LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, Asunción, Paraguay.
ISSN en línea: 2789-3855, 2025, Volumen VI

Protección de datos personales y tecnologías de vigilancia en el espacio público: desafíos normativos y garantías constitucionales

Protection of Personal Data and Surveillance Technologies in Public Spaces: Regulatory Challenges and Constitutional Guarantees

Luis Fernando Sanchez Guanoluisa
lsanchez45@indoamerica.edu.ec
https://orcid.org/0009-0006-7034-2702
Facultad de Jurisprudencia y Ciencias Políticas de la Universidad Indoamérica
Ecuador

Juan Pablo Santamaria Velasco
juansantamaria@uti.edu.ec
https://orcid.org/0000-0002-8775-4600
Universidad Tecnológica Indoamérica (UTI)
Ecuador

DOI: https://doi.org/10.56712/latam.v6i5.4679

Artículo recibido: 25 de junio de 2025
Aceptado para publicación: 20 de octubre de 2025.
Conflictos de Interés: Ninguno que declarar.

Redilat
Red de Investigadores Latinoamericanos

NÚMERO

DOI: https://doi.org/10.56712/latam.v6i5.4679

Protección de datos personales y tecnologías de vigilancia en el espacio público: desafíos normativos y garantías constitucionales

Protection of Personal Data and Surveillance Technologies in Public Spaces: Regulatory Challenges and Constitutional Guarantees

Luis Fernando Sanchez Guanoluisa
lsanchez45@indoamerica.edu.ec
https://orcid.org/0009-0006-7034-2702
Facultad de Jurisprudencia y Ciencias Políticas de la Universidad Indoamérica
Ecuador

Juan Pablo Santamaria Velasco
juansantamaria@uti.edu.ec
https://orcid.org/0000-0002-8775-4600
Universidad Tecnológica Indoamérica (UTI)
Ecuador

Artículo recibido: 25 de junio de 2025. Aceptado para publicación: 20 de octubre de 2025.
Conflictos de Interés: Ninguno que declarar.

Resumen

El uso acelerado de tecnologías de videovigilancia y reconocimiento facial en espacios públicos del Ecuador plantea serias tensiones entre la seguridad ciudadana y la protección de derechos fundamentales como la intimidad y los datos personales. El objetivo principal de esta investigación es analizar los vacíos normativos existentes en el ordenamiento jurídico ecuatoriano frente a estas prácticas, y proponer criterios que permitan garantizar un equilibrio entre seguridad y derechos constitucionales. La problemática se centra en la falta de regulación específica sobre el tratamiento de datos recolectados mediante tecnologías de vigilancia, así como en la ausencia de mecanismos efectivos de control institucional. Para abordar esta cuestión, se empleó una metodología cualitativa con enfoque jurídico, a través de tres métodos complementarios: el método jurídico-exegético para analizar la Constitución y leyes vigentes; el método documental para revisar literatura especializada y estándares internacionales; y el método descriptivo-analítico para identificar casos y prácticas vulneradoras en el contexto nacional. Entre los principales hallazgos se identifican: la insuficiencia del marco legal actual para proteger los derechos frente al uso de tecnologías intrusivas; la delegación normativa inadecuada en la Ley Orgánica de Vigilancia y Seguridad Privada; y la debilidad de los mecanismos de supervisión y rendición de cuentas. En conclusión, se advierte la necesidad urgente de una reforma normativa que incorpore principios de legalidad, proporcionalidad, transparencia y control democrático, a fin de garantizar la vigencia efectiva de los derechos fundamentales frente al avance de las tecnologías de vigilancia en el espacio público.

Palabras clave: datos personales, derechos fundamentales, intimidad, tecnologías de vigilancia, videovigilancia

Abstract

The accelerated use of video surveillance and facial recognition technologies in public spaces in Ecuador raises serious tensions between citizen security and the protection of fundamental rights

such as privacy and personal data. The main objective of this research is to analyze the existing regulatory gaps in Ecuador's legal framework regarding these practices and to propose criteria that ensure a balance between security and constitutional rights. The core issue lies in the lack of specific regulations on the processing of data collected through surveillance technologies, as well as the absence of effective institutional control mechanisms. To address this issue, a qualitative methodology with a legal approach was used, through three complementary methods: the legal-exegetical method to analyze the Constitution and current laws; the documentary method to review specialized literature and international standards; and the descriptive-analytical method to identify cases and rights-violating practices in the national context. Among the main findings are: the insufficiency of the current legal framework to protect rights against intrusive technologies; the improper normative delegation in the Organic Law of Private Security and Surveillance; and the weakness of oversight and accountability mechanisms. In conclusion, the study highlights the urgent need for regulatory reform incorporating principles of legality, proportionality, transparency, and democratic control, in order to effectively guarantee fundamental rights in the face of advancing surveillance technologies in public spaces.

Keywords: fundamental rights, personal data, privacy, surveillance technologies, video surveillance

Cómo citar: Sanchez Guanoluisa, L. F., & Santamaria Velasco, J. P. (2025). Protección de datos personales y tecnologías de vigilancia en el espacio público: desafíos normativos y garantías constitucionales. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 6 (4), 1436 – 1450. https://doi.org/10.56712/latam.v6i5.4679*

INTRODUCCIÓN

En los últimos años, el uso de tecnologías de videovigilancia y reconocimiento facial en espacios públicos ha experimentado un crecimiento acelerado en el Ecuador, impulsado principalmente por el discurso de fortalecimiento de la seguridad ciudadana. Este fenómeno responde a una tendencia global en la que se han incorporado herramientas de inteligencia artificial y sistemas biométricos capaces de identificar rostros humanos, rastrear movimientos y almacenar información sensible de manera automatizada. Sin embargo, la implementación de estas tecnologías en el país se ha llevado a cabo sin un marco normativo suficiente ni con garantías institucionales adecuadas que protejan los derechos fundamentales de las personas, particularmente el derecho a la privacidad, la intimidad y la protección de datos personales.

