InvestiGO Revista Científica Multidisciplinaria

ISSN 2953-6367
http://revistainvestigo.com

enero-junio-2025
Vol. 6, No.14, PP.324-340
https://doi.org/10.56519/vc5gan94

PROTECCIÓN DE DATOS EN ECUADOR - UN ANÁLISIS AL PROCESO DE ANONIMIZACIÓN DE LOS DATOS PERSONALES EN ECUADOR

DATA PROTECTION IN ECUADOR - AN ANALISIS OF THE ANONYMIZATION PROCESS OF PERSONAL DATA IN ECUADOR

Jennifer María Cornejo Viejó[1], José Miguel Castro Macias[2], Marielisa López Puentes[3], Ángel Miguel Maya Monar[4], Enrique Colon Ferruzola Gomez[5]

{jcornejov@unemi.edu.ec[1], jcastrom14@unemi.edu.ec[2], mlopezp8@unemi.edu.ec[3], amayam@unemi.edu.ec[4], eferruzolag@unemi.edu.ec[5]}

Fecha de recepción: 06/12/2024 / Fecha de aceptación: 03/01/2025 / Fecha de publicación: 06/01/2025

RESUMEN: Este estudio examina la anonimización de datos personales en Ecuador según la Ley Orgánica de Protección de Datos Personales (LOPDP), implementada en 2021. Esta ley crea un marco legal solido para proteger la privacidad de los ciudadanos ecuatorianos. El objetivo de este investigacion es analizar la conexión entre la LOPDP y los estándares internacionales de protección de datos como el GDPR de la Unión Europea y la LGDP de Brasil ofreciendo un análisis comparativo. La metodología utilizada es una revisión biobibliográfica, donde se analiza las técnicas de anonimizacion utilizadas en áreas cruciales como salud, finanzas y administración logrando evaluar la eficacia para evitar la re-identificación de las personas. Se reconoce que, aunque la anonimización es crucial para salvaguardar la privacidad, presenta desafíos técnicos y éticos en su aplicación, como la carencia de infraestructura tecnológica adecuada y la necesidad de más formación especializada en Ecuador. Asimismo, el análisis aborda las consecuencias éticas del manejo de los datos anonimizados de los ciudadanos y su vínculo con el derecho a la autodeterminación informativa. Las conclusiones enfatizan la necesidad de mejorar las estrategias de anonimización para salvaguardar los datos personales en un entorno digital global, equilibrando la privacidad con la utilidad de los datos anonimizados.

Palabras clave: Anonimización, privacidad, datos, derecho, conexión

[1]Estudiante Derecho, Universidad Estatal de Milagro (UNEMI), https://orcid.org/0009-0002-7766-668X.
[2]Estudiante Derecho, Universidad Estatal de Milagro (UNEMI), https://orcid.org/0009-0009-3609-9827.
[3]Estudiante Derecho, Universidad Estatal de Milagro (UNEMI), https://orcid.org/0009-0005-1164-2193.
[4]Universidad Estatal de Milagro (UNEMI), https://orcid.org/0009-0009-2170-2267.
[5]Universidad Estatal de Milagro (UNEMI), https://orcid.org/0000-0002-6842-9634.

ABSTRACT: This study examines the anonymization of personal data in Ecuador under the Organic Law on Personal Data Protection (LOPDP), implemented in 2021. This law creates a solid legal framework to protect the privacy of Ecuadorian citizens. The objective of this research is to analyze the connection between the LOPDP and international data protection standards such as the GDPR of the European Union and the LGDP of Brazil, offering a comparative analysis. The methodology used is a biobibliographic review, where the anonymization techniques used in crucial areas such as health, finance, and administration are analyzed, managing to evaluate the effectiveness in avoiding the re-identification of individuals. It is recognized that, although anonymization is crucial to safeguard privacy, it presents technical and ethical challenges in its application, such as the lack of adequate technological infrastructure and the need for more specialized training in Ecuador. Likewise, the analysis addresses the ethical consequences of handling citizens' anonymized data and its link to the right to informational self-determination. The findings emphasize the need to improve anonymization strategies to safeguard personal data in a global digital environment, balancing privacy with the utility of anonymized data.

Keywords: Anonymization, privacy, data, law, connection

INTRODUCCIÓN

La anonimización de identidad es clave para proteger la privacidad en la era digital, donde las tecnologías que analizan grandes volúmenes de datos presentan nuevos desafíos. Este avance se relaciona con técnicas para recuperar identificadores que asocian la identidad a un cuerpo específico, garantizando que el testimonio sea seguro sin comprometer la filiación de los titulares (1).

La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, de 2021, establece un entorno universitario que protege la privacidad de los ciudadanos, alineándose con altos estándares internacionales como el GDPR de la Unión Europea (2). El objetivo de este artículo es analizar la LOPDP en el contexto y su relación con estándares internacionales de protección de datos, evaluando la anonimización para respaldar la privacidad en sectores clave como salud, economía y sector público (3).

Esta observación analiza cómo el estatuto ecuatoriano permite el testimonio anónimo sin comprometer la filiación de los ciudadanos y los desafíos en su implementación. En una atmósfera donde la privacidad es cada vez más valorada, la anonimización se convierte en una práctica técnica y un imperativo moral que afecta la información pública y los derechos individuales (4).

