Verdad y Derecho
Revista Arbitrada de Ciencias Jurídicas y Sociales
Vol. 5(especial4), 13-23, 2026
DOI: https://doi.org/10.62574/dm3arb95

Interceptaciones telefónicas y vigilancia digital: límites constitucionales y control judicial en Ecuador

Telephone interception and digital surveillance: Constitutional limits and judicial control in Ecuador

Brandon Paul Adriano-Caiza
ur.brandonac62@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Chimborazo, Ecuador
https://orcid.org/0000-0002-5510-6019

Melany Liliana Paguay-Llamuca
melanypl45@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Chimborazo, Ecuador
https://orcid.org/0009-0005-8159-3630

Kevin Alexander Novillo-Nieto
kevinnn55@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Chimborazo, Ecuador
https://orcid.org/0009-0003-6643-7862

RESUMEN

El artículo analizó los límites constitucionales y el control judicial de las interceptaciones de comunicaciones en Ecuador, a partir de la Sentencia 77-16-IN/22 de la Corte Constitucional. Un estudio cualitativo, documental, jurisprudencial y comparado examinó la Constitución, el Código Orgánico Integral Penal, la Ley Orgánica de Telecomunicaciones, la Ley de Seguridad Pública y del Estado, la Ley Orgánica de Protección de Datos Personales, estándares interamericanos y europeos y doctrina arbitrada. La Corte mantuvo la interceptación como técnica de investigación, pero exigió autorización judicial motivada con análisis de idoneidad, necesidad y proporcionalidad, y la eliminación de la información irrelevante. Persisten, sin embargo, riesgos: la interceptación por servicios de inteligencia carece de garantías equivalentes y la vigilancia de metadatos y comunicaciones digitales no tiene una regulación específica. Se concluye que la protección de la intimidad exige extender el control judicial a todas las formas de vigilancia.
Descriptores: intimidad; vigilancia; control judicial. (Fuente: Tesauro UNESCO).

ABSTRACT

The article analysed the constitutional limits and judicial control of communications interception in Ecuador, based on Judgment 77-16-IN/22 of the Constitutional Court. A qualitative, documentary, case-law and comparative study examined the Constitution, the Comprehensive Organic Criminal Code, the Organic Telecommunications Law, the Public and State Security Law, the Organic Law on Personal Data Protection, Inter-American and European standards and peer-reviewed doctrine. The Court upheld interception as an investigative technique but required a reasoned judicial authorisation assessing suitability, necessity and proportionality, and the deletion of irrelevant information. Risks nevertheless remain: interception by intelligence services lacks equivalent safeguards, and the surveillance of metadata and digital communications has no specific regulation. It is concluded that protecting privacy requires extending judicial control to all forms of surveillance.
Descriptors: privacy; surveillance; judicial review. (Source: UNESCO Thesaurus).

Recibido: 02/09/2026. Revisado: 04/09/2026. Aprobado: 04/10/2026. Publicado: 20/10/2026.
Sección artículos de investigación

INTRODUCCIÓN

La interceptación de comunicaciones es una de las técnicas de investigación más eficaces frente a la delincuencia organizada, pero también una de las más intrusivas para los derechos fundamentales. Hoy no se limita a las llamadas telefónicas: incluye correos electrónicos, mensajería instantánea, redes sociales y metadatos que permiten reconstruir los hábitos, las relaciones y los desplazamientos de una persona. El reto del derecho es permitir su uso para investigar delitos graves sin convertirlo en un instrumento de vigilancia generalizada.

La Constitución reconoce el derecho a la intimidad personal y familiar y el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual, que no puede ser retenida, abierta ni examinada salvo en los casos previstos en la ley, previa intervención judicial (Asamblea Constituyente, 2008, art. 66.20 y 21). La Corte Interamericana de Derechos Humanos ha sostenido que las conversaciones telefónicas están protegidas por el derecho a la vida privada y que su interceptación debe estar prevista en la ley, perseguir un fin legítimo y ser idónea, necesaria y proporcional (Corte Interamericana de Derechos Humanos, 2009).

En Ecuador, la Corte Constitucional examinó estas cuestiones en la Sentencia 77-16-IN/22, en la que analizó la constitucionalidad del artículo 476 del Código Orgánico Integral Penal (COIP) y del reglamento de la Fiscalía General del Estado sobre el subsistema de interceptación. El objetivo del artículo es analizar los límites constitucionales y el control judicial de las interceptaciones y de la vigilancia digital en Ecuador, a partir de esa sentencia, del marco normativo y de la experiencia comparada.

