14

Fecha de presentación: junio, 2024
Fecha de aceptación: noviembre, 2024
Fecha de publicación: diciembre, 2024

# INJERENCIA

## DE LOS SISTEMAS DE VIGILANCIA EN EL DERECHO A LA PRIVACIDAD EN ECUADOR

## INTERFERENCE OF SURVEILLANCE SYSTEMS IN THE RIGHT TO PRIVACY IN ECUADOR

Pablo Espinosa Pico [1*]
E-mail: ua.pabloep80@unaindes.edu.ec
ORCID: https://orcid.org/0009-0009-2768-5912
Byron Javier Chulco Lema [1]
E-mail: ua.byron97@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-2584-9564
Nathaly Nicole Palate Ayme [1]
E-mail: nathalypa32@uniandes.edu.ec
ORCID: https://orcid.org/0009-0006-5334-9064
Katiusca Brigett Corozo Duarte [1]
E-mail: katiuscacd88@uniandes.edu.ec
ORCID: https://orcid.org/0009-0006-2719-3238
[1] Universidad Regional Autónoma de los Andes. Ambato, Ecuador.
*Autor para correspondencia

Cita sugerida (APA, séptima edición)

Espinosa Pico, P., Chulco Lema, B. J., Palate Ayme, N.N., & Corozo Duarte, K. B. (2024). Injerencia de los sistemas de vigilancia en el derecho a la privacidad en Ecuador. ***Universidad y Sociedad 16*** (S2). 131-138.

RESUMEN

En un contexto de creciente criminalidad y amenazas transnacionales, Ecuador enfrenta el desafío de implementar sistemas de vigilancia que, aunque destinados a mejorar la seguridad pública, pueden afectar gravemente el derecho a la privacidad de los ciudadanos. Esta investigación tiene como objetivo analizar el impacto de la vigilancia masiva en las libertades civiles, evaluando el marco legal vigente y proponiendo estrategias regulatorias que equilibren la seguridad y la privacidad. Se empleó un enfoque cualitativo-descriptivo mediante revisión documental, entrevistas semiestructuradas y estudios de caso. Los resultados revelan importantes brechas normativas en la legislación ecuatoriana, que permiten el uso desmedido de tecnologías como el reconocimiento facial sin suficiente regulación o supervisión. La mayoría de los expertos entrevistados expresaron preocupaciones sobre el abuso potencial de estas tecnologías, subrayando la urgencia de fortalecer el marco normativo y establecer controles judiciales. Aunque se justifican en nombre de la seguridad, los sistemas de vigilancia sin regulación adecuada pueden llevar a violaciones de derechos humanos, como la privacidad y la libertad de expresión. Las propuestas regulatorias sugeridas buscan no solo mejorar la seguridad pública, sino también salvaguardar los derechos de los ciudadanos, fomentando un entorno donde la vigilancia se realice de manera ética y responsable, y se respete la dignidad de todos los individuos.

Palabras clave: Libertades civiles, Seguridad, Marco legal, Estrategias regulatorias, Brechas normativas.

ABSTRACT

In a context of increasing criminality and transnational threats, Ecuador faces the challenge of implementing surveillance systems that, while intended to enhance public security, may severely impact citizens' right to privacy. This research aims to analyze the impact of mass surveillance on civil liberties, evaluating the existing legal framework and proposing regulatory strategies that balance security and privacy. A qualitative-descriptive approach was employed through document review, semi-structured interviews, and case studies. The results reveal significant normative gaps in Ecuadorian legislation, allowing for the excessive use of technologies such as facial recognition without sufficient regulation or oversight. Most experts interviewed expressed concerns about the potential abuse of these technologies, emphasizing the urgency to strengthen the regulatory framework and establish judicial controls. While justified in the

name of security, surveillance systems without adequate regulation can lead to violations of human rights, such as privacy and freedom of expression. The proposed regulatory strategies aim not only to enhance public security but also to safeguard citizens' rights, fostering an environment where surveillance is conducted ethically and responsibly, and the dignity of all individuals is respected.

