INNOVACIÓN & SABER

Inteligencia estratégica antidelincuencial y protección de datos en Ecuador: aplicación del test de proporcionalidad

Strategic Crime Intelligence and Data Protection in Ecuador: Application of the Proportionality Test

Adriana Raquel Reyes Asanza[1]
Luis Miguel Espinosa Baldassari[2]

Recibido: 19 de mayo de 2026
Aceptado: 22 de mayo de 2026
Publicado: 08 junio de 2026

Resumen

Este artículo examina el uso de la inteligencia estratégica antidelincuencial en el marco del derecho a la protección de datos personales en Ecuador, con énfasis en los riesgos derivados del tratamiento masivo de la información, el perfilamiento y monitoreo por parte de las autoridades. Se adopta una metodología cualitativa basada en la revisión documental y el análisis doctrinario. Además, se aplica el test de proporcionalidad como criterio de control jurídico. Se concluye que la eficacia preventiva solo resulta legítima cuando el tratamiento de los datos responde a fines determinados, minimiza la información recolectada, incorpora salvaguardas y se somete a mecanismos de control y rendición de cuentas.

Palabras clave: datos personales; inteligencia; legalidad; minimización; proporcionalidad; seguridad; transparencia.

Abstract

This article examines the use of strategic anti-crime intelligence within the framework of the right to personal data protection in Ecuador, with an emphasis on the risks arising from the mass processing of information, profiling, and surveillance by authorities. A qualitative methodology based on a review of the literature and doctrinal analysis is adopted. Furthermore, the proportionality test is applied as a control criterion. It is concluded that preventive effectiveness is legitimate only when data processing serves specific purposes, minimizes the information collected, incorporates safeguards, and is subject to control and accountability mechanisms.

Keywords: accountability; data protection; strategic intelligence; legality; minimization; proportionality; security; transparency.

1 Instituto Superior Tecnológico Policía Nacional, Quito-Ecuador, raar1712753241@isupol.edu.ec, 0009-0000-3420-9708
2 Universidad Internacional SEK, Quito-Ecuador, luis.espinosa@uisek.edu.ec, 0000-0001-7161-629X

Introducción

La evolución contemporánea de los esquemas de seguridad integral exige reinterpretar de manera constante los mecanismos de inteligencia estratégica antidelincuencial, especialmente en contextos que priorizan el respeto de los derechos fundamentales y la privacidad. En el marco de la Ley Orgánica de Protección de Datos Personales de Ecuador, es necesario revisar críticamente las técnicas y estrategias de inteligencia empleadas por los cuerpos policiales, con atención en la pertinencia, necesidad y proporcionalidad de la obtención y el tratamiento de los datos personales.

Este análisis adquiere mayor relevancia en el contexto ecuatoriano, donde la actuación policial debe responder a los nuevos desafíos delictivos y, al mismo tiempo, ajustarse a los marcos regulatorios. En este contexto, el presente artículo examina el concepto de inteligencia estratégica antidelincuencial en Ecuador y su marco de actuación en un Estado de derechos. Se evalúa los principios rectores de la inteligencia estratégica desde la lógica de la ciencia clásica moderna y su adaptación al paradigma de responsabilidad pública.

Asimismo, se identifican las oportunidades y los retos para la gestión policial (Noboa y Moreano, 2019; Moreano y Noboa 2018). Se aplica el test de proporcionalidad a casos concretos, con el propósito de identificar tensiones y sinergias entre la eficacia operativa y la protección de los derechos fundamentales.

Objetivo general

Analizar la inteligencia estratégica antidelincuencial aplicada a la seguridad integral del Estado ecuatoriano, con énfasis en el tratamiento de datos personales utilizados y a partir de los límites establecidos por la Ley Orgánica de Protección de Datos Personales, los derechos fundamentales y el test de proporcionalidad.

Objetivos específicos

- Analizar el rol de la inteligencia estratégica antidelincuencial como herramienta orientada a prevenir el delito, identificar los riesgos y detectar las amenazas.
- Examinar el tratamiento de los datos personales con atención en los procesos de recopilación, uso y almacenamiento de la información, a fin de determinar su adecuación a los límites establecidos por la Ley Orgánica de Protección de Datos Personales.
- Aplicar el test de proporcionalidad para evaluar la legitimidad jurídica del uso de datos personales en la inteligencia antidelincuencial, e identificar los riesgos asociados con prácticas desproporcionadas que desbordan la protección de la privacidad y la dignidad humana.