MARCO REFERENCIAL TEÓRICO

La intimidad y el secreto de las comunicaciones

La doctrina norteamericana de la expectativa razonable de intimidad, desarrollada a partir de la jurisprudencia de la Corte Suprema de los Estados Unidos, ha sido adoptada por otros sistemas para determinar cuándo una medida de investigación afecta la intimidad y requiere control judicial (Guerrero Peralta, 2011). En España, ante la ausencia prolongada de una ley que desarrollara el secreto de las comunicaciones, fueron los tribunales los que construyeron caso por caso sus garantías (Ridaura Martínez, 2017), hasta la reforma procesal de 2015, que reguló la interceptación con base en los principios de legalidad y proporcionalidad (Varona Jiménez, 2020).

La interceptación de comunicaciones electrónicas plantea problemas propios, porque el volumen de datos y la facilidad de almacenarlos multiplican el riesgo de intromisión (Zoco Zabala, 2011). Además, ciertas comunicaciones gozan de una protección reforzada. La comunicación entre el abogado y su cliente forma parte del derecho de defensa, por lo que su interceptación solo es admisible en supuestos excepcionales y bajo un estricto juicio de proporcionalidad (López-Barajas Perea, 2010), aunque el secreto profesional no puede servir para encubrir la comisión de delitos (Perdomo Torres y Guerrero Osorio, 2025).

Seguridad pública, inteligencia y vigilancia masiva

La doctrina distingue entre la interceptación con fines de investigación penal, dirigida a esclarecer delitos bajo control judicial y con fines probatorios, y la que realizan los servicios de inteligencia para proteger la seguridad nacional, que recopila información sin un proceso penal en curso y suele estar sometida a controles más débiles (Alfonso Rodríguez, 2024).

El Tribunal Europeo de Derechos Humanos, en el caso Big Brother Watch contra el Reino Unido, consideró que la falta de supervisión adecuada de la interceptación masiva vulneraba el derecho a la vida privada y la libertad de prensa (Seefeldt Pessoa y Santos de Oliveira, 2019), y el Tribunal de Justicia de la Unión Europea, en el caso Schrems, anuló el régimen de transferencia de datos a los Estados Unidos por la falta de garantías frente a la vigilancia (Puerto y Sferrazza Taibi, 2017). La inteligencia artificial amplía aún más la capacidad de vigilancia y exige salvaguardas éticas y normativas (Iturmendi Rubia, 2024).

MÉTODO

Se realizó un estudio cualitativo, con enfoque documental, jurisprudencial y comparado. La unidad central de análisis fue la Sentencia 77-16-IN/22 de la Corte Constitucional del Ecuador. El análisis normativo comprendió la Constitución, el COIP, la Ley Orgánica de Telecomunicaciones, la Ley de Seguridad Pública y del Estado, la Ley Orgánica de Protección de Datos Personales, la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos.

La comparación se centró en los estándares de la Corte Interamericana y del Tribunal Europeo de Derechos Humanos y en la experiencia de España y Colombia. La doctrina se obtuvo de revistas arbitradas registradas en el Directory of Open Access Journals (DOAJ), con búsquedas como «interceptación de comunicaciones» y «vigilancia masiva privacidad». Se aplicaron los métodos analítico-sintético, hermenéutico e histórico-lógico.

RESULTADOS

El marco normativo ecuatoriano

El COIP regula la interceptación de comunicaciones o datos informáticos como técnica especial de investigación. Debe ser ordenada por el juez de garantías penales, a solicitud motivada del fiscal, cuando existan indicios relevantes para la investigación; su duración inicial es de noventa días, prorrogable por una sola vez en casos de delincuencia organizada; y se prohíbe interceptar las comunicaciones protegidas por el secreto profesional y religioso (Asamblea Nacional, 2014, art. 476). La Ley Orgánica de Telecomunicaciones dispone que los prestadores de servicios solo pueden facilitar la interceptación con orden judicial y deben cooperar con la Fiscalía (Asamblea Nacional, 2015, art. 77). La Ley Orgánica de Protección de Datos Personales impone a los responsables del tratamiento deberes de seguridad y confidencialidad y reconoce a los titulares derechos como la supresión de sus datos (Asamblea Nacional, 2021).

La Ley de Seguridad Pública y del Estado, en cambio, regula la actividad de los organismos de inteligencia, que pueden solicitar la interceptación como parte de operaciones encubiertas para proteger la seguridad del Estado, sin que exista necesariamente un proceso penal en curso (Asamblea Nacional, 2009). La doctrina nacional ha advertido que Ecuador carece de una legislación general que proteja de forma integral la privacidad frente a la vigilancia (Sarmiento Vallejo, 2022).

La Sentencia 77-16-IN/22

En la Sentencia 77-16-IN/22, de 27 de enero de 2022, la Corte Constitucional examinó la acción de inconstitucionalidad contra el artículo 476 del COIP y varias disposiciones del reglamento del subsistema de

interceptación de la Fiscalía. Los accionantes alegaban que el reglamento restringía derechos más allá de lo permitido y otorgaba a la Fiscalía una discrecionalidad excesiva. La Corte aplicó un test de proporcionalidad y concluyó que la interceptación es una medida idónea para investigar delitos graves, pero que su regulación debía precisarse (Corte Constitucional del Ecuador, 2022). La Tabla 1 resume la decisión.

Tabla 1. *Decisión de la Sentencia 77-16-IN/22 sobre la interceptación de comunicaciones.*

Disposición	Decisión	Efecto
COIP, art. 476, inciso primero	Constitucionalidad aditiva	La autorización judicial debe justificar la necesidad de la medida, además de su idoneidad y proporcionalidad
COIP, art. 476, inciso sexto	Constitucionalidad aditiva	La información irrelevante para la investigación debe eliminarse, con constancia en el expediente
Reglamento de la Fiscalía, art. 2	Constitucionalidad aditiva	Se precisa el ámbito de los delitos en que procede la interceptación
Reglamento de la Fiscalía, arts. 8 y 9	Constitucionalidad condicionada	Se limita la discrecionalidad del fiscal en la gestión de la información
Reglamento de la Fiscalía, arts. 5 y 7	Constitucionalidad	Se mantienen las reglas sobre el funcionamiento del subsistema

Nota. Elaboración propia a partir de Corte Constitucional del Ecuador (2022).

Como consecuencia, el control judicial de la interceptación se refuerza en tres momentos: antes, porque el juez debe autorizarla mediante auto motivado que justifique la existencia de indicios relevantes y la idoneidad, necesidad y proporcionalidad de la medida; durante, porque su duración está limitada; y después, porque la información irrelevante debe eliminarse. La Fiscalía expidió en 2022 una regulación sobre la eliminación de la información obtenida mediante interceptaciones.

Los vacíos pendientes

El análisis permite identificar tres vacíos. El primero es la asimetría entre la interceptación penal y la de inteligencia: mientras la primera está sometida a un control judicial reforzado, la segunda carece de parámetros equivalentes de idoneidad, necesidad y proporcionalidad y de un control independiente

(Alfonso Rodríguez, 2024; Sarmiento Vallejo, 2022). El segundo es la vigilancia de metadatos y comunicaciones digitales, que no tiene una regulación específica sobre su conservación, acceso y eliminación. El tercero es la ausencia de mecanismos de notificación posterior a las personas afectadas, que les permitan conocer la intromisión una vez concluida la investigación e impugnarla.

DISCUSIÓN

Los resultados muestran que la Sentencia 77-16-IN/22 alineó la regulación ecuatoriana de la interceptación penal con los estándares interamericanos. La exigencia de justificar la necesidad de la medida responde al criterio de que la interceptación solo es legítima cuando no existen medios menos lesivos para obtener la información (Corte Interamericana de Derechos Humanos, 2009), y la eliminación de la información irrelevante limita el riesgo de que la intromisión se extienda más allá de lo necesario. Estas garantías coinciden con las que el legislador español incorporó en 2015 tras años de desarrollo jurisprudencial (Varona Jiménez, 2020; Ridaura Martínez, 2017).

El control judicial previo es la garantía central. La experiencia colombiana muestra que incluso las actuaciones investigativas que no requieren autorización previa deben someterse a un control judicial posterior para evitar abusos (Ramírez Carvajal y Paniagua Galeano, 2024), y el régimen disciplinario de los funcionarios es un complemento necesario frente a las interceptaciones ilegales (Velásquez Arango et al., 2011). En Ecuador, la eficacia de este control depende de que los jueces examinen realmente la motivación de la solicitud y no se limiten a validarla formalmente.

El vacío más grave se encuentra en la actividad de inteligencia. La jurisprudencia europea ha mostrado que la vigilancia sin supervisión

independiente vulnera el derecho a la vida privada aunque persiga fines legítimos de seguridad (Seefeldt Pessoa y Santos de Oliveira, 2019). Por ello, la Ley de Seguridad Pública y del Estado debería reformarse para exigir autorización judicial o de un órgano independiente, limitar la duración de la medida, establecer reglas de conservación y eliminación de la información y prever un control posterior.