Keywords: Civil liberties, Security, Legal framework, Regulatory strategies, Normative gaps.

## INTRODUCCIÓN

El contexto histórico contemporáneo enfrenta desafíos cada vez más complejos en términos de seguridad nacional e internacional, debido al surgimiento de nuevas formas de criminalidad que se adaptan rápidamente a un mundo globalizado e interconectado. Entre estos retos, los ataques terroristas continúan siendo una grave amenaza para numerosos países, afectando tanto a naciones desarrolladas como en vías de desarrollo, y evidenciando la naturaleza transnacional del terrorismo. Además, el crecimiento exponencial de la criminalidad organizada, impulsada por el narcotráfico, la trata de personas y los cibercrímenes, ha intensificado la presión sobre los Estados para diseñar e implementar estrategias más efectivas de seguridad.

Frente a este panorama, los gobiernos han recurrido a sistemas de vigilancia más avanzados que permiten la recopilación masiva de datos e información a fin de detectar amenazas con antelación y evitar ataques o actividades delictivas. Estas medidas incluyen desde el monitoreo de redes de comunicación y plataformas digitales hasta el uso de tecnologías como el reconocimiento facial y la inteligencia artificial para analizar patrones de comportamiento sospechoso (Ribeiro et al., 2021). Sin embargo, el aumento de estas tecnologías plantea interrogantes sobre cómo los Estados pueden mantener un equilibrio entre la protección de la seguridad y la preservación de los derechos fundamentales, como el derecho a la privacidad y la libertad individual, en un contexto donde la prevención del crimen requiere cada vez más intervención y vigilancia.

Para ello, los Estados disponen de una amplia gama de herramientas tecnológicas, que en muchos casos se utilizan para la vigilancia y monitoreo de la población, así como para llevar a cabo investigaciones preventivas y en el marco de procesos judiciales. En este contexto, algunos países han implementado sistemas de vigilancia masiva de alta tecnología, diseñados para interceptar las comunicaciones de los ciudadanos con el fin de realizar tareas de inteligencia que permitan identificar la posible comisión de delitos, particularmente aquellos vinculados con el terrorismo (Ou et al., 2023).

En la era digital, los sistemas de vigilancia han adquirido una relevancia sin precedentes, impulsados por el avance de las tecnologías de la información y la comunicación. Estos sistemas, implementados tanto por gobiernos como por empresas privadas, tienen el propósito de mejorar la seguridad y prevenir actividades delictivas, especialmente en contextos relacionados con el terrorismo y el crimen organizado. Sin embargo, el uso extendido de tecnologías de vigilancia plantea serias preocupaciones sobre el derecho a la privacidad, un pilar fundamental de las sociedades democráticas (Sujkowski et al., 2023).

El equilibrio entre seguridad y privacidad ha generado un intenso debate, ya que los sistemas de vigilancia pueden, en muchos casos, derivar en una intrusión en la vida privada de los ciudadanos. La capacidad de interceptar comunicaciones, monitorizar actividades en línea y realizar seguimientos biométricos sin el consentimiento explícito de los individuos crea un entorno en el que el control estatal sobre los datos personales puede desbordar los límites de lo aceptable desde una perspectiva de derechos humanos (González Monje, 2017).

En este contexto, la investigación tiene como objetivo, analizar el impacto de los sistemas de vigilancia masiva, tanto gubernamentales como privados, sobre el derecho a la privacidad de los individuos, evaluando cómo estas tecnologías afectan las libertades civiles y los derechos humanos. Se busca, además, identificar los marcos legales vigentes y proponer estrategias y regulaciones que equilibren la protección de la seguridad pública con el respeto y la garantía del derecho a la privacidad.