La importancia de este artículo radica en el papel creciente de las organizaciones en decisiones, políticas públicas e investigaciones científicas. En Ecuador, al igual que en otros lugares, las identidades se han vuelto vulnerables y su revelación puede acarrear graves

consecuencias, como la invasión de la privacidad y el uso indebido para fines discriminatorios o delictivos. La anonimización de datos permite aprovechar testimonios legítimos sin comprometer la privacidad de los titulares (5).

La implementación de estas técnicas enfrenta desafíos, especialmente en un condado con infraestructura y capacitación técnica limitadas. Este trabajo es crucial para analizar los avances y obstáculos de la anonimización de datos en Ecuador, comparándolo con normativas internacionales (6).

Esta investigación identifica avances del condado y áreas urgentes de mejora en infraestructura tecnológica y capacitación de profesionales en gestión de datos. Este trabajo examina las implicaciones éticas de la anonimización, balanceando la privacidad y la libertad de información. La observación ofrece un análisis completo del entorno ecuatoriano, incluyendo recomendaciones sobre mejores prácticas internacionales en la protección de datos (7), (8).

La disertación destaca la necesidad de que las instituciones ecuatorianas adopten métodos más avanzados para manejar el testimonio partidista en un entorno digital en crecimiento, abordando las implicaciones sociales, técnicas y éticas de la anonimización de datos. La anonimización en la vida es un avance técnico que afecta cómo se expresa el amor por los impuestos en el entorno digital. Este trabajo ayuda a analistas, legisladores y grupos civiles, a comprender los retos y oportunidades de la protección de datos en Ecuador, respaldando investigaciones y desarrollos normativos, donde la implementación adecuada de la LOPDP y técnicas avanzadas de anonimización refuerzan la privacidad y son cruciales para asegurar la protección de los datos ciudadanos en un entorno interconectado (9).

MATERIALES Y MÉTODOS

El enfoque metodológico sobre la protección de datos en el ámbito académico de Ecuador incluye aspectos normativos y operativos, utilizando fuentes primarias y secundarias. Se ha investigado cómo la Ley Orgánica de Protección de Datos Personales se relaciona con estándares internacionales y la influencia de la anonimización en la privacidad en áreas como salud, economía y administración.

Se emplearon estrategias metodológicas como revisión documental, comparación de normativas internacionales y análisis de desafíos técnicos para la implementación de la anonimización. La revisión documental ha sido esencial para comprender el efecto de la LOPDP. La investigación se fundamenta en la Ley Orgánica de Protección de Datos Personales (2021) y la Constitución del Ecuador en relación con la privacidad y autonomía informativa.

Se analizaron estos documentos para confirmar la concordancia de la Constitución del Ecuador sobre protección de datos con el GDPR, la LGPD de Brasil y la APPI de Japón relacionados con tesis y artículos académicos que contenían esta información relevante.

Este estudio permite comparar similitudes y diferencias en métodos de anonimización y protección de datos en distintos contextos regulatorios.

Por lo que, se centra en la LOPDP sobre la anonimización, especialmente en el artículo 4, que establece criterios para que los datos anonimizados no estén protegidos por la ley, y en el artículo 37, que exige medidas para resguardar la confidencialidad ante amenazas tecnológicas. Se analizó la conformidad de estas disposiciones con las mejores prácticas internacionales y su impacto técnico en las instituciones ecuatorianas. La investigación incluyó una revisión comparativa internacional de marcos regulatorios de protección de datos en la UE, América Latina y EE. UU. y Asia Oriental.

Las técnicas de disección comparativa mostraron patrones en políticas de anonimización, resaltando áreas donde la constitución ecuatoriana podría coincidir con mejores prácticas internacionales. Se llevó a cabo un análisis técnico de los métodos de anonimización más utilizados en Ecuador, enfocado en la ilusión de datos, generalización, seudonimización y algoritmos de privacidad diferencial.

Se estudió la educación de eventos en vitalidad y economías, donde la anonimización de datos resulta esencial. Se exploraron las implicaciones técnicas y éticas de estos métodos, analizando su eficacia en protección contra la reidentificación y su utilidad para el análisis de datos posterior, donde se abordaron los desafíos de aplicar técnicas de anonimización en Ecuador, como la escasez de infraestructura tecnológica y la necesidad de capacitación especializada.

La investigación evaluó organismos reguladores como la Autoridad de Protección de Datos Personales de Ecuador para analizar la efectividad de las políticas actuales y las carencias en su implementación. El enfoque metodológico examinó la transformación tecnológica y su repercusión en la anonimización de datos, resaltando la reidentificación en conjuntos previamente anonimizados por técnicas de Big Data.

Finalmente, el enfoque metodológico incluyó conclusiones operativas sobre datos normativos y recomendaciones para que Ecuador implemente técnicas de anonimización más efectivas. Se discutieron las implicaciones normativas y soluciones tecnológicas para abordar desafíos, proponiendo estrategias para mejorar la coordinación interinstitucional y la protección de datos.

RESULTADOS

Marco normativo de la protección de datos en Ecuador

La Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021, apoya la protección de datos en Ecuador. Esta ley pretende asegurar el derecho a la autodeterminación informativa, mencionado en el artículo 66 numeral 19 de la Constitución

de la República del Ecuador (2008), que resguarda los datos personales y el derecho de decidir sobre su tratamiento.

El artículo 1 de la LOPDP "protege los datos personales, garantizando un tratamiento transparente, confidencial y seguro" (10). La ley define principios para su aplicación, como el de lealtad, que asegura el uso correcto de los datos con el consentimiento del titular. Se enfatiza también el principio de transparencia, que obliga a quienes gestionan datos a informar claramente sobre su uso y objetivos.

