Review. https://archive.org/details/jstor-1321160/page/n11/mode/2up