La Constitución de la República del Ecuador (CRE), en su artículo 66, numeral 19, reconoce expresamente el derecho a la protección de datos personales. Este derecho otorga a toda persona la facultad de acceder, rectificar, cancelar y oponerse al tratamiento de su información personal, estableciendo un marco de garantías fundamentales que cobra especial relevancia en contextos de vigilancia tecnológica. No obstante, pese a este mandato constitucional, el marco jurídico actual presenta serias deficiencias. La recientemente aprobada Ley Orgánica de Vigilancia y Seguridad Privada (LOVSP) no regula de manera específica el uso de tecnologías de videovigilancia ni contempla disposiciones técnicas o jurídicas que establezcan límites claros para el uso de datos biométricos o imágenes faciales.

Esta situación se agrava por la ausencia de estándares técnicos mínimos, obligaciones de transparencia institucional, evaluación de impacto en derechos fundamentales, ni mecanismos eficaces de control y supervisión independientes. Asimismo, la normativa no contempla garantías como el consentimiento informado ni criterios de proporcionalidad y necesidad en el uso de estas tecnologías, permitiendo prácticas institucionales que han derivado en vulneraciones documentadas al derecho a la privacidad, a la libertad de expresión y a otros derechos conexos. Casos como el uso político de la videovigilancia por parte de organismos de inteligencia en el pasado, como la desaparecida SENAIN, revelan el riesgo latente de que estas herramientas se empleen con fines ajenos a la seguridad pública y en contravención a los principios democráticos.

La presente investigación se justifica por la necesidad de evidenciar los vacíos normativos que afectan directamente la protección de datos personales frente al uso de tecnologías de vigilancia en espacios públicos. La falta de regulación específica y el limitado control institucional sobre herramientas altamente intrusivas constituyen una amenaza estructural para el ejercicio de derechos fundamentales en el Ecuador. Esta situación exige no solo una revisión crítica del marco legal vigente, sino también una reflexión sobre las medidas necesarias para garantizar un equilibrio entre seguridad y derechos humanos, conforme al principio de legalidad, proporcionalidad y transparencia. En este sentido, el estudio busca aportar a la construcción de un enfoque jurídico que permita proteger eficazmente los derechos de los ciudadanos frente al avance de tecnologías que, si bien pueden ser útiles para la seguridad, también representan un riesgo si se aplican sin límites ni garantías.

Desde un enfoque cualitativo, la investigación se desarrollará a través de tres métodos complementarios. En primer lugar, mediante el método jurídico-exegético, se realizará un análisis detallado de la Constitución del Ecuador y de la Ley Orgánica de Vigilancia y Seguridad Privada, con el objetivo de identificar los vacíos normativos en torno al tratamiento de datos sensibles recolectados a través de videovigilancia. En segundo lugar, se aplicará el método documental o bibliográfico, con el fin de revisar estudios académicos y literatura especializada que permita comprender el funcionamiento de los sistemas de videovigilancia, así como los riesgos asociados a la ausencia de control legal e institucional. Finalmente, a través del método descriptivo-analítico, se abordarán casos concretos y datos disponibles para describir el impacto real del uso de estas tecnologías en los

derechos ciudadanos, identificando prácticas vulneradoras y deficiencias estructurales que requieren ser atendidas con urgencia.

METODOLOGÍA

La presente investigación adopta un enfoque cualitativo con orientación jurídica, ya que busca analizar las normas, principios y prácticas relacionadas con el uso de tecnologías de vigilancia en espacios públicos y su incidencia en la protección de datos personales y derechos fundamentales en el Ecuador. Este enfoque permite comprender la dimensión normativa y doctrinaria del problema, así como identificar las tensiones existentes entre seguridad ciudadana y garantías constitucionales.

Se emplearon tres métodos complementarios. En primer lugar, el método jurídico-exegético, mediante el cual se realizó un análisis detallado de la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales (2021) y la Ley Orgánica de Vigilancia y Seguridad Privada (2024), con el fin de identificar los vacíos normativos y contradicciones que afectan el derecho a la intimidad y a la autodeterminación informativa.

En segundo lugar, se aplicó el método documental o bibliográfico, consistente en la revisión de literatura académica, estudios comparados, doctrina especializada y estándares internacionales, tales como el Reglamento General de Protección de Datos de la Unión Europea (RGPD) y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Esta revisión permitió contrastar la regulación ecuatoriana con experiencias comparadas y con los compromisos internacionales asumidos por el país.

Finalmente, se utilizó el método descriptivo-analítico, con el objetivo de examinar casos concretos y prácticas institucionales documentadas en el contexto ecuatoriano. Este método permitió no solo describir la implementación de tecnologías de videovigilancia y reconocimiento facial en espacios públicos, sino también analizar críticamente su impacto en el ejercicio de derechos fundamentales, evidenciando las debilidades estructurales en materia de control, supervisión y transparencia.

La combinación de estos métodos posibilitó construir un análisis integral que articula la revisión normativa, la doctrina especializada y la realidad práctica de la vigilancia en el Ecuador. De esta manera, se garantiza que las conclusiones y propuestas del estudio tengan un sustento tanto jurídico como empírico.

DESARROLLO

Derecho a la protección de datos personales en Ecuador

El derecho a la protección de datos personales en Ecuador ha experimentado una evolución significativa en las últimas décadas, consolidándose como una garantía fundamental en el ordenamiento jurídico nacional. Este derecho se articula como una manifestación directa de la autodeterminación informativa y de la dignidad humana, en tanto que reconoce a las personas la titularidad sobre su información personal, así como el poder de decidir cuándo, cómo y para qué fines sus datos pueden ser tratados.