Por otro lado, la LOPDP abarca un extenso y detallado campo de aplicación, donde la normativa se aplica a cualquier manejo de datos personales en Ecuador, sea automatizado o manual. Esto abarca datos en cualquier formato, sin importar la nacionalidad del encargado, si impacta en los derechos de ciudadanos o residentes en Ecuador. Esta legislación no se aplica a datos anonimizados que impidan identificar a su propietario, garantizando así protección de privacidad a través de anonimización y seudonimización, como menciona el artículo 4.

La LOPDP establece la Autoridad de Protección de Datos, encargada de supervisar la ley según el artículo 4 esta entidad proporciona directrices para asegurar el cumplimiento normativo y aplica sanciones por violaciones, donde la instauración de esta autoridad representa un progreso en Ecuador, asegurando el control sobre datos personales y protecciones ante vulneraciones (10).

El artículo 7 "regula el tratamiento legítimo de datos, en el cual, este es válido solo si se cumple una condición, como el consentimiento explícito del titular, la obligación legal o la protección de intereses vitales" (10). El consentimiento debe ser claro, libre y específico, informando al titular sobre el uso de sus datos, de acuerdo con el artículo 8, donde este enfoque garantiza que los ciudadanos controlen sus datos personales, un principio fundamental en la legislación de protección de datos.

El artículo 10 define los principios fundamentales para el tratamiento de datos personales, que incluye el principio de proporcionalidad, que demanda un tratamiento adecuado y no excesivo para los fines previstos (10). La confidencialidad asegura que los datos no se compartirán sin el consentimiento del propietario, excepto en casos legales.

De tal modo, que la protección de datos personales es esencial para salvaguardar derechos individuales en la era digital. La anonimización evita identificar individuos, permitiendo el uso de datos con fines estadísticos e históricos sin afectar la privacidad. Es fundamental resguardar la identidad en el manejo de datos sensibles, como los de salud o financieros.

Asimismo, la LOPDP concede derechos a los propietarios de datos y establece obligaciones a quienes los manejan. El artículo 37 "requiere adoptar medidas de seguridad para salvaguardar la integridad y confidencialidad de los datos personales frente a amenazas o

accesos indebidos" (10). Estas medidas deben cumplir con las mejores prácticas internacionales en tecnología de la información.

Por lo que, la LOPDP progresa en la salvaguarda de la privacidad de los ciudadanos frente al manejo masivo de información. Su concordancia con el Reglamento General del Protección de Datos (GDPR) fortalece su validez y eficacia, conciliando la innovación tecnológica con la defensa de los derechos ciudadanos, donde la adecuada implementación de esta norma es crucial para resguardar los datos personales en una sociedad interconectada.

Anonimización de datos personales: conceptos y definiciones

La anonimización de datos es esencial para proteger la privacidad en la era de tecnologías que recopilan información masivamente. Este concepto es un conjunto de técnicas para identificar indirectamente datos mediante normativas de protección. El crecimiento busca proteger la confidencialidad al eliminar pistas que vinculen datos a un individuo, esencial para salvaguardar los derechos fundamentales del titular. Según (11) la anonimización implica transformaciones irreversibles de los datos, a diferencia de la seudonimización, donde los datos se desvinculan temporalmente pero aún pueden ser identificados con claves o información adicional.

Por otro lado, la anonimización puede fallar, permitiendo identificar a individuos incluso en condiciones extremas, donde la anonimización es clave para equilibrar la rapidez en la conservación de datos con la privacidad ciudadana. La Ley Orgánica de Protección de Datos Personales de Ecuador define la anonimización como medidas para evitar la reidentificación de un individuo sin esfuerzos desproporcionados. Esta delimitación destaca la importancia del equilibrio entre la reidentificación del cuerpo y la viabilidad de la anonimización.

Los datos completamente anonimizados no se consideran identificables y no están sujetos a la legislación correspondiente. Las medidas deben ser robustas para resistir reidentificación y proteger la privacidad permanente en a anonimización plantea retos técnicos y legales. Un obstáculo clave es asegurar que los datos del crecimiento sigan siendo útiles para el análisis y la toma de decisiones, mientras se cuestiona la solidez de la anonimización (12).

Existen varias técnicas para lograr la anonimización, como la ofuscación, que distorsiona los datos eliminando identificadores, y la generalización, que agrupa datos en categorías amplias. También se pueden utilizar métodos avanzados como la encriptación irreversible y algoritmos de perturbación que distorsionan los datos originales para dificultar su reversión. La efectividad de la anonimización en la vida romanza depende de técnicas adecuadas y del contexto. Las autoridades, como la de Protección de Datos en Ecuador, establecen criterios estrictos para evaluar la adecuada anonimia de los datos, considerando su tipo, contexto y posibles identificaciones.

La regulación internacional, especialmente el GDPR de la Unión Europea, ha influido en la Constitución de la República del Ecuador al establecer altos estándares para la anonimización y proteger los derechos de los titulares de datos. Conceptualmente, la anonimización y seudonimización son procesos distintos con diferentes finalidades y niveles de protección (12).

La seudonimización permite rastrear datos con un identificador reversible, mientras que la anonimización elimina totalmente cualquier rastro identificable. En la investigación científica, la seudonimización se usa para reducir el valor explicativo de los datos, permitiendo reidentificación si es necesario, donde la anonimización contundente asegura la desconexión de los datos de identidades específicas, fortaleciendo la privacidad en contextos de reidentificación pasiva.