La metodología empleada es cualitativa con corte jurídico doctrinal, basada en la revisión documental y el análisis argumentativo. En primer lugar, se delimitaron los conceptos operativos de inteligencia estratégica antidelincuencial y protección de datos, e identificaron los principios —finalidad, minimización, proporcionalidad, seguridad y rendición de cuentas— que condicionan el tratamiento de la información personal en contextos de seguridad integral del Estado.

En segundo lugar, se sistematizaron los escenarios típicos de intervención, como el monitoreo, perfilamiento, cruces de bases de datos y vigilancia focalizada, con el propósito de modelar las tensiones entre eficacia preventiva y derechos. En tercer lugar, se aplicó el test de proporcionalidad —idoneidad, necesidad y proporcionalidad — como matriz de evaluación. Para cada escenario se definió: el fin legítimo; la medida concreta de tratamiento; las alternativas menos lesivas; y las salvaguardas técnicas y jurídicas orientadas a reducir riesgos, tales como controles de acceso, trazabilidad, plazos de conservación y control.

La selección y revisión documental se efectuó desde los documentos alojados en las bases de datos de Scopus, Dialnet, Google Scholar, así

como en el repositorio jurídico de la Universidad Externado de Colombia. En la búsqueda se emplearon descriptores, entre ellos inteligencia antidelincuencial, test de proporcionalidad, seguridad integral del Estado, vigilancia y derechos fundamentales, y Ley Orgánica de Protección de Datos Personales Ecuador.

Se aplicaron los siguientes criterios de inclusión: documentos que aborden la relación entre actividades de inteligencia estatal y el derecho a la privacidad o la protección de datos personales; fuentes que desarrollen el test de proporcionalidad en contextos de seguridad pública; normativa nacional e internacional vigente sobre el objeto de estudio; y publicaciones en idioma español o inglés con respaldo académico o institucional verificable. Se excluyeron documentos sin identificación de autoría; fuentes sin fecha de edición y publicación; y materiales no relacionados con el contexto jurídico-institucional.

La principal limitación de la investigación es su carácter teórico-propositivo, pues los hallazgos derivan del análisis doctrinal y no de datos empíricos obtenidos de unidades operativas de inteligencia ecuatoriana. Aunque esta condición es coherente con el diseño cualitativo adoptado, restringe la generalización de los resultados a contextos específicos de implementación.

Fundamentos conceptuales

Inteligencia estratégica antidelincuencial en la lógica determinista y mecánica

La inteligencia estratégica aplicada al ámbito de la seguridad integral ha estado influenciada por la ciencia clásica moderna, en particular por la perspectiva mecánica y determinista que entiende la seguridad como resultado de la anticipación lógica y racional de las amenazas (Moreano y Noboa, 2019). Tal inteligencia se vincula con el paradigma de la disyunción y simplificación: prioriza la obtención, el procesamiento y el análisis sistémico de datos, con el propósito de identificar patrones delictivos susceptibles de intervención táctica.

Sin embargo, esta visión mecanicista es cuestionada por las sociedades actuales. La criminalidad contemporánea se desarrolla en escenarios marcados por la volatilidad, la incertidumbre y la posnormalidad, en los que la predictibilidad rigurosa cede ante la necesidad de flexibilidad metodológica (Moreano y Noboa, 2018). En esta transición, el ejercicio de la inteligencia debe incorporar variables ético-legales, especialmente aquellas que delimitan los marcos de actuación frente al tratamiento de los datos personales.

Protección de datos personales: un derecho fundamental

La Ley Orgánica de Protección de Datos Personales en Ecuador surgió como una respuesta al impulso internacional de reconocer el derecho a la autodeterminación informativa. Su marco normativo establece principios como legalidad, lealtad, finalidad, proporcionalidad y seguridad que deben atender las entidades públicas y privadas. En este contexto, el acceso, almacenamiento, análisis y difusión de información por parte de las unidades de inteligencia policial deben someterse al control previsto por esta ley, de modo que la eficacia para prevenir el delito se equilibre con la protección de dignidad y autonomía de las personas.

Surge una tensión entre los objetivos de la inteligencia estratégica y los derechos de protección de datos. En dicha tensión se impone la necesidad de aplicar mecanismos de control como el test de proporcionalidad, cuya función consiste en examinar si las restricciones al derecho a la privacidad superan un análisis de idoneidad, necesidad y proporcionalidad respecto a los fines perseguidos.