Álvarez (2017) plantea que la protección de datos personales debe entenderse como un sistema normativo integral, diseñado para resguardar la privacidad de los individuos frente al tratamiento de su información en entornos digitales. Este sistema incluye no solo la identificación clara de qué constituye un dato personal, sino también la responsabilidad de quienes los recopilan, procesa o almacenan, así como las condiciones en las que deben hacerlo. Además, establece principios fundamentales como la seguridad, confidencialidad, conservación y acceso a los datos, incluyendo reglas específicas para su transferencia a otros países.

La primera aproximación formal a la protección de datos en Ecuador se dio con la reforma constitucional de 1996, cuando se incorporó el hábeas data como una garantía jurisdiccional. Sin embargo, es con la Constitución de 2008 que se reconoce de forma expresa y autónoma el derecho a la protección de datos personales, estableciendo estándares cercanos a los europeos sobre esta materia (Rosas-Lanas & Pila-Cárdenas, 2023). La CRE (2008) consagra:

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. (art. 66. 19).

Este artículo declara este derecho como parte de los derechos de libertad. Así, el constituyente ecuatoriano reconoce la titularidad de los datos personales como un atributo inalienable de la persona humana, vinculandolo con el respeto a su privacidad, dignidad e integridad. En estrecha relación con este derecho, el artículo 66 también incluye, en sus numerales 20 y 21, los derechos a la intimidad personal y familiar, y a la inviolabilidad de la correspondencia física y virtual, que refuerzan la protección de los datos en contextos tecnológicos y comunicacionales, estableciendo límites al acceso o retención de información personal sin orden judicial, lo que refuerza el principio de legalidad y el debido proceso.

Sin embargo, tal como lo señala Álvarez (2017), esta disposición constitucional, aunque valiosa, presenta ambigüedades e insuficiencias. Por ejemplo, no define qué se entiende por dato personal, ni establece directrices claras para su tratamiento en el ámbito público o privado. La imprecisión conceptual entre dato e información que en términos técnicos y jurídicos no son equivalentes– puede dar lugar a interpretaciones erróneas. Mientras el dato representa una unidad mínima, aislada y sin contexto, la información implica un proceso de organización y valoración de datos que genera significado. Esta omisión puede debilitar la efectividad de la tutela constitucional al dejar áreas grises para la interpretación judicial y administrativa.

Para proteger a este derecho la CRE (2008) establece la garantía de hábeas data, e indica:

> Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. (art. 92).

Este precepto fortalece el principio de autodeterminación informativa, al permitir que el titular de los datos pueda ejercer un poder real sobre su información, lo que implica no solo acceso pasivo, sino también la posibilidad de ejercer derechos derivados como la rectificación, actualización o eliminación de los datos. Al extender este derecho frente tanto al sector público como al privado, el artículo rompe con una visión tradicional limitada al ámbito estatal, reconociendo la simetría de riesgos que representan las entidades privadas en el tratamiento masivo de datos, especialmente en contextos digitales.

Según Naranjo (2017) esta garantía incorpora, de hecho, los principios ARCO (Acceso, Rectificación, Cancelación y Oposición), fundamentales en la protección de datos personales. A través de esta acción, el titular puede controlar activamente el tratamiento de su información, incluso respecto a los fines, origen y tiempo de conservación de la misma. Tal como señala este autor, este mecanismo no solo protege la privacidad, sino que también refuerza el principio de autodeterminación informativa, es decir, la facultad que tiene cada persona para decidir sobre el uso y circulación de su información

personal. En un contexto de acelerado desarrollo tecnológico y creciente recolección de datos por parte de empresas y Estados, esta facultad adquiere una importancia vital.

En el plano internacional, Ecuador ha asumido compromisos sustanciales respecto a la protección de datos personales. Por ejemplo, forma parte de la Red Iberoamericana de Protección de Datos, donde, en el año 2017, se aprobaron los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, que constituyen una guía para la adopción de marcos regulatorios. Asimismo, Ecuador suscribió la Carta Iberoamericana de Gobierno Electrónico, donde se estableció el principio de legalidad para el tratamiento de datos personales, y ha acogido recomendaciones de la Organización de Estados Americanos (OEA), como la Ley Modelo sobre Protección de Datos Personales del año 2015. Además, el Acuerdo Comercial entre la Unión Europea y Ecuador, en su artículo 164, obliga a desarrollar o mantener una normativa adecuada para la protección de datos personales, lo que refuerza la necesidad de adecuarse a estándares internacionales como el Reglamento General de Protección de Datos (RGPD) europeo. (Aguilar et al., 2022). Estos compromisos internacionales no son meramente declarativos: constituyen fuentes de derecho relevantes en virtud del artículo 417 de la Constitución, que otorga jerarquía constitucional a los tratados internacionales de derechos humanos.

En cumplimiento de estos compromisos y ante la necesidad de un marco legal específico, el Ecuador promulgó la Ley Orgánica de Protección de Datos Personales (LOPDP) el 26 de mayo de 2021. Esta ley, compuesta por 77 artículos, establece un régimen jurídico detallado para el tratamiento de datos personales y consolida el sistema nacional de protección.

Según Aguilar et al. (2022), la LOPDP busca garantizar el derecho a la autodeterminación informativa y regular todo el ciclo de tratamiento de los datos personales, desde su obtención hasta su supresión. Además, contempla categorías especiales de datos, como los datos sensibles, de menores de edad, y datos de salud o discapacidades, para los cuales se exigen medidas de seguridad reforzadas.

Uno de los aportes más significativos de esta ley es la creación de una Autoridad de Protección de Datos Personales, como órgano autónomo adscrito a la Superintendencia de Protección de Datos. Esta autoridad no solo debe supervisar el cumplimiento de la ley, sino también dictar políticas públicas, imponer sanciones, promover buenas prácticas y educar a la ciudadanía en materia de protección de datos. La ley también establece el Registro Nacional de Protección de Datos Personales, y regula de forma detallada el consentimiento, la transferencia internacional de datos, las medidas de seguridad, la responsabilidad de los responsables del tratamiento, y el régimen sancionatorio.