El Big Data y la genialidad han creado nuevos retos para la anonimización, donde las crecientes capacidades de estas tecnologías acoplan grandes volúmenes de datos, aumentando el riesgo de reidentificación, incluso de datos anonimizados, superando métodos tradicionales. Es crucial mejorar las técnicas de anonimización ante nuevas amenazas. Los algoritmos de privacidad diferencial, que alteran los datos para proteger la privacidad sin comprometer su utilidad, son una solución moderna ante los desafíos del Big Data.

Técnicas de anonimización aplicadas en Ecuador

Las técnicas de anonimización de datos personales son cruciales en Ecuador hoy en día, el aumento de la información digital y la Ley de Protección de Datos han promovido procesos avanzados para garantizar la privacidad mediante la desreidentificación irreversible de datos. La legislación ecuatoriana exige métodos sólidos para evitar la reidentificación, preservando el uso legítimo de datos anonimizados en la investigación y el desarrollo (13).

En Ecuador, la ofuscación de datos es un método común y efectivo para anonimizar información. Este proceso consiste en alterar los atributos de los datos al sustituir o eliminar elementos que puedan identificar a una persona. La ofuscación puede ocultar nombres, direcciones y otros datos clave para identificar a una persona. La eficacia de este método se debe a que disocia la información sin alterar su estructura, protegiendo así la privacidad del sujeto.

La generalización transforma datos específicos en categorías más amplias, en lugar de guardar la fecha de nacimiento exacta, se puede usar rangos de edad. La generalización de datos oculta la identidad del individuo y protege contra correlaciones de múltiples fuentes. La generalización desafía a equilibrar la granularidad de los datos y su utilidad analítica. Una excesiva generalización puede disminuir la precisión y aplicabilidad de los resultados (14).

Ecuador ha comenzado a usar algoritmos de perturbación de datos para mejorar la seguridad, además de las técnicas básicas. Este método altera deliberadamente los datos mediante ruido estadístico controlado, dificultando su recuperación. La perturbación es útil para mantener datos útiles en análisis agregados sin comprometer la privacidad del individuo. Este enfoque ha sido efectivo en salud y finanzas, donde se maneja información sensible.

El artículo 4 de la LOPDP ecuatoriana exige que la anonimización evite la reidentificación de personas sin esfuerzos desproporcionados. Este mandato destaca la necesidad de utilizar métodos avanzados que eliminen identificadores y aborden vulnerabilidades potenciales. La seudonimización, a diferencia de la anonimización, no ofrece la misma protección, pues los datos seudonimizados pueden ser relacionados con una persona usando información adicional. Por ello, las entidades en Ecuador están adoptando estrategias de anonimización más complejas.

Para (13) “un enfoque internacionalmente emergente que se explora en Ecuador es el uso de algoritmos de privacidad diferencia. Estos algoritmos garantizan que los datos individuales no se pueden inferir al publicar datos agregados, incluso al combinar múltiples conjuntos. La privacidad diferencial añade “ruido” a los resultados, asegurando que la inclusión o exclusión de una persona no afecte significativamente los resultados y protegiendo su confidencialidad. Esta técnica, aún en sus primeras etapas en Ecuador, avanza en la anonimización de grandes bases de datos para análisis agregados sin comprometer la identidad.

La evaluación continua del riesgo de reidentificación es clave en el proceso de anonimización en Ecuador. Las entidades que tratan datos deben actualizar regularmente las técnicas de anonimización, según el artículo 37 de la LOPDP. Incluye vigilar nuevas amenazas tecnológicas y mejorar las estrategias de protección a medida que surgen nuevas capacidades de análisis de datos. En un entorno dinámico, la anonimización debe evolucionar junto a la inteligencia artificial y el aprendizaje automático para seguir siendo efectiva.

La combinación de técnicas de anonimización es clave para fortalecer el proceso, donde las organizaciones pueden combinar técnicas como ofuscación, generalización y perturbación para complicar la reidentificación. Esta estrategia de capas mejora la seguridad y mantiene la utilidad de los datos anonimizados, maximizando su valor sin violar derechos fundamentales.

Retos del proceso de anonimización en Ecuador

Según (15) anonimización de datos personales enfrenta complejos desafíos tecnológicos, normativos y sociales. La LOPDP ofrece un marco sólido para la gestión de datos, pero su implementación enfrenta obstáculos que requieren un enfoque multidimensional. Estos

desafíos están relacionados con la complejidad de la anonimización y la evolución tecnológica, así como con la alineación a estándares internacionales.

Un reto en Ecuador es la falta de infraestructura tecnológica, donde la anonimización avanzada necesita una infraestructura robusta de hardware y software. Sin embargo, muchas organizaciones aún utilizan sistemas sin la tecnología necesaria para procesos eficientes y seguros. La adopción de estas técnicas requiere inversiones significativas en tecnología, un reto en un país con limitaciones en su modernización digital.

Es innegable que hay un desafío en la capacitación técnica del personal para la anonimización en la LOPDP establece responsabilidades para los responsables del tratamiento de datos, pero es crucial que los profesionales tengan formación especializada en protección de datos y anonimización. En Ecuador, la falta de capacitación en anonimización y ciberseguridad crea una brecha de conocimiento que afecta la efectividad del proceso. Se necesita un esfuerzo conjunto de gobierno, educación y sector privado para fomentar la formación continua y especialización.