Estrategia argumentativa y paradigmas de actuación

De la disyunción a la complejidad

La literatura enfatiza en la transición del paradigma de la disyunción —propio de la ciencia clásica-moderna— hacia la comprensión de la inteligencia basada en paradigmas de articulación

compleja, que reconocen no solo la multiplicidad de las variables delictivas, sino también la variedad de derechos involucrados en operaciones policiales (Moreano y Noboa 2019). Este enfoque multidimensional exige que el operador policial integre información del entorno social, político, legal y psicológico, y que evalúe la eficacia operativa y el impacto de sus actuaciones sobre los derechos de las personas.

En Ecuador, el desafío consiste en superar un imaginario político, poco permeable a las prioridades vigentes en otros contextos regionales. Ello exige adaptar el sentido institucional alrededor del uso de la inteligencia y el respeto a los principios antes mencionados (Moreano y Noboa, 2018). La sofisticación de los delitos y la sensibilidad pública frente al abuso de poder refuerzan la legitimidad de la actuación policial solo cuando esta se fundamenta en criterios de razonabilidad y proporcionalidad.

El test de proporcionalidad como eje de legitimación

El test de proporcionalidad constituye una herramienta clave para la actuación policial, para conocer si la intervención sobre los datos personales está justificada. Este test se compone de tres etapas interrelacionadas, que siguen a continuación:

- Idoneidad o adecuación: permite determinar si la medida de obtención o tratamiento de datos personales es apta para alcanzar el objetivo legítimo de prevención, investigación o persecución del delito.
- Necesidad: exige verificar que no existan medios menos lesivos para alcanzar el mismo fin de protección social.
- Proporcionalidad en sentido estricto: impone examinar el equilibrio entre la gravedad de la restricción y la importancia del interés público perseguido.

Este test no constituye una formalidad procesal, sino un filtro sustantivo de carácter garantista que obliga a justificar, caso por caso, toda medida restrictiva del derecho a la privacidad. En consecuencia, solo pueden considerarse legítimas las medidas que superen el umbral de razonabilidad democrática.

Desafíos y oportunidades en la aplicación de la inteligencia estratégica antidelincuencial

Complejidad sociopolítica y legitimidad del accionar policial

La realidad ecuatoriana enfrenta el desafío de armonizar un aparato de inteligencia históricamente orientado a la eficiencia operativa con las exigencias normativas de transparencia y respeto de los derechos fundamentales (Moreano y Noboa, 2018). La transición hacia un modelo de seguridad ciudadana exige repensar las culturas organizacionales de la Policía Nacional e incorporar mecanismos de rendición de cuentas, auditoría interna y control judicial.

Por otra parte, la percepción pública de la peligrosidad delictiva puede presionar a los operadores institucionales para maximizar la obtención de información bajo criterios de urgencia, lo que tiende a subestimar los riesgos de vulneración a la privacidad. Este fenómeno evidencia la necesidad de renovar la formación de los agentes de la Policía con énfasis en ética profesional, derechos humanos y protección de datos, a fin de sentar las bases para una gestión más responsable y legítima (Noboa y Moreano, 2019).

Gobernanza de la seguridad y gestión de riesgos informativos

En relación con los paradigmas contemporáneos de gobernanza de la seguridad, el enfoque de riesgos sustituye a la lógica clásica de amenaza. La gestión de riesgos informativos exige delimitar con precisión los alcances y las limitaciones de obtener y almacenar datos personales en la inteligencia antidelincuencial. Es imprescindible adoptar protocolos que garanticen el cumplimiento de los principios de minimización, exactitud y temporalidad en el tratamiento de la información.

Estos protocolos deben privilegiar la obtención exclusiva de datos para cumplir los fines constitucionales en materia de seguridad ciudadana.

El diseño institucional debe asegurar que instancias y mecanismos independientes auditen los flujos de datos gestionados por los organismos de inteligencia y verifiquen la existencia de salvaguardas efectivas frente a potenciales abusos. La obligación de documentar operaciones y decisiones relativas a recoger y analizar datos personales constituye un componente de la Administración de justicia, del control jurídico y del fortalecimiento de la confianza ciudadana.

Casuística y proyecciones: aplicación del test de proporcionalidad

Escenarios típicos de tensión: del monitoreo a la intervención

Los escenarios de intervención de los organismos que componen el Sistema Nacional de Inteligencia suelen ubicarse en un espectro que va desde el monitoreo discreto de personas hasta el despliegue de operaciones encubiertas y recolección masiva de datos. En cada caso, el operador debe documentar y justificar la pertinencia de la medida, así como someterla a los tres niveles del test de proporcionalidad.