A pesar de los avances normativos, subsisten retos importantes. Como advierte Jurado et al. (2023), la ley no aborda con suficiente claridad el tratamiento de datos en contextos transnacionales, lo que plantea desafíos frente a plataformas digitales globales que operan fuera del territorio ecuatoriano. Esta limitación podría debilitar la aplicación efectiva del marco normativo, en especial en lo que concierne al seguimiento de empresas tecnológicas que recolectan datos de los ecuatorianos sin sujeción a la jurisdicción nacional.

Según la doctrina, es fundamental que el derecho ecuatoriano avance hacia una definición más precisa y operativa del concepto de dato personal, diferenciándolo de la información y delimitando de manera clara sus categorías y tratamiento. Como lo señala Naranjo (2017), el reconocimiento del derecho debe basarse en el principio de legalidad y en la finalidad específica para la cual los datos fueron recolectados, evitando usos arbitrarios o desproporcionados que afecten la privacidad del titular.

Derecho a la intimidad personal frente a las nuevas tecnologías

El derecho a la intimidad personal constituye una de las garantías fundamentales del ser humano, consagrada expresamente en el numeral 20 del artículo 66 de la CRE (2008), el cual establece la protección frente a cualquier injerencia indebida en la vida privada, familiar o en la correspondencia de las personas. A nivel penal, esta garantía también cuenta con respaldo en el artículo 178 del Código Orgánico Integral Penal (COIP, 2014), que tipifica como delito la violación a la intimidad, reforzando así su carácter inviolable dentro del ordenamiento jurídico ecuatoriano.

Este reconocimiento no es aislado ni exclusivamente nacional, sino que responde a un marco normativo internacional, como lo refleja el artículo 12 de la Declaración Universal de los Derechos Humanos (1948), que prohíbe expresamente las intromisiones arbitrarias en la vida privada, la familia, el domicilio o la correspondencia, y garantiza la protección legal frente a tales actos. Este marco normativo revela que la intimidad no es simplemente un derecho formal, sino una expresión concreta de la dignidad humana, cuyo resguardo exige mecanismos efectivos de protección, especialmente en la actual era digital.

La intimidad, como bien jurídico protegido, no solo abarca el ámbito doméstico o familiar, sino que se extiende a todo aquello que una persona decide reservar para sí, sea en su cuerpo, pensamientos, hábitos, emociones o información personal, tal como lo define Murillo Carrasco (2020), quien afirma que este derecho alude a lo más íntimo del ser, una dimensión esencialmente personal e intransferible. Esta conceptualización pone en evidencia que el respeto a la intimidad implica reconocer la autonomía del individuo sobre su propia vida interior y la facultad de decidir qué aspectos compartir y cuáles mantener en reserva. No obstante, este derecho enfrenta una amenaza creciente en el contexto contemporáneo, donde el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) ha transformado profundamente la forma en que se produce almacena y difunde la información. Como advierte Solórzano Vera (2023), los dispositivos tecnológicos actuales ordenadores, teléfonos móviles, memorias, servidores contienen una cantidad inmensa de datos personales, lo cual multiplica las posibilidades de acceso no autorizado y vulneración, incluso sin consentimiento del titular.

En este escenario, las nuevas tecnologías representan una de las principales vías por las cuales la intimidad puede verse comprometida, tanto por la imprudencia de los propios usuarios como por las prácticas abusivas de terceros. Baño Carvajal y Reyes Estrada (2020) sostienen que muchas personas comparten en internet información privada sin medir las consecuencias, o peor aún, pueden ser víctimas de publicaciones maliciosas que se viralizan en segundos y generan daños psicosociales y emocionales significativos. Esta realidad evidencia que la vulneración de la intimidad no requiere contacto físico ni intervención directa: basta una publicación no autorizada, una imagen filtrada o un comentario difamatorio para que el espacio íntimo de una persona sea invadido y su dignidad afectada. Así, las TIC, aunque útiles para el ejercicio de derechos y libertades, también se han convertido en un canal de riesgos jurídicos y sociales que requieren atención normativa urgente.

Desde el enfoque filosófico-jurídico, autores como García (2017) sostienen que la intimidad constituye un atributo exclusivo del ser humano, sobre el cual ningún otro tiene derecho a intervenir. En esta línea, el derecho a la intimidad no es absoluto, pues encuentra límites cuando entra en conflicto con otros derechos, como la libertad de expresión o el interés público; sin embargo, su núcleo esencial lo secreto, reservado y personal debe permanecer protegido. En consonancia, Martínez (2022) subraya que este derecho se manifiesta como una libertad negativa, es decir, como un espacio libre de coacciones externas en el que el individuo puede tomar decisiones sin injerencia ajena. Esto es especialmente relevante en el entorno digital, donde la capacidad de decidir quién accede a la información personal y con qué finalidad debe estar garantizada por mecanismos legales efectivos. La intimidad, entonces, no solo protege hechos o datos, sino el poder de decisión sobre estos, es decir, la autodeterminación informativa, íntimamente vinculada con la dignidad humana y el desarrollo de la personalidad.

Adicionalmente, resulta pertinente considerar que la intimidad implica el derecho de toda persona a vivir en paz dentro de su esfera privada, sin interferencias indebidas, y a mantener en reserva comportamientos o rasgos personales como deseos, emociones y gestos (Caino Arboleda, 2020). Esta idea refuerza la noción de que la intimidad no se limita a lo que se oculta, sino que representa una elección consciente sobre qué se quiere preservar. Así, en una sociedad donde la exposición pública se ha normalizado incluso incentivado es fundamental reafirmar que la decisión de mantenerse en el anonimato o el silencio también constituye una manifestación legítima de libertad.