Un reto clave es la complejidad técnica de la anonimización en las técnicas como la generalización, ofuscación y perturbación de datos tienen limitaciones y riesgos propios. El reto es equilibrar la anonimización y la utilidad de los datos. La anonimización puede disminuir tanto la granularidad de los datos que su utilidad para análisis estadísticos se reduce. Las organizaciones enfrentan un dilema: ¿cómo aprovechar los datos anonimizados sin afectar la privacidad? Es un reto que requiere una estrategia y técnicas diversas para mantener la utilidad de los datos sin sacrificar su anonimato.

La reidentificación de datos sigue siendo un desafío global, incluido Ecuador. A pesar de los esfuerzos en anonimización, los avances en inteligencia artificial y Big Data han aumentado la reidentificación de datos. Las técnicas de machine learning pueden unir datos disociados para revelar patrones que reidentifican individuos. El riesgo de reidentificación plantea un desafío constante para quienes manejan datos, que deben asegurar técnicas efectivas frente a avances tecnológicos (16).

El cambiante marco normativo es otro gran reto, en el cual, la Ley de Protección de Datos exige principios de anonimización, pero el rápido avance digital necesita actualizaciones constantes en la legislación. La actualización normativa puede ser lenta, causando desincronización con las realidades tecnológicas de las organizaciones. Este desajuste normativo puede generar lagunas en la protección de datos y confusión para las entidades responsables.

El consentimiento y la transparencia también enfrentan desafíos en la anonimización los datos anonimizados no necesitan consentimiento, pero la anonimización debe ser transparente y clara. Las organizaciones a menudo tienen problemas para explicar cómo protegerán y anonimizarán los datos de los titulares. Esto es complejo en un país con una cultura de protección de datos en desarrollo, lo que genera desconfianza entre los

usuarios. Para enfrentar este reto, las entidades que gestionan grandes datos deben adoptar políticas de comunicación efectivas que cumplan legalmente y generen confianza pública.

Según (16) "la falta de coordinación interinstitucional es un reto crítico en Ecuador en la anonimización de datos necesita colaboración constante entre el sector público, privado y reguladores". La desalineación entre estas partes puede causar inconsistencias en la anonimización y en el cumplimiento normativo. Este reto destaca la necesidad de un ecosistema colaborativo para intercambiar prácticas y garantizar una anonimización efectiva de datos en todos los sectores.

Impacto de la anonimización en los derechos de los ciudadanos

La anonimización de datos personales impacta significativamente los derechos civiles, sobre todo la privacidad, la autodeterminación informativa y la protección de la identidad digital. Esta práctica resguarda a los ciudadanos de peligros como el uso abusivo de datos, la vigilancia desmedida y la discriminación al suprimir conexiones identificativas. Este proceso no es neutral y puede influir en otros derechos, creando problemas en transparencia, confianza pública y gestión de información (17).

Asimismo, la anonimización defiende el derecho a la privacidad de los ciudadanos, reconocido por la Constitución y la LOPDP de Ecuador. Al garantizar que los datos no se asocien a un individuo, se salvaguarda su privacidad. Esta protección contra la reidentificación es esencial para resguardar los datos personales de usos comerciales, políticos o delictivos que impactan la vida del ciudadano.

Por otro lado, la anonimización impacta otros derechos de los ciudadanos, además de potenciar la privacidad. Existe un dilema entre la anonimización y el derecho a manejar los datos personales. La anonimización refuerza la seguridad al salvaguardar datos identificables, aunque puede limitar el derecho del ciudadano a acceder, corregir o eliminar su información después del proceso. La anonimización puede llevar a una "desposesión" de datos, excluyendo al propietario de algunos derechos sobre su información.

Es crucial evaluar el efecto en la transparencia y la confianza del público, donde la anonimización puede provocar opacidad en el manejo de datos, ya que suprimir identificadores personales podría hacer que los ciudadanos se sientan distantes de los procesos que afectan su información. La LOPDP autoriza el uso de datos anonimizados sin permiso, lo que inquieta a varios ciudadanos. Es esencial que las organizaciones que anonimizan datos establezcan políticas de comunicación efectivas para describir el proceso y mitigar la desconfianza.

En el cual, la anonimización impacta considerablemente el derecho a la protección contra la discriminación. Los datos anonimizados resguardan a las personas de usos inapropiados de información sensible. La anonimización de datos en salud, educación y empleo previene

la discriminación por etnicidad, género, salud o historial financiero. Este punto es crucial en Ecuador, donde las desigualdades pueden incrementar el riesgo de discriminación por el manejo indebido de datos.

Aunque la anonimización tiene ventajas, el riesgo de reidentificación impacta los derechos ciudadanos. En un entorno digital interconectado, los datos anonimizados pueden fusionarse con otros conjuntos y reidentificar a personas. Esta vulnerabilidad pone en peligro la anonimización y afecta derechos fundamentales como la privacidad y la seguridad (17). Es esencial que las técnicas de anonimización se adapten a la tecnología y que las autoridades realicen evaluaciones constantes para garantizar que los datos permanezcan inidentificables.

Junto a los riesgos técnicos, aparecen retos en los derechos colectivos por la anonimización, en la anonimización de datos puede restringir los derechos comunitarios en justicia social y equidad. La total despersonalización puede eliminar la identidad de grupos marginalizados, complicando investigaciones sobre sus desigualdades. Esto requiere considerar el equilibrio entre derechos individuales y colectivos en la anonimización.