## MATERIALES Y MÉTODOS

Para llevar a cabo la investigación, se adoptó un enfoque cualitativo-descriptivo (Guamán et al., 2021), empleando una combinación de análisis documental y entrevistas semiestructuradas. Los métodos específicos empleados se detallan a continuación:

1. Revisión documental y análisis jurídico

Se realizó una exhaustiva revisión de la literatura y análisis de marcos normativos relacionados con los sistemas de vigilancia y la protección de la privacidad en Ecuador y a nivel internacional. Los documentos analizados incluyeron:

- Legislación ecuatoriana pertinente, como la Constitución de Ecuador (artículos relacionados con la privacidad y los derechos humanos) y la Ley Orgánica de Protección de Datos Personales (LOPDP).
- Tratados internacionales ratificados por Ecuador, como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos.
- Informes de organizaciones no gubernamentales (ONG) y organismos internacionales, como la Comisión Interamericana de Derechos Humanos

(CIDH) y Human Rights Watch, que documentan el uso de tecnologías de vigilancia en América Latina.

- Estudios académicos previos sobre la relación entre los sistemas de vigilancia, derechos civiles y privacidad, tanto a nivel global como en el contexto ecuatoriano.

El análisis jurídico se centró en identificar las brechas normativas y las formas en que las leyes ecuatorianas y los estándares internacionales protegen o fallan en proteger la privacidad frente a los sistemas de vigilancia masiva.

2. Entrevistas semiestructuradas

Se realizaron entrevistas semiestructuradas con expertos en derechos humanos, tecnología y seguridad. Las mismas, tuvieron como objetivo explorar percepciones sobre el impacto de los sistemas de vigilancia en los derechos civiles y evaluar el marco legal vigente en Ecuador. Se diseñaron preguntas abiertas que cubrieron aspectos relacionados con el equilibrio entre la seguridad pública y el derecho a la privacidad, así como las implicaciones éticas de los sistemas de vigilancia.

3. Estudio de caso: uso de tecnologías de vigilancia en Ecuador

Se seleccionaron casos relevantes de vigilancia gubernamental y privada para un análisis detallado. Estos casos incluyeron el uso de cámaras de seguridad con reconocimiento facial en ciudades ecuatorianas y tecnologías de monitoreo digital empleadas por agencias gubernamentales y empresas privadas. La selección de los casos se basa en reportes de medios de comunicación y documentos públicos.

Finalmente, se elaboraron propuestas de estrategias regulatorias basadas en los resultados, con recomendaciones para equilibrar la protección de la seguridad y el respeto a la privacidad en Ecuador.

## RESULTADOS-DISCUSIÓN

En esta sección se presentan los resultados derivados del análisis documental, las entrevistas semiestructuradas y el estudio de caso realizado sobre la injerencia de los sistemas de vigilancia en el derecho a la privacidad en Ecuador. A través de estos enfoques, se busca identificar cómo las tecnologías de vigilancia masiva implementadas por entidades gubernamentales y privadas afectan las libertades civiles y los derechos humanos. Asimismo, se exploran los marcos normativos vigentes y se exponen las percepciones de expertos sobre la efectividad de dichas regulaciones.

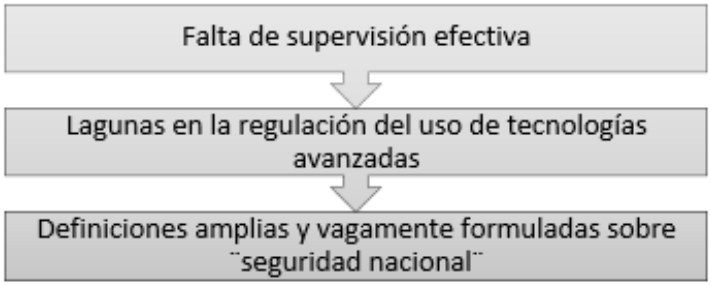
El análisis exhaustivo de los marcos normativos y la literatura revela importantes hallazgos en relación con la protección de la privacidad frente a los sistemas de vigilancia en Ecuador. A continuación, se detallan los principales resultados obtenidos de la revisión documental:

- El artículo 66 de la Constitución garantiza el derecho a la privacidad, la inviolabilidad de la correspondencia y la protección de datos personales, lo cual es un avance significativo para la protección de las libertades individuales frente a la vigilancia. Sin embargo, el artículo 19 establece excepciones en casos donde la seguridad nacional está en riesgo, lo que deja margen para interpretaciones amplias por parte del Estado (Asamblea Nacional del Ecuador. Decreto Legilativo 0. Registro Oficial 449., 2008).
- Ley Orgánica de Protección de Datos Personales (LOPDP) regula la recolección, tratamiento y almacenamiento de datos personales por parte de entidades públicas y privadas. Si bien la ley representa un esfuerzo por alinear la normativa ecuatoriana con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, aún presenta debilidades en cuanto a la supervisión efectiva de las agencias de seguridad que manejan tecnologías de vigilancia masiva. La ley no establece claramente cómo las entidades de seguridad pública deben gestionar los datos obtenidos a través de sistemas de monitoreo, dejando un vacío legal en este aspecto (Asamblea Nacional del Ecuador, 2013).
- Pacto Internacional de Derechos Civiles y Políticos (PIDCP): Este tratado garantiza la protección de la privacidad en su artículo 17, prohibiendo cualquier injerencia arbitraria o ilegal en la vida privada de las personas. Ecuador, como país signatario, está obligado a respetar y proteger estos derechos. Sin embargo, a pesar de estar alineado con este compromiso, las excepciones por seguridad pública y nacional, tanto en la legislación local como en los tratados internacionales, permiten que los sistemas de vigilancia se implementen sin la adecuada rendición de cuentas (ONU, 1966).
- Convención Americana sobre Derechos Humanos (CADH): Similar al PIDCP, la CADH protege la privacidad en su artículo 11. El problema identificado es que, aunque estos tratados ofrecen un marco sólido de protección, la falta de armonización con las regulaciones nacionales y la falta de sanciones efectivas para violaciones a la privacidad limitan su impacto (OEA, 2016).
- Human Rights Watch (HRW): En su informe de 2021, señala que Ecuador ha ampliado el uso de cámaras de videovigilancia con sistemas de reconocimiento facial, en particular en áreas urbanas, sin garantizar un marco legal robusto que proteja la privacidad de los ciudadanos. A pesar de que estas tecnologías son justificadas bajo la premisa de la seguridad pública, HRW advirtió sobre el potencial abuso de estos sistemas para fines de control social o político, especialmente en el monitoreo de manifestaciones y actividades de la sociedad civil (Slezkine, 2014).

Varios estudios, tanto globales como específicos de América Latina, han destacado que los sistemas de vigilancia masiva, como el reconocimiento facial y la vigilancia de redes, tienden a operar en un vacío normativo en muchos países. En el caso de Ecuador, estudios locales han subrayado que, aunque existen leyes como la LOPDP, los mecanismos de aplicación y supervisión son insuficientes. Esto abre la posibilidad de que los sistemas de vigilancia sean usados de manera desproporcionada y sin control judicial adecuado (Pilamunga, 2021).

A partir del análisis de la legislación nacional y los tratados internacionales, se identificaron las siguientes brechas normativas en la protección de la privacidad frente a la vigilancia en Ecuador (figura 1):

Fig 1: Brechas identificadas en la protección de la privacidad.




Fuente: Elaboración propia.

Se detecta que no existen órganos de control independientes que supervisen adecuadamente el uso de tecnologías de vigilancia por parte de las fuerzas de seguridad y agencias gubernamentales. El Consejo Nacional de Protección de Datos, creado bajo la LOPDP, aún no tiene plena capacidad operativa para hacer cumplir sus disposiciones en relación con el monitoreo y la vigilancia masiva.

Las leyes actuales no contemplan disposiciones específicas para tecnologías emergentes como el reconocimiento facial, la biometría o la vigilancia digital en redes sociales, lo que permite su uso sin garantías suficientes de protección de la privacidad. Además de que, la legislación ecuatoriana, tanto en la Constitución como en la LOPDP, utiliza el concepto de "seguridad nacional" de manera amplia, lo que da margen para justificar el uso de sistemas de vigilancia en una variedad de situaciones, sin un control judicial riguroso o una evaluación proporcional.