En un caso de monitoreo preventivo, por ejemplo, la vigilancia de espacios públicos, acompañada de la captación incidental de imágenes o datos personales solo puede considerarse legítima si se demuestra que la medida es idónea para prevenir la comisión de delitos, que no existe método menos invasivo —como el patrullaje físico— y que el interés en la seguridad pública prevalece sobre la afectación puntual de la privacidad (Noboa y Moreano, 2018).

La interceptación exige un estándar de justificación aún más riguroso en el ámbito de las comunicaciones. Esta medida solo puede admitirse bajo una orden judicial expresa y después de constatar que obtener datos resulta imprescindible ante la ineficacia de técnicas alternativas menos lesivas. En este supuesto, el test de proporcionalidad exige una ponderación entre la gravedad del delito investigado y la intensidad de la restricción del derecho a la privacidad.

Recomendaciones para la consolidación de buenas prácticas

La aplicación sistemática del test de proporcionalidad debe institucionalizarse como práctica ordinaria dentro de las unidades de inteligencia estratégica antidelincuencial de la Policía Nacional. Para ello se requiere lo siguiente:

- Implementar procesos de capacitación continua sobre normas de protección de datos y criterios probatorios de proporcionalidad.
- Adoptar protocolos estandarizados para justificar la recolección, el tratamiento y la gestión de datos personales en operaciones de inteligencia.
- Establecer mecanismos de supervisión y control, incluidas la auditoría interna y la revisión judicial de las medidas restrictivas de derechos, y
- Fomentar una cultura de rendición de cuentas que permita a la sociedad conocer el alcance, los límites y las garantías aplicables a la intervención policial en materia de protección de datos personales.

Estas recomendaciones se alinean con la política editorial orientada al fortalecimiento de la investigación policial en Ecuador, pues promueven la reflexión teórica, el rigor metodológico y la protección efectiva de los derechos fundamentales.

Resultados

Los resultados muestran que la relación entre seguridad integral y protección de datos personales no debe entenderse como una confrontación entre intereses opuestos. La inteligencia estratégica antidelincuencial puede contribuir a prevenir el delito, sin embargo, su empleo debe sujetarse a reglas claras que protejan a las personas frente a posibles abusos. Por ello, la seguridad no

justifica cualquier tratamiento de datos, sino únicamente aquel que corresponda a una finalidad concreta, que sea necesaria y respete los derechos fundamentales.

Asimismo, los principales riesgos surgen cuando la información personal se utiliza de manera amplia, indefinida o sin controles suficientes. Esto puede ocurrir en prácticas como el tratamiento masivo de datos, el perfilamiento injustificado, el cruce de bases de información, el monitoreo permanente o la vigilancia desproporcionada. Frente a estos riesgos, toda medida de inteligencia debe responder preguntas básicas: qué datos se utilizarán, a quiénes corresponden, cuánto tiempo se conservarán, qué controles se aplicarán, bajo qué criterios de riesgo se procesarán y qué mecanismos de supervisión garantizarán su uso legítimo.

Finalmente, el test de proporcionalidad se presenta como una herramienta útil para ordenar y controlar el tratamiento de datos personales en actividades de inteligencia antidelincuencial. Su aplicación permite verificar si la medida es idónea para prevenir delitos, si resulta estrictamente necesaria y si mantiene un equilibrio razonable entre la seguridad pública y la protección de los derechos de las personas.

En este sentido, la inteligencia estratégica antidelincuencial puede ser compatible con la ley de protección de datos, siempre que incorpore salvaguardas como el control de accesos, la trazabilidad, la conservación limitada de la información, la supervisión institucional y la rendición de cuentas.

Discusión

El test de proporcionalidad permite analizar con mayor claridad cuándo el uso de datos personales en la inteligencia estratégica antidelincuencial es legítimo y cuándo puede convertirse en una actuación excesiva del Estado. Cuando una medida se plantea de forma amplia —por ejemplo, el monitoreo masivo sin una hipótesis concreta de riesgo o amenaza— su justificación pierde fuerza, porque puede afectar a personas que no tienen relación directa con un hecho delictivo y porque podrían existir alternativas menos invasivas, como la focalización, la anonimización, la segmentación de datos o las auditorías posteriores.

En cambio, cuando la inteligencia estratégica se aplica en el marco de una investigación específica, con base legal, finalidad clara y controles institucionales, el tratamiento de los datos personales puede considerarse válido. Para concretar esta posibilidad, debe explicarse qué información se usa, por qué es necesaria, quién puede acceder a ella, durante cuánto tiempo se conserva y qué mecanismos existen para evitar abusos.