Anonimización de datos en sectores clave: salud, finanzas y gobierno

Según (18) la anonimización se ha vuelto crucial para proteger la privacidad en sectores como la salud, la economía y la gestión. Estos ámbitos gestionan grandes volúmenes de datos sensibles que, si se exponen o tratan inapropiadamente, pueden tener graves consecuencias para sus propietarios. La LOPDP de Ecuador establece normas estrictas para el manejo y anonimización de datos, evitando su uso indebido para reidentificación.

Cada sector presenta retos únicos y las técnicas de anonimización deben ajustarse a su comunicación. En la parte del vigor, la anonimización de identidades es crucial para una comunicación estable. Los datos médicos contienen información sensible sobre la salud física, mental y emocional de los pacientes, cuya divulgación podría violar la privacidad y provocar discriminación. La LOPDP exige la anonimización efectiva de los datos para fines de investigación científica o estadística relacionados con la curiosidad médica.

Por lo que, se usa la seudonimización, que sustituye identificaciones por un identificador simple, evitando la filiación directa sin claves de seguridad adicionales. La seudonimización por sí sola no es suficiente, por lo que se combinan otras técnicas para evitar la reidentificación. Los datos anonimizados son clave para el avance del examen biomédico y la expansión de políticas públicas. Asimismo, los datos anonimizados son esenciales para la educación epidemiológica, permitiendo identificar patrones de enfermedades sin comprometer la privacidad de los pacientes.

Es esencial garantizar que los datos anonimizados sigan siendo útiles para el análisis, manteniendo la máxima protección de la comunicación independiente. Esto exige un delicado equilibrio entre anonimización e interés de datos, un reto que las instituciones

públicas de Ecuador enfrentan al adoptar algoritmos avanzados de anonimización y evaluar riesgos de reidentificación. La anonimización de datos es crucial en las economías, ya que protege información valiosa y vulnerable, como historiales crediticios y activos financieros. Los bancos y aseguradoras almacenan datos sensibles que, si se comprometen, podrían causar fraudes y pérdidas económicas.

Por otro lado, la anonimización de datos es clave para reducir los daños de ciberataques y proteger a los consumidores. La técnica de anonimización más común es el cifrado, que hace los datos ilegibles sin la clave adecuada. Esta lógica asegura que los datos no sean interceptados ni utilizados por terceros no autorizados. Además, los datos anonimizados son cada vez más importantes para analizar casos y crear modelos predictivos sin comprometer la privacidad del consumidor. Esto es notable dado el uso creciente de Big Data y la inteligencia artificial para analizar grandes volúmenes de comunicación y crear perfiles de inversión.

Sin embargo, el uso de tecnología puede ocultar el riesgo de que la combinación de datos reidentifique a los usuarios. Las instituciones financieras deben adoptar enfoques multifacéticos que protejan la privacidad de datos y minimicen la reversión a formas identificables. La anonimización de datos es crucial en el gobierno para proteger la privacidad ciudadana y evitar la vigilancia excesiva.

La dirección gestiona datos de identificación, comunicación fiscal, informes judiciales y contribuciones a programas sociales. Estos datos, si no se manejan con cuidado, pueden causar discriminación y persecución a los ciudadanos. La anonimización ayuda a que la dirección utilice estos datos de manera responsable, promoviendo políticas públicas y protegiendo la privacidad (18).

El artículo 33 de la LOPDP detalla cómo las instituciones públicas deben anonimizar las identidades de los ciudadanos en transferencias a terceros. Este entorno exige que los gobiernos implementen estrictas medidas de anonimización al usar datos para análisis estadísticos o investigaciones sin necesidad de identificar a las personas. En el cual, esta relación permite el intercambio de datos anonimizados entre entidades públicas si se garantiza que no habrá reidentificación (19).

Comparación Internacional: anonimización en Ecuador y el mundo

El GDPR europeo es uno de los sistemas más avanzados en protección de datos y un estándar mundial. Similar a Ecuador, el GDPR estipula que los datos totalmente anonimizados no son personales y no están sujetos a regulaciones de privacidad. El GDPR impone normas más estrictas sobre la anonimización (20). Exige que los datos anonimizados sean irreversiblemente desvinculados y que se evalúen continuamente los riesgos de reidentificación, un aspecto también presente en la LOPDP de Ecuador, aunque con menor énfasis en los procedimientos de evaluación. Esta diferencia resalta una variación clave en la exhaustividad de las normativas.

El GDPR considera la privacidad diferencial un estándar óptimo, pero Ecuador no la ha adoptado ni regulado por completo. Esta técnica añade "ruido" a los datos para salvaguardar la información personal en análisis estadísticos y en inteligencia artificial. La LOPDP permite técnicas de anonimización sofisticadas, pero su uso y comprensión local son limitados en comparación con la Unión Europea.

Por otro lado, la regulación de EE. UU. "exhibe una protección de datos fragmentada y sectorial, menos integrada que la de Ecuador o la Unión Europea. En EE. UU. no hay una ley federal como el GDPR, pero hay regulaciones sectoriales como la HIPAA para datos de salud" (20). La Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) exige anonimizar datos médicos quitando identificadores, parecido a la LOPDP en Ecuador sobre protección de datos sensibles. En EE. UU., la ausencia de una ley federal de protección de datos provoca diferencias en la anonimización entre sectores y estados, a diferencia del enfoque homogéneo de Ecuador con la LOPDP.