Se realizaron 10 entrevistas semiestructuradas con expertos en derechos humanos, tecnología y seguridad, seleccionados por su trayectoria y experiencia en el ámbito de la privacidad y la protección de datos en Ecuador (tabla 1). La muestra incluye a:

Tabla 1: Detalles de la muestra de estudio.

| Tipo de participante | Cantidad | Descripción |
|---|---|---|
| Abogados especializados en derechos digitales | 3 | Con experiencia en litigios y asesoría legal en protección de datos. |
| Académicos | 3 | Investigadores que han estudiado el impacto de la vigilancia en los derechos humanos, en Universidades de Ecuador. |
| Representantes de organizaciones de la sociedad civil. | 2 | Miembros de organizaciones que monitorean el uso de tecnologías de vigilancia y su impacto en los derechos civiles. |
| Funcionarios públicos | 2 | Personal del Consejo Nacional de Protección de Datos y del Ministerio de Telecomunicaciones. |
| TOTAL | 10 | |

Fuente: Elaboración propia.

- Percepciones sobre el impacto de los sistemas de vigilancia:

De los 10 entrevistados, 8 expresan preocupación por la expansión de las tecnologías de vigilancia, como el reconocimiento facial y la vigilancia digital, sin un adecuado control y supervisión. Los abogados y académicos destacan que estas tecnologías pueden ser utilizadas para la vigilancia masiva sin el consentimiento informado de los ciudadanos, lo que representa una vulneración de los derechos a la privacidad y la libertad de expresión. Mientras que, un funcionario

público señala que el uso de estas tecnologías está justificado en la lucha contra la delincuencia y el terrorismo, pero admite que falta un marco normativo sólido que regule su uso y garantice la protección de los derechos civiles.

- Evaluación del marco legal vigente:

Todos los entrevistados coincidieron en que la LOPDP es un avance importante, pero insuficiente para regular eficazmente el uso de tecnologías de vigilancia masiva. Los académicos y representantes de la sociedad civil señalaron que la ley no aborda con suficiente claridad el uso de tecnologías avanzadas como el reconocimiento facial y los sistemas de vigilancia en línea.

A su vez, 6 de los 10 expertos afirmaron que la falta de un ente regulador independiente y con capacidad sancionatoria limita la efectividad de la LOPDP en la protección de la privacidad frente a la vigilancia estatal y corporativa. El Consejo Nacional de Protección de Datos, aunque previsto en la ley, aún no cuenta con los recursos suficientes para ejercer un control efectivo sobre el uso de estas tecnologías.

- Equilibrio entre seguridad pública y derecho a la privacidad:

La mayoría de los entrevistados señalan que existe una tensión creciente entre la seguridad pública y la privacidad. Los representantes de la sociedad civil y los académicos advierten que, en muchos casos, la justificación de la seguridad pública se utiliza como pretexto para implementar sistemas de vigilancia intrusivos, sin la debida supervisión o proporcionalidad en su aplicación. En contraste, los funcionarios públicos argumentan que la implementación de estos sistemas es necesaria para combatir el aumento de la delincuencia, pero reconocen que se requieren mejores regulaciones y mecanismos de control para garantizar un equilibrio adecuado entre la seguridad y los derechos civiles.

- Implicaciones éticas de los sistemas de vigilancia:

Todos los expertos plantean serias preocupaciones éticas sobre el uso indiscriminado de tecnologías de vigilancia. Señalan que el monitoreo constante y la recolección masiva de datos pueden generar un efecto inhibidor en la libertad de expresión y la participación política, especialmente en contextos de protesta social. Los representantes de las organizaciones de la sociedad civil mencionan casos documentados de vigilancia de activistas y periodistas, lo que exacerba el temor de que estas tecnologías puedan ser usadas con fines políticos. Por su parte, los académicos subrayan la falta de transparencia en la implementación de estos sistemas, lo que crea un ambiente de desconfianza y vulneración de los derechos fundamentales.