No obstante, como advierte Solórzano Vera (2023), el problema actual radica en que muchas veces los sistemas informáticos, que antes eran controlados por personas, ahora procesan automáticamente información sensible sin supervisión directa. Esto genera una nueva forma de amenaza, más compleja, en la cual no basta con proteger físicamente la información, sino que se requiere una arquitectura legal y tecnológica sólida para garantizar que el tratamiento de datos respete la esfera privada del individuo. Es por ello que Martínez (2022) enfatiza la necesidad de analizar las TIC no solo desde lo técnico, sino desde lo jurídico, social y económico, dado que sus implicaciones trascienden lo tecnológico y afectan directamente los derechos fundamentales.

Tecnologías de vigilancia masiva y los derechos fundamentales

El desarrollo de las tecnologías de vigilancia masiva ha supuesto una transformación radical en la forma en que el Estado ejerce su poder de control sobre la ciudadanía, generando profundas tensiones con el respeto y la garantía de los derechos fundamentales. Esta evolución no es un fenómeno aislado del presente, sino que se inscribe en una genealogía del poder, donde la vigilancia ha sido una herramienta esencial para el ejercicio del control social desde hace siglos.

Desde una perspectiva histórica, es posible identificar en el siglo XVIII un momento fundacional del despliegue moderno de los sistemas de vigilancia, vinculado especialmente a los movimientos de reforma penitenciaria. Durante este periodo, se comenzaron a plantear modelos que, si bien buscaban racionalizar el castigo, también promueven estructuras cada vez más complejas de observación, control y aislamiento. Un ejemplo paradigmático fue el diseño arquitectónico del panóptico, concebido como una herramienta para que los reclusos se sintieran constantemente observados, incluso sin certeza de estarlo, generando así un mecanismo de autocontrol que interioriza la vigilancia como forma de disciplina. Este modelo sentó las bases de una vigilancia organizada científicamente desde el Estado, orientada a imponer orden y seguridad mediante tecnologías adaptadas al contexto histórico (Gómez & Rodríguez, 2018).

Ya en épocas más recientes, se advierte cómo estas prácticas de vigilancia se han trasladado del encierro físico a la sociedad abierta, dando paso a mecanismos de control que alcanzan al conjunto de la ciudadanía. La visibilidad constante, que otrora se limitaba al espacio penitenciario, se ha expandido a todos los ámbitos de la vida cotidiana, erosionando los espacios de intimidad y privacidad. La vigilancia contemporánea, al posibilitar que los individuos se perciban permanentemente observados, produce efectos similares de autocontrol, ya no por la fuerza, sino por la interiorización de la mirada vigilante. En este nuevo contexto, se consolida un modelo de control más sofisticado y sutil, donde el poder no necesita imponerse con coacción directa, sino que actúa sobre la conducta mediante la percepción constante de ser vigilado (Santiago & Rodríguez, 2018).

En la actualidad, como bien señalan Gómez y Rodríguez (2018), esta dinámica de control se ha sofisticado enormemente gracias a las tecnologías de vigilancia masiva. Herramientas como drones, cámaras inteligentes, software de reconocimiento facial y plataformas de análisis de big data permiten una observación sistemática, automatizada y permanente de la población. Aunque estas herramientas suelen justificarse en nombre de la seguridad y la prevención del delito, su uso indiscriminado

representa un grave riesgo para derechos como la intimidad, la privacidad, el anonimato y la libertad personal.

Un argumento común para legitimar esta vigilancia sostiene que, si las personas no tienen nada que ocultar, no deberían temer ser observadas (Parmo, 2018). Este enfoque parte de una premisa profundamente errónea, pues presupone que la privacidad solo es relevante para los culpables o sospechosos, lo cual desnaturaliza su esencia como derecho inherente a toda persona. El interés del Estado en prevenir el delito no es absoluto y debe ser ponderado frente a otros principios constitucionales, como la dignidad humana, la libertad individual y la autonomía personal.

El derecho a la privacidad no se reduce a un espacio libre de intervención estatal, sino que constituye un elemento esencial para el desarrollo de la personalidad, la libertad de expresión, la participación democrática y la vida en sociedad. Así lo ha reconocido el derecho internacional de los derechos humanos, en particular a partir de la preocupación de organismos como la ONU sobre el uso masivo e indiscriminado de tecnologías de vigilancia. En 2014, la Asamblea General advirtió cómo estas herramientas aumentaban la capacidad de los Estados para espiar e interceptar comunicaciones, afectando el derecho a la privacidad (Parmo, 2018). Ese mismo año, el Alto Comisionado de Naciones Unidas calificó la vigilancia masiva como un hábito peligroso, que ya no se aplica como medida excepcional, sino como regla general, atentando contra el carácter excepcional que deberían tener las restricciones a los derechos fundamentales.

Más allá de la captación de imágenes o datos, el problema se agudiza en el tratamiento sistemático e indiscriminado de esa información. Las tecnologías actuales permiten una observación intensiva y continua de los movimientos de las personas en espacios públicos, convirtiendo lo que antes era una vigilancia ocasional en una especie de crónica enciclopédica de la vida cotidiana (Parmo, 2018). Este tipo de vigilancia conlleva riesgos concretos: inhibe el ejercicio libre de derechos como la reunión, la manifestación, la expresión o la circulación; disuade la presencia en espacios públicos y genera una forma de autocensura colectiva. Además, elimina el anonimato, que es un componente importante de la autonomía personal, al permitir a los ciudadanos actuar sin ser etiquetados, perfilados o evaluados por sus acciones presentes o pasadas.