En Japón y Corea del Sur, la anonimización de datos personales combina principios occidentales y normas adaptadas a su contexto cultural y tecnológico. Japón, mediante la Protección de Información Personal (APPI), ha establecido estándares altos de anonimización, similar al GDPR, debido a su compromiso con la privacidad. Según (21) la ley japonesa incluye técnicas avanzadas como transformación irreversible de datos y sanciones severas por incumplimiento. En Corea del Sur, la PIPA impone requisitos estrictos para la gestión y anonimización de datos. La LOPDP en Ecuador está en proceso de consolidación y no ha alcanzado la sofisticación técnica de otras jurisdicciones, aunque avanza en la protección de derechos digitales.

Ecuador lidera en la protección de datos en América Latina, solo detrás de Brasil, que implementó la LGPD en 2020. La LGPD brasileña, inspirada en el GDPR, exige procesos estrictos de anonimización de datos antes de su uso comercial, estadístico o científico. Ambas, LGPD y LOPDP, son semejantes y comparten principios, aunque la brasileña es más clara en anonimización y seudonimización. Esta influencia normativa impulsa la armonización regulatoria en América Latina, con Ecuador siguiendo a Brasil hacia un entorno más seguro en la protección de datos.

La reidentificación de datos anónimos es un reto habitual en Ecuador y globalmente. A pesar de métodos sofisticados de anonimización, la IA y el aprendizaje automático permiten reidentificar personas al estudiar grandes cantidades de datos. Este reto es mundial; en Ecuador y en naciones con legislaciones más avanzadas, las autoridades deben actualizar regularmente sus normativas para salvaguardar la privacidad de los ciudadanos frente a nuevas amenazas tecnológicas (21).

La anonimización de datos en Ecuador intenta cumplir con normas internacionales como el GDPR y la LGPD, aunque existe espacio para avanzar en tecnologías de anonimización y en el análisis de riesgos de reidentificación. La LOPDP proporciona un robusto marco que

posiciona a Ecuador en América Latina por su protección de datos personales, ajustándose a las mejores prácticas globales**.**

DISCUSIÓN

La anonimización de datos plantea un debate complejo en Ecuador, particularmente al considerar los avances legislativos de la LOPDP y su aplicación práctica. Este análisis coincide con autores como (22) quienes argumentan que la anonimización nunca es absoluta, ya que los avances tecnológicos pueden facilitar la reidentificación incluso en conjuntos de datos cuidadosamente procesados. La normativa ecuatoriana, aunque inspirada en marcos como el GDPR europeo, enfrenta desafíos similares, especialmente en cuanto a mantener la funcionalidad de los datos anonimizados para fines de investigación sin comprometer la privacidad.

De acuerdo con (23), las técnicas como la privacidad diferencial representan un estándar emergente para abordar estos desafíos, permitiendo un equilibrio entre privacidad y utilidad. Sin embargo, en Ecuador, la limitada infraestructura tecnológica y la falta de capacitación dificultan la adopción de estas técnicas avanzadas, un problema también señalado por autores como (24), quien destaca que la implementación de la privacidad diferencial requiere recursos significativos y personal especializado.

Además, el riesgo de reidentificación enfatizado por este estudio se alinea con las preocupaciones expresadas por (25), quien advierte que la proliferación de Big Data y la inteligencia artificial aumenta las probabilidades de que datos anonimizados puedan ser revertidos a su estado original. Esto subraya la necesidad de enfoques dinámicos para la anonimización, algo que la LOPDP aborda, pero con retos significativos en su aplicación práctica.

En cuanto a la dimensión ética, este análisis resuena con autores como (26), quien argumenta que la anonimización, aunque esencial para la privacidad, puede limitar la autodeterminación informativa y generar tensiones éticas. La armonización entre los derechos individuales y colectivos, como se menciona en este estudio, es crucial para construir confianza social, un aspecto también subrayado por (27), quien destaca que la confianza en el uso de datos está profundamente ligada a la percepción de justicia y transparencia en su manejo.

En resumen, el debate sobre la anonimización de datos en Ecuador refleja desafíos globales, pero con matices locales específicos como la infraestructura tecnológica limitada y la capacitación insuficiente. La convergencia entre marcos legales, avances tecnológicos y consideraciones éticas resulta esencial para lograr una implementación efectiva que beneficie tanto a la privacidad individual como a la utilidad colectiva de los datos.

CONCLUSIONES

La anonimización de datos, como lo establece la LOPDP, enfrenta el desafío de equilibrar la protección de la privacidad y la utilidad de los datos para la investigación y las políticas públicas. Aunque las técnicas avanzadas, como la privacidad diferencial y los algoritmos de perturbación, ofrecen garantías de confidencialidad, su implementación puede limitar la granularidad de los datos. Esto resalta la necesidad de adoptar un enfoque dinámico y contextualizado para garantizar que las herramientas tecnológicas puedan evolucionar sin sacrificar la capacidad analítica de los datos.

La limitada infraestructura tecnológica en Ecuador dificulta la adopción de técnicas avanzadas de anonimización, lo que representa un obstáculo para el cumplimiento efectivo de la LOPDP. Es fundamental invertir en la modernización tecnológica y en la capacitación técnica de los profesionales responsables del manejo de datos. Esto permitiría implementar metodologías robustas de anonimización que salvaguarden la privacidad y aseguren la confianza pública en las instituciones que manejan datos personales.

La anonimización plantea dilemas éticos y sociales significativos, especialmente en relación con el control individual sobre los datos personales y las implicaciones colectivas de su manejo. La pérdida de control por parte de los ciudadanos sobre la corrección o eliminación de sus datos tras la anonimización puede generar desconfianza en las instituciones.