El análisis de las entrevistas revela un consenso entre los expertos sobre la necesidad de reforzar el marco normativo y establecer mecanismos más sólidos de supervisión y control sobre el uso de tecnologías de vigilancia en Ecuador. Las percepciones recogidas indican que, aunque existe una comprensión clara sobre la necesidad de estos sistemas para mejorar la seguridad pública, su uso desmedido y no regulado pone en riesgo los derechos fundamentales, especialmente el derecho a la privacidad y la libertad de expresión. Los entrevistados hicieron hincapié en la urgencia de establecer límites claros y garantizar que la vigilancia esté sujeta a controles judiciales efectivos y normas de transparencia rigurosas.

Para el análisis detallado de los sistemas de vigilancia en el país, se seleccionan tres casos relevantes que ilustran las implementaciones de tecnologías de vigilancia (ver tabla 2), tanto gubernamentales como privadas.

Tabla 2: Estudio de casos.

| Caso | Descripción | Evaluación de cumplimiento |
|---|---|---|
| Cámaras de seguridad con reconocimiento facial en Quito. | Implementación de aproximadamente 1000 cámaras en puntos estratégicos de la ciudad desde 2021 para mejorar la seguridad y reducir el delito (Cerezo & de los Ángeles, 2024). | La Defensoría del Pueblo de Ecuador destaca la falta de un marco regulatorio claro, contradiciendo estándares internacionales de protección de la privacidad. Se reportaron identificaciones incorrectas y falta de transparencia en el manejo de datos. |
| Monitoreo digital de redes sociales por el Ministerio de Gobierno. | Programa iniciado en 2020 para identificar y prevenir delitos relacionados con violencia y terrorismo mediante el análisis de publicaciones en plataformas como Twitter y Facebook. | Según la Comisión Nacional de Derechos Humanos, el monitoreo carece de supervisión judicial y podría ser usado para silenciar a críticos del gobierno. Falta de transparencia en los criterios de monitoreo crea un clima de autocensura. |

| | | |
|---|---|---|
| Vigilancia privada por empresas de seguridad. | Más de 500 empresas de seguridad han implementado sistemas de vigilancia que incluyen cámaras con análisis de video y monitoreo en tiempo real para proteger activos y personal. | Un estudio de la Universidad Central del Ecuador (2022) revela que el 80% de los trabajadores no están informados sobre la recolección y uso de sus datos. Las políticas de privacidad son poco claras o inexistentes, lo que viola la LOPDP. |

Fuente: Elaboración propia.

El análisis de los tres casos seleccionados evidencia que, aunque las tecnologías de vigilancia en Ecuador pueden ser justificadas bajo la premisa de la seguridad pública, existen serias deficiencias en los marcos normativos que regulan su uso. La falta de supervisión, la ambigüedad en los criterios de aplicación y la ausencia de transparencia son elementos comunes que facilitan el riesgo de violaciones a los derechos humanos y a la privacidad de los ciudadanos (Díaz, 2024). Además, la implementación de estas tecnologías sin un marco adecuado no solo afecta la confianza pública, sino que también puede ser utilizada para fines de control social, limitando así la libertad de expresión y el ejercicio de otros derechos fundamentales. Estos resultados demuestran la necesidad de una regulación más robusta que garantice el equilibrio entre la seguridad pública y la protección de la privacidad (Mozur et al., 2019).

En el contexto actual de creciente uso de tecnologías de vigilancia en Ecuador, es fundamental establecer un marco regulatorio que garantice un equilibrio entre la protección de la seguridad pública y el respeto por el derecho a la privacidad de los ciudadanos. Las propuestas de estrategias regulatorias que se presentan a continuación (Tabla 3) buscan abordar las deficiencias identificadas en la implementación de sistemas de vigilancia, asegurando que se utilicen de manera transparente, responsable y en conformidad con los estándares de derechos humanos.