En el contexto ecuatoriano, este análisis exige no solo cumplir la ley, sino también fortalecer la confianza ciudadana mediante reglas claras, trazabilidad, supervisión y rendición de cuentas. Desde esta perspectiva, la protección de datos no debilita la seguridad integral, por el contrario, contribuye a construir una inteligencia más responsable, eficaz y respetuosa de los derechos fundamentales.

Conclusiones

La inteligencia estratégica antidelincuencial constituye un componente relevante de la seguridad integral del Estado, en la medida en que permite anticipar riesgos, prevenir delitos y responder oportunamente a amenazas concretas. No obstante, su legitimidad depende de que su aplicación se mantenga estrictamente subordinada al respeto de los derechos fundamentales y a los límites establecidos por la Ley Orgánica de Protección de Datos Personales.

El tratamiento de los datos personales por parte de las entidades de seguridad e inteligencia solo resulta jurídicamente válido cuando se sustenta en una finalidad legítima, una base constitucional y legal suficiente, y mecanismos de control orientados a prevenir abusos. La recopilación, el uso y el almacenamiento de información deben ser necesarios, proporcionales y verificables. Se deben evitar prácticas indiscriminadas que puedan derivar en vigilancia generalizada o en afectaciones indebidas a la privacidad y la dignidad de las personas.

El test de proporcionalidad se consolida como una herramienta jurídica esencial para evaluar la legitimidad del uso de datos personales en la inteligencia antidelincuencial, pues permite verificar que las medidas adoptadas sean idóneas, necesarias y proporcionales. Su aplicación sistemática contribuye a prevenir riesgos asociados al tratamiento masivo de información, al perfilamiento injustificado y a la vigilancia desproporcionada. De este modo, se garantiza que la seguridad pública no se convierta en un pretexto para vulnerar derechos fundamentales.

Bibliografía

Bueno de Mata, F., Cabezudo, M., Dalia, G., Fontestad, L., Guerrero, S., Jiménez, M., *et al*. (2022). *El uso de las TICs en la cooperación jurídica penal internacional*. Tirant lo Blanch. https://doi.org/10.69592/978-84-1359-690-7

Fuentes, I. (2019). Datos personales al servicio de la investigación y detección de infracciones penales. *Revista General de Derecho Procesal*, *(48)*, 1–41. https://www.semanticscholar.org/paper/a3bf438431edfc16bae5094e0a04b235e656f6e1

Gaibor, D. (2025). Los datos biométricos como objeto de protección en el ámbito laboral en el Ecuador. *Ciencia Latina Revista Científica Multidisciplinar, 9*(4), 3698–3717. https://doi.org/10.37811/cl_rcm.v9i4.19021

Llamas, J. (2025). Cybersecurity in Mexico: An In-Depth Analysis of a Fragmented Regulatory Landscape. *Mexican Law Review, 18*(1), 69–115. https://doi.org/10.22201/iij.24485306e.2025.1.19686

Maldonado-Meléndez, M. (2024). El tránsito de la Administración digital hacia una Administración pública algorítmica en la era de la inteligencia artificial: la necesidad de un ordenamiento jurídico constitucional y legal garantista en la prestación de servicios públicos en el Perú. *Revista de Derecho Político*, *(120)*, 395-425. https://doi.org/10.5944/rdp.120.2024.41775

Moreano, H., y Noboa, M. (2018*).* La inteligencia para la seguridad vecinal de Ecuador. Ecuador: Un desafío en tiempos posnormales. *Opera*, (23), 97-114. https://doi.org/10.18601/16578651.n23.07

Noboa, M., y Moreano, H. (2019). Inteligencia, anti-diplomacia y vigilancia líquida. *Athenea Digital*, 19(1), e2200. https://doi.org/10.5565/rev/athenea.2200

Quiñonez, W., y Salavarria, P. (2025). Protección de datos y propiedad intelectual en el uso de la inteligencia artificial en la educación superior. *Ciencia Latina Revista Científica Multidisciplinar*, *9*(6), 10441–10462. https://doi.org/10.37811/cl_rcm.v9i6.22199

Sánchez, M. (2024). Fuentes de información y perfiles de riesgos en el ámbito de la administración tributaria electrónica. El derecho de acceso a la información por parte del obligado tributario. *Crónica Tributaria*, *(4)*, 5. https://doi.org/10.47092/ct.24.4.5

Vallés, L. (2013). *La policía judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal* [Tesis doctoral, Universidad Nacional de Educación a Distancia]. https://www.semanticscholar.org/paper/f910eaf5b3fe0a8fadbf26990f7c00f3544678c4