Es crucial que las organizaciones adopten estrategias transparentes y educativas que informen a los titulares sobre los beneficios, riesgos y garantías asociados con la anonimización, fomentando así la confianza y promoviendo la equidad en el uso de datos anonimizados.

REFERENCIAS BIBLIOGRÁFICAS

1. Rosa-Lanas G, Pila-Cardenas G. LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR. Revista Internacional de Cultura Visual. 2023;2-16.
2. Asamblea Nacional. Ley Orgánica de Portección de Datos Personales. Registro Oficial Suplemento 459. 2021.
3. Martínez-Jara JN, Pérez-Ycaza JC. Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano. Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas. 2022;1:7.
4. Roldán Carrillo FN. Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. USFQ LAW REVIEW. 2021;7(1):175-202.
5. Morales Oñate DA. Implicaciones jurídicas del algoritmo: derechos intelectuales y privacidad. FORO, Revista de Derecho. 2021;(36):111-130.

6. Peñaherrera Yanez J. Garantía en los procedimientos de anonimización de historia clínica. Revista Médico Científica CAMbios. 2023;22(1).
7. Durán Ramírez MF, Zamora Vázquez AF. Vulneración de derechos y protección de datos personales en Ecuador. Caso de estudio: Empresa SmartSolutions. MQRInvestigar. 2023;7(1):330-343.
8. Muñoz-del-Carpio-Toia A, Mondragón-Barrios L, Alfredo Duro E, Rueda Castro L, Sorokin P. Protección de datos de salud: el reto de la armonización legislativa en América Latina. Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo. 2023;16(2).
9. Andrade Armas D, Toapanta Toapanta M, Baño Hifong M, Gómez Díaz E. Un enfoque de la inteligencia artificial para la protección de datos personales sustentado en la base legal. Revista Latinoamericana de Ciencias Sociales y Humanidades. 2023;4:5.
10. Andrade Armas, D., Toapanta Toapanta, M., Baño Hifong, M., & Gómez Díaz, E. (2023). Un enfoque de la inteligencia artificial para la protección de datos personales sustentado en la base legal. *Revista Latinoamericana de Ciencias Sociales y Humanidades, 4*, 5. https://doi.org/10.56712/latam.v5i4.2530
11. Asamblea Nacional. (2021). Ley Orgánica de Portección de Datos Personales. *Registro Oficial Suplemento 459*. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
12. Asamblea Nacional Constituyente. (2021). Constitución de la Repúbica del Ecuador. *Registro Oficial 449*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf
13. Córdova-Real, J. L., & López-Sevilla, G. M. (2024). Técnicas de anonimización y pseudonimización en la protección de datos personales. *MQRInvestigar, 8*(1), 204-235. https://doi.org/10.56048/MQR20225.8.1.2024.204-235
14. Durán Ramírez, M. F., & Zamora Vázquez, A. F. (2023). Vulneración de derechos y protección de datos personales en Ecuador. Caso de estudio: Empresa SmartSolutions. *MQRInvestigar, 7*(1), 330-343. https://doi.org/10.56048/MQR20225.7.1.2023.330-343
15. Lasso Roldan, E. A. (2024). “INCIDENCIA DE LA ANONIMIZACIÓN DE BASES DE DATOS EN EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR. *INSTITUTO SUPERIOR TECNOLOGICO REY DAVID*. https://dspace-api.itred.edu.ec/server/api/core/bitstreams/07e1a6d3-6b52-4fa6-9909-907f56bb666b/content
16. Martínez-Jara, J. N., & Pérez-Ycaza, J. C. (2022). Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas, 1*, 7.
17. Morales Oñate, D. A. (2021). Implicaciones jurídicas del algoritmo: derechos intelectuales y privacidad. *FORO, Revista de Derecho*(36), 111-130. https://www.redalyc.org/journal/900/90071840007/90071840007.pdf
18. Muñoz-del-Carpio-Toia, A., Mondragón-Barrios, L., Alfredo Duro, E., Rueda Castro, L., & Sorokin, P. (2023). Protección de datos de salud: el reto de la armonización

legislativa en América Latina. *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo, 16*(2). https://doi.org/10.35434/rcmhnaaa.2023.162.1886

19. Peñaherrera Yanez, J. (2023). Garantía en los procedimientos de anonimización de historia clínica. *Revista Médico Científica CAMbios, 22*(1). https://doi.org/10.36015/cambios.v22.n1.2023.908
20. Roldán Carrillo, F. N. (2021). Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. *USFQ LAW REVIEW, 7*(1), 175-202. https://doi.org/10.18272/ulr.v8i1.2184
21. Rosa-Lanas, G., & Pila-Cardenas, G. (2023). LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR. *Revista Internacional de Cultura Visual*, 2 – 16
22. Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*. Information and Privacy Commissioner of Ontario, Canada.
23. Dwork, C. (2006). *Differential Privacy*. In *33rd International Colloquium on Automata, Languages, and Programming* (pp. 1–12). Springer.
24. Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.
25. Narayanan, A., & Shmatikov, V. (2008). *Robust De-anonymization of Large Sparse Datasets*. In *2008 IEEE Symposium on Security and Privacy* (pp. 111–125). IEEE.
26. Nissenbaum, H. (2004). *Privacy as Contextual Integrity*. *Washington Law Review*, 79(1), 119–158.
27. Ohm, P. (2010). *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*. *UCLA Law Review*, 57, 1701–1777.