Tecnologías como el reconocimiento facial ocupan un lugar especialmente sensible. Estas herramientas procesan enormes cantidades de datos biométricos, y su implementación –aunque motivada por discursos de seguridad– no siempre asegura la proporcionalidad ni el respeto a los principios de necesidad y legalidad. Como advierten Burbano et al (2021), la biometría, y especialmente el reconocimiento facial, se ha convertido en uno de los métodos más utilizados para la individualización y el control de las personas. Aunque su uso se justifica con base en la seguridad, esto no garantiza que se respeten los principios fundamentales del derecho a la intimidad. De hecho, se ha documentado que estas tecnologías generan desigualdades al enfocarse de manera desproporcionada en grupos vulnerables o estigmatizados, reproduciendo prácticas discriminatorias y afectando la dignidad de quienes son objeto de vigilancia constante.

En este marco, resulta fundamental cuestionar la neutralidad de las tecnologías de vigilancia. Como señalan Bauman & Lyon (2013) la vigilancia ya no busca disciplinar cuerpos, como en el modelo clásico del panóptico, sino que opera a través del procesamiento de información. Esto implica una nueva forma de control que evalúa, predice y categoriza comportamientos, integrándose de forma casi invisible en la vida cotidiana. En la era digital, según Ramonet (2015), asistimos a un choque de realidades: la posibilidad técnica de una vigilancia total, la necesidad de proteger la vida privada y la demanda social de seguridad. La vigilancia digital aparece entonces como una solución a los miedos colectivos, pero su legitimidad jurídica debe ser examinada con rigor.

Es por eso que Bauman y Lyon (2013) introducen el concepto del sinóptico, como contraparte al panóptico, para describir una vigilancia globalizada y digitalizada en la que los ciudadanos, voluntariamente o no, entregan su información, la cual es utilizada para su control. Esta nueva estructura de poder no necesita la torre del panóptico: se articula a través de redes, datos y algoritmos, en un mundo donde la seguridad es fluida, pero también ilusoria. En este sentido, la vigilancia digital ya no persigue únicamente el orden social o la productividad, sino que configura identidades, excluye, clasifica y moldea el comportamiento humano.

Desde una perspectiva jurídica, esto obliga a repensar los límites del poder estatal en materia de seguridad. Las políticas públicas deben someterse a estrictos criterios de proporcionalidad, legalidad, necesidad y rendición de cuentas. La mera existencia de una amenaza no autoriza la instauración de sistemas de control permanente que supriman la esfera íntima del individuo. El Tribunal Europeo de Derechos Humanos, por ejemplo, ha sostenido que incluso las medidas de vigilancia en espacios públicos deben justificarse caso por caso y estar reguladas por normas claras y accesibles.

Las tecnologías de vigilancia masiva, lejos de constituir herramientas neutrales para garantizar la seguridad, implican desafíos cruciales para el derecho a la intimidad, la autonomía y la dignidad humana. La creciente digitalización del poder requiere una vigilancia ciudadana del vigilante, es decir, un control democrático del ejercicio del poder estatal. Solo así podrá asegurarse que el uso de la tecnología no derive en una sociedad sometida al miedo, la estigmatización y la autocensura, sino en una convivencia basada en el respeto a los derechos fundamentales.

Análisis de la Ley Orgánica de Vigilancia y Seguridad Privada

La LOVSP, publicada en el Registro Oficial Suplemento N.º 496 del 9 de febrero de 2024, regula el funcionamiento de las empresas y servicios de seguridad privada en el Ecuador. Si bien la finalidad principal de esta norma es fortalecer la seguridad ciudadana a través del apoyo del sector privado, su articulado incluye disposiciones que suscitan serias preocupaciones respecto al respeto del derecho a la intimidad y la protección de datos personales en el contexto específico de la vigilancia en espacios públicos. La LOVSP (2024) consagra:

El Sistema de Vigilancia y Seguridad Privada es el conjunto de instituciones, políticas, estrategias, normativas, planes, programas que tienen por objeto conducir, de manera estratégica y preventiva, la seguridad privada dentro del territorio ecuatoriano, en la que se encuentran involucrados y articulados el sector público y privado. El Sistema de Vigilancia y Seguridad Privada, como parte del Sistema de Seguridad Pública y del Estado, se alineará a la política de seguridad integral. (art. 6).

Aunque esta integración puede verse como una medida para fortalecer la coordinación institucional, también plantea riesgos importantes en cuanto a la difuminación de responsabilidades y la falta de límites claros entre lo público y lo privado en el ejercicio de actividades de vigilancia. Esta fusión estructural puede permitir que tareas propias de la función estatal de seguridad —que deben estar sujetas a control democrático y a mecanismos de rendición de cuentas— sean ejecutadas por actores privados con menor supervisión y sin las garantías propias del derecho público. En el contexto de la vigilancia en espacios públicos, esto significa que la presencia de cámaras, el tratamiento de imágenes, la identificación de personas o la generación de perfiles conductuales podrían estar en manos de operadores privados que, aunque formalmente integrados a un sistema estatal, carecen de legitimidad directa y de controles efectivos.

Uno de los artículos más controvertidos es el artículo 25 de la LOVSP que indica:

> En el reglamento a esta ley, se normará la forma en que se articulará el Sistema Nacional de Vigilancia y Seguridad Privada con el Sistema de Seguridad Pública y del Estado, el Sistema

> Integrado de Seguridad ECU 911; y, la Policía Nacional, a fin de promover la cooperación en las políticas para la seguridad integral con fines preventivos. La reglamentación a la que se refiere el inciso precedente incorporará los mecanismos, entidades involucradas, periodicidad, indicadores y resultados esperados de la coordinación y articulación. (LOVSP, 2024, art. 25).

El principal problema jurídico radica en que la ley remite al reglamento el desarrollo de aspectos sustanciales de la coordinación entre entidades públicas y privadas que realizan actividades de vigilancia. Esta remisión resulta cuestionable en tanto que la regulación de aspectos que puedan implicar limitaciones o afectaciones a derechos fundamentales como la captación, tratamiento y transferencia de imágenes o datos personales en espacios públicos debe estar contenida en una norma con rango legal, conforme al principio de reserva de ley. De lo contrario, se corre el riesgo de que elementos esenciales del ejercicio de derechos queden sujetos a una regulación administrativa de menor jerarquía, sin control parlamentario ni garantía de debate democrático.