La vigilancia digital plantea, además, desafíos que la regulación telefónica no resuelve. Los metadatos revelan información tan sensible como el contenido de las comunicaciones, y su acceso masivo, sumado a las herramientas de inteligencia artificial, permite elaborar perfiles detallados de las personas (Iturmendi Rubia, 2024). La Ley Orgánica de Protección de Datos Personales ofrece una base, pero se requiere una regulación específica del acceso de las autoridades a los datos de comunicaciones, con control judicial y criterios de proporcionalidad.

La regla de exclusión probatoria es la consecuencia procesal de estas garantías. El COIP establece que toda prueba o elemento de convicción obtenido con violación de los derechos constitucionales o de los instrumentos internacionales carece de eficacia probatoria (Asamblea Nacional, 2014, art. 454.6). Una interceptación sin autorización judicial, o autorizada sin la motivación exigida por la Corte, debe ser excluida, al igual que la prueba derivada de ella. La eficacia de esta regla depende, sin embargo, de que la defensa pueda conocer el auto de autorización y la forma en que se ejecutó la medida, lo que refuerza la necesidad de una notificación posterior y del acceso a la cadena de custodia de la información.

Finalmente, la cooperación con los prestadores de servicios de telecomunicaciones plantea un riesgo adicional. La ley les obliga a cooperar

con la Fiscalía cuando existe orden judicial, pero el acceso técnico a las redes y a los datos de los usuarios exige controles que impidan intervenciones no autorizadas. Los registros de las solicitudes atendidas, la auditoría independiente de los sistemas de interceptación y la sanción disciplinaria y penal de las interceptaciones ilegales son garantías complementarias del control judicial (Velásquez Arango et al., 2011).

El estudio tiene limitaciones. Se basó en el análisis de una sentencia y del marco normativo, sin examinar autos de autorización de interceptaciones ni datos sobre su número y resultados. Futuras investigaciones deberían analizar la práctica judicial de autorización y la aplicación de la regulación sobre eliminación de la información.

CONCLUSIONES

La Sentencia 77-16-IN/22 mantuvo la interceptación de comunicaciones como técnica de investigación penal, pero reforzó su control judicial al exigir una autorización motivada que justifique la idoneidad, la necesidad y la proporcionalidad de la medida, y al ordenar la eliminación de la información irrelevante. Con ello, la regulación penal ecuatoriana se aproximó a los estándares interamericanos y comparados.

Persisten, sin embargo, vacíos en la interceptación realizada por los servicios de inteligencia, que carece de garantías equivalentes, y en la vigilancia de metadatos y comunicaciones digitales. Se concluye que la protección efectiva de la intimidad exige extender el control judicial o independiente a todas las formas de vigilancia, regular el acceso a los datos de comunicaciones y prever la notificación posterior a las personas afectadas.

FINANCIAMIENTO

No monetario.

CONFLICTO DE INTERÉS

No existe conflicto de interés con personas o instituciones ligadas a la investigación.

AGRADECIMIENTOS

A la Universidad Regional Autónoma de los Andes (UNIANDES), por el apoyo brindado al desarrollo de esta investigación.

REFERENCIAS

Alfonso Rodríguez, A. J. (2024). Interceptación de comunicaciones telefónicas, seguridad(es) y garantías procesales [Telephone interception, security and procedural guarantees]. *Ciencia Policial*, (182), 97-144. https://doi.org/10.14201/cp.31812

Asamblea Constituyente. (2008). *Constitución de la República del Ecuador* [Constitution of the Republic of Ecuador]. Registro Oficial 449, 20 de octubre de 2008.

Asamblea Nacional. (2009). *Ley de Seguridad Pública y del Estado* [Public and State Security Law]. Registro Oficial Suplemento 35, 28 de septiembre de 2009.

Asamblea Nacional. (2014). *Código Orgánico Integral Penal* [Comprehensive Organic Criminal Code]. Registro Oficial Suplemento 180, 10 de febrero de 2014.

Asamblea Nacional. (2015). *Ley Orgánica de Telecomunicaciones* [Organic Telecommunications Law]. Registro Oficial Tercer Suplemento 439, 18 de febrero de 2015.

Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales* [Organic Law on Personal Data Protection]. Registro Oficial Quinto Suplemento 459, 26 de mayo de 2021.

Corte Constitucional del Ecuador. (2022). *Sentencia 77-16-IN/22* [Judgment 77-16-IN/22]. Juez ponente: Enrique Herrería Bonnet, 27 de enero de 2022.

Corte Interamericana de Derechos Humanos. (2009). *Caso Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009 (excepciones preliminares, fondo, reparaciones y costas)* [Escher et al. v. Brazil].

Guerrero Peralta, Ó. J. (2011). La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal [The reasonable expectation of privacy in criminal proceedings]. *Derecho Penal y Criminología, 32*(92).

Iturmendi Rubia, J. M