Tabla 3: Propuestas de Estrategias Regulatorias.

| Estrategia | Recomendación | Justificación |
|---|---|---|
| Desarrollo de un marco normativo específico para tecnologías de vigilancia. | Crear una legislación que regule específicamente el uso de tecnologías de vigilancia, como cámaras de reconocimiento facial y monitoreo digital, estableciendo estándares claros sobre su implementación, uso y almacenamiento de datos. | Esto garantiza que las tecnologías se utilicen de manera transparente y responsable, con protección adecuada de los derechos fundamentales. |
| Establecimiento de un organismo regulador independiente. | Instituir un ente regulador independiente encargado de supervisar el uso de tecnologías de vigilancia, con poderes para realizar auditorías y sancionar a las entidades que no cumplan con la normativa. | Un organismo autónomo actúa con imparcialidad y efectividad en la supervisión de la aplicación de leyes, garantizando el cumplimiento de estándares de privacidad y derechos humanos. |
| Mecanismos de control judicial. | Implementar un sistema que requiera autorización judicial previa para el uso de tecnologías de vigilancia en situaciones que impliquen recolección de datos personales, especialmente en contextos que afecten la privacidad de individuos. | Esto asegura que las intervenciones en la privacidad sean proporcionales, justificadas y supervisadas por la autoridad judicial, evitando abusos de poder. |
| Transparencia y rendición de cuentas. | Exigir a las entidades públicas y privadas que implementen sistemas de vigilancia que publiquen informes anuales sobre su uso, incluyendo el número de datos recolectados, el propósito de la vigilancia y cualquier incidencia de abuso o errores. | La rendición de cuentas y la transparencia fomentan la confianza pública en el uso de tecnologías de vigilancia y permiten un monitoreo ciudadano más efectivo. |
| Capacitación y concienciación. | Desarrollar programas de capacitación para funcionarios públicos, empresas y ciudadanos sobre los derechos de privacidad, el uso ético de la tecnología y las implicaciones de la vigilancia. | Promover una mayor comprensión de la importancia de la privacidad y la protección de datos personales puede ayudar a mitigar los riesgos asociados con la vigilancia. |
| Protección de datos personales. | Fortalecer la LOPDP para incluir directrices claras sobre la recolección, almacenamiento y uso de datos personales obtenidos a través de tecnologías de vigilancia. | Asegurar que se respeten los derechos de los individuos a ser informados sobre la recolección de sus datos y darles control sobre su información personal es fundamental para proteger la privacidad. |

| | | |
|---|---|---|
| Auditorías regulares y evaluación de impacto. | Implementar auditorías regulares y evaluaciones de impacto sobre los derechos humanos en relación con el uso de tecnologías de vigilancia, realizadas por organismos independientes. | Estas evaluaciones ayudarán a identificar riesgos y brechas en la protección de la privacidad, permitiendo ajustes en las políticas y regulaciones según sea necesario. |
| Participación ciudadana en la formulación de políticas. | Fomentar la participación de la sociedad civil en la creación y revisión de políticas sobre vigilancia y privacidad, asegurando que se escuchen las voces de quienes pueden verse afectados por estas tecnologías. | Incluir la perspectiva de la ciudadanía en el proceso de toma de decisiones fortalece la democracia y garantiza que las regulaciones sean más inclusivas y respetuosas de los derechos de todos. |

Fuente: Elaboración propia.

Con la aplicación de las estrategias regulatorias propuestas, se garantiza establecer un equilibrio entre la necesidad de proteger la seguridad pública y el respeto a la privacidad en Ecuador. La implementación de mismas contribuye a un entorno más seguro y justo, donde los derechos de los ciudadanos sean salvaguardados y la vigilancia se lleve a cabo de manera ética y responsable.

## CONCLUSIONES

La investigación ha puesto de manifiesto que, en el contexto actual de Ecuador, los sistemas de vigilancia masiva, impulsados por la necesidad de enfrentar retos en materia de seguridad nacional e internacional, tienen un impacto significativo en el derecho a la privacidad de los individuos. A través de un análisis exhaustivo de la legislación vigente y entrevistas con expertos en derechos humanos y tecnología, se identificaron importantes brechas normativas que permiten el uso indiscriminado de tecnologías de vigilancia, como el reconocimiento facial y el monitoreo digital, sin la debida regulación y supervisión.

Los hallazgos revelan que, aunque existe una creciente preocupación entre los especialistas sobre el potencial abuso de estas tecnologías, la falta de un marco normativo claro y de órganos de control independientes perpetúa un vacío en la protección de los derechos civiles. A pesar de la justificación que ofrecen las autoridades en nombre de la seguridad pública, la implementación de sistemas de vigilancia sin un adecuado control judicial y sin la transparencia necesaria puede llevar a violaciones graves de derechos fundamentales, como la privacidad y la libertad de expresión.