La articulación entre sistemas como el ECU 911, la Policía Nacional y empresas privadas de seguridad en el contexto de la vigilancia en espacios públicos puede generar un modelo de interoperabilidad y circulación de datos que afecte la privacidad de las personas. La norma no establece claramente los límites del acceso, tratamiento ni transferencia de la información captada por sistemas de videovigilancia, ni define con precisión los principios de finalidad, proporcionalidad o minimización de datos, lo cual es esencial para garantizar el derecho a la protección de datos personales. Esta ausencia normativa abre la posibilidad de que información recabada por agentes privados en espacios públicos termine siendo utilizada o almacenada por el Estado sin el consentimiento del titular, sin control judicial ni mecanismos de oposición.

El reglamento deberá establecer indicadores, periodicidad y resultados esperados de la coordinación institucional. Sin embargo, no se exige que este diseño contemple mecanismos efectivos de transparencia, fiscalización o rendición de cuentas hacia la ciudadanía. En contextos democráticos, toda práctica de vigilancia debe ser controlada tanto interna como externamente, y debe garantizar la trazabilidad del tratamiento de datos, especialmente cuando se involucran actores no estatales operando en espacios públicos. El enfoque de “seguridad integral con fines preventivos” no puede ser utilizado como una justificación genérica para implementar vigilancia masiva o sin controles, especialmente cuando la vigilancia en lugares públicos —donde las personas desarrollan libremente sus actividades cotidianas, se expresan o se asocian— tiene un alto impacto sobre los derechos fundamentales.

Este artículo evidencia una delegación normativa excesiva a la reglamentación posterior, lo que resulta problemático si se considera el estándar constitucional que exige que las restricciones a los derechos fundamentales se regulen mediante ley formal. La articulación entre sistemas públicos y privados de vigilancia en espacios públicos, en tanto afecta derechos como la intimidad y la protección de datos personales, requiere un marco normativo claro, preciso y con límites definidos. Por tanto, se recomienda que esta disposición sea desarrollada mediante un reglamento riguroso, que incorpore los principios constitucionales y que garantice mecanismos de supervisión, transparencia, y protección efectiva de los derechos de los ciudadanos frente al uso de tecnologías de vigilancia.

DISCUSIÓN

El presente estudio evidencia una tensión estructural entre la expansión de las tecnologías de vigilancia en espacios públicos y la garantía efectiva de los derechos fundamentales en Ecuador. A pesar de los avances en el reconocimiento constitucional del derecho a la protección de datos personales y la aprobación de una ley específica en la materia, persisten serias deficiencias normativas e institucionales que debilitan la tutela efectiva de los ciudadanos frente al uso masivo e indiscriminado de tecnologías como la videovigilancia y el reconocimiento facial.

Uno de los principales problemas identificados radica en la ausencia de un marco legal que establezca criterios claros sobre la proporcionalidad, legalidad, necesidad y finalidad del tratamiento de datos personales en contextos de vigilancia pública. La LOVSP, lejos de llenar este vacío, delega a la reglamentación posterior aspectos esenciales que afectan derechos fundamentales, como la forma de articulación entre sistemas de vigilancia públicos y privados. Esta delegación vulnera el principio de reserva de ley y permite que decisiones cruciales sobre derechos como la intimidad, el anonimato o la protección de datos se tomen sin control parlamentario ni debate democrático.

La literatura revisada confirma esta preocupación. Álvarez (2017) y Naranjo (2017) destacan la necesidad de una definición precisa y operativa del concepto de dato personal, así como la importancia de establecer límites normativos rigurosos al tratamiento de datos por parte de entidades públicas y privadas. Asimismo, Jurado et al. (2023) señalan las limitaciones de la Ley Orgánica de Protección de Datos Personales frente a fenómenos transnacionales como el tratamiento de datos por parte de plataformas digitales que operan fuera del ámbito jurisdiccional ecuatoriano.

A nivel filosófico-jurídico, los aportes de autores como García (2017), Martínez (2022) y Murillo Carrasco (2020) permiten comprender que tanto la privacidad como la intimidad son componentes esenciales de la dignidad humana, que no pueden ser subordinados al discurso securitario sin una estricta evaluación de impacto y legalidad. Estas perspectivas coinciden en que el avance tecnológico debe ser acompañado por una arquitectura legal robusta, que priorice la autodeterminación informativa y la transparencia.

La implementación acrítica de tecnologías de reconocimiento facial plantea riesgos adicionales. Tal como advierten Burbano et al. (2021), estas herramientas no solo pueden perpetuar prácticas discriminatorias, sino también erosionar el principio de presunción de inocencia al perfilar conductas o estigmatizar a ciertos grupos sociales. Esta situación se agrava por la falta de mecanismos de rendición de cuentas y control ciudadano sobre el uso y almacenamiento de datos biométricos, lo cual puede derivar en una vigilancia permanente que inhiba la libre expresión, la protesta o incluso la circulación en el espacio público.

La visión crítica de Parmo (2018), Gómez y Rodríguez (2018), y Bauman y Lyon (2013), complementa esta discusión al evidenciar cómo la vigilancia actual ya no se limita a la observación física, sino que opera a través del procesamiento automatizado de grandes volúmenes de datos, generando formas de control sutiles, pero igualmente eficaces. La figura del sinóptico, propuesta por Bauman y Lyon, ilustra un escenario en el que los ciudadanos se vuelven colaboradores conscientes o inconscientes del sistema de vigilancia, al entregar voluntariamente información a plataformas tecnológicas que la utilizan para clasificarlos, predecir sus conductas o moldear sus decisiones.