Es crucial que Ecuador adopte las estrategias regulatorias propuestas, que no solo buscan proteger la seguridad pública, sino también garantizar el respeto por los derechos de los ciudadanos. La creación de un marco normativo robusto y la implementación de mecanismos de supervisión efectiva son pasos esenciales para asegurar que el uso de tecnologías de vigilancia se realice de manera ética y responsable.

## *REFERENCIAS BIBLIOGRÁFICAS*


Asamblea Nacional del Ecuador. Constitución del Ecuador. Decreto Legilativo 0. Registro Oficial 449. (2008). In Quito. Ecuador. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Asamblea Nacional del Ecuador. (2013). REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. Norma 904. Registro Oficial Suplemento 435. https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORGÁNICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf

Cerezo, R. A., & de los Ángeles Enríquez, C. (2024). Software de control de asistencia por reconocimiento facial, para Dependencias del Gobierno. ***Revista Ecuatoriana de Derecho y Administración, 1***(1), 62–86. https://revistas.itecsur.edu.ec/index.php/reda/article/view/126

Díaz Méndez, E. M. (2024). Desafíos contemporáneos en la protección del derecho a la libertad personal frente a medidas de seguridad. ***Revista Diversidad Científica, 4***(2), 193–203. https://revistadiversidad.com/index.php/revista/article/view/140

González Monje, A. (2017). Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto. ***Revista Europea de Derechos Fundamentales, 29***, 267–294. https://gredos.usal.es/handle/10366/157196

Guamán Chacha, K. A., Hernández Ramos, E. L., & Lloay Sánchez, S. I. (2021). El proyecto de investigación: la metodología de la investigación científica o jurídica. Conrado, 17(81), 163–168. http://scielo.sld.cu/scielo.php?pid=S1990-86442021000400163&script=sci_arttext&tlng=en

Mozur, P., Kessel, J., & Chan, M. (2019). Hecho en China y exportado a Ecuador: el aparato de vigilancia estatal. The New York Times, 24, 1–10. https://www.centroculturalsol.com/chinaecuador.pdf

OEA. (2016). Convención Americana de Derechos Humanos. 1ra Edición. https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_colecciondebolsillo_10_convencion_americana_ddhh.pdf

ONU. (1966). Pacto Internacional de Derechos Civiles y Políticos. https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Ou, Q., Zhu, X., Chen, X., & Liu, Q. (2023). Human Behavior Recognition of Video Surveillance System Based on Neural Network. Procedia Computer Science, 228, 64–70. https://www.sciencedirect.com/science/article/pii/S187705092301832X?via%3Dihub

Pilamunga Coro, J. L. (2021). ***Uso de cámaras de vigilancia con reconocimiento facial y la vulneración de los derechos constitucionales*** [Informe de Investigación previo a la obtención del título de Abogada de los Tribunales y Juzgados de la República del Ecuador. Universidad Nacional de Chimborazo]. http://dspace.unach.edu.ec/handle/51000/7280

Ribeiro Navarrete, S., Saura, J. R., & Palacios Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. ***Technological Forecasting and Social Change,*** 167, 120681. https://www.sciencedirect.com/science/article/pii/S004016252100113X?via%3Dihub

Slezkine, P. (2014). From Helsinki to Human Rights Watch: how an American cold war monitoring group became an international human rights institution. Humanity: ***An International Journal of Human Rights, Humanitarianism, and Development, 5***(3), 345–370. https://muse.jhu.edu/article/562801

Sujkowski, M., Kozuba, J., Uchroński, P., Banaś, A., Pulit, P., & Gryżewska, L. (2023). Artificial Intelligence Systems for Supporting Video Surveillance Operators at International Airport. ***Transportation Research Procedi***a, 74, 1284–1291. https://www.sciencedirect.com/science/article/pii/S2352146523005707?via%3Dihub