La LOVSP, al integrar el sistema de vigilancia privada al aparato estatal sin establecer límites precisos ni criterios de fiscalización independientes, reproduce un modelo de vigilancia que carece de legitimidad democrática y que pone en riesgo el equilibrio entre seguridad y derechos humanos. El artículo 25 de dicha ley evidencia esta problemática, al remitir a una norma de menor jerarquía la regulación de un aspecto sustancial que afecta el núcleo esencial del derecho a la intimidad.

CONCLUSIÓN

La investigación demuestra que el marco normativo ecuatoriano vigente es insuficiente para garantizar una protección efectiva de los datos personales frente al creciente uso de tecnologías de vigilancia en espacios públicos. Aunque la CRE reconoce expresamente el derecho a la protección de datos personales y se han adoptado leyes específicas como la LOPDP, subsisten importantes vacíos jurídicos, especialmente en lo relativo al uso de sistemas de videovigilancia, reconocimiento facial y la articulación entre actores públicos y privados en tareas de control y seguridad.

En particular, la LOVSP presenta un enfoque normativo que no satisface los estándares de legalidad exigidos para la limitación de derechos fundamentales. La remisión a la reglamentación secundaria para regular aspectos sensibles como la interoperabilidad entre el sistema de vigilancia estatal y el privado, sin establecer límites claros ni garantías sustantivas, vulnera el principio de reserva de ley previsto en el orden constitucional ecuatoriano.

El uso de tecnologías de vigilancia debe estar condicionado por normas claras, precisas y accesibles que desarrollen los principios de legalidad, necesidad, proporcionalidad, finalidad y rendición de cuentas. Todo tratamiento de datos personales en el contexto de la vigilancia pública debe estar sujeto a evaluación previa de impacto en derechos, contar con mecanismos de supervisión independientes, y garantizar al titular de los datos el ejercicio pleno de sus derechos ARCO.

Además, el uso de datos biométricos y tecnologías como el reconocimiento facial exige un régimen de protección reforzada, conforme a los principios del derecho internacional de los derechos humanos y las mejores prácticas comparadas. En este sentido, es indispensable que el legislador ecuatoriano reformule la normativa vigente, delimitando claramente las competencias de los actores involucrados y estableciendo garantías judiciales, institucionales y ciudadanas que aseguren que la vigilancia no se convierta en una herramienta de control social desmedido o discriminatorio.

Solo mediante un enfoque normativo riguroso y garantista será posible cumplir con el mandato constitucional de proteger la intimidad y los datos personales, sin renunciar a los fines legítimos de seguridad ciudadana. La seguridad no puede convertirse en una excusa para debilitar el Estado de derecho, sino que debe construirse sobre el respeto y la protección efectiva de los derechos fundamentales de todas las personas.

REFERENCIAS

Aguilar, M. R. M., López, J. A. P., Cevallos, D. P. G., & Burgos, G. P. L. (2022). La protección de datos personales en Ecuador. Estudios del Desarrollo Social: Cuba y América Latina, 10(especial 1).

Álvarez, L. E. (2017). 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. Obtenido de: http://scielo.senescyt.gob.ec/scielo.php?pid=S2631-24842017000100043&script=sci_arttext

Baño Carvajal, Ángela E. ., & Reyes Estrada, J. L. (2020). Vulneración del derecho a la intimidad personal y familiar en las redes sociales. Revista Jurídica Crítica Y Derecho, 1(1), 49–60. https://doi.org/10.29166/criticayderecho.v1i1.2447

Bauman, Z. y Lyon, D. (2012). Vigilancia Líquida. España: Editorial Ediciones Paidós. Bjørn, M. (1996) Conceptos sobre seguridad: nuevos riesgos y desafíos. Reviewed work(s): Source: Desarrollo Económico, vol. 36, no. 143, pp. 769-792. Published by: Instituto de Desarrollo Económico y Social Stable. Recuperado de http://www.jstor.org/stable/34672

Burbano, A. A., Navia, A. L., Loriet, S. L. (2021). Sistemas de vigilancia y su efecto en el derecho a la intimidad desde el discurso de la seguridadEn la actualidad, existen sistemas de vigilancia, como las herramientas de reconocimiento facial, que justifican su existencia en la noción de seguridad perso. Revista Latinoamericana De Derechos Humanos, 33(1), 33-51. https://doi.org/10.15359/rldh.33-1.2

Gómez, E. S., & Rodríguez-Rodríguez, C. (2018). Tecnologías de la vigilancia: una mirada hacia la violencia legítima del Estado en cuestiones de seguridad y control. Encrucijadas: Revista Crítica de Ciencias Sociales, (16), 14.

Jurado, Z. E. R., Riera, L. E. R., & Méndez, J. A. C. (2023). Protección de datos en el contexto de la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador. Polo del Conocimiento, 8(8), 1355-1373.

Martínez, J. A. S. (2022). Protección constitucional de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías. Anuario de derecho canónico: revista de la Facultad de Derecho Canónico integrada en la UCV, (11), 93-126.

Naranjo Godoy, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y hábeas data en Ecuador. Foro. Revista de Derecho, 27, 63-82. Obtenido de: https://revistas.uasb.edu.ec/index.php/foro/article/view/501/488

Parmo, D. A. L. (2018). Privacidad, espacios públicos y vigilancia. Anuario de Derecho Público, (1), 35-62.

Ramonet, I. (2015). El Imperio de la Vigilancia. Traducción de Martín Sacristán. Madrid: Editorial Clave Intelectual.

Rosas-Lanas, G., & Pila-Cárdenas, G. (2023). The protection of personal data in Ecuador: A historical-normative review of this fundamental right in the South American country. VISUAL REVIEW. International Visual Culture Review Revista Internacional De Cultura Visual, 13(2), 1–16. https://doi.org/10.37467/revvisual.v10.4568

Solorzano Vera, R. U. (2023). Derecho a la intimidad y el uso de las tecnologías de la información (Bachelor's thesis). Obtenido de: https://dspace.uniandes.edu.ec/handle/123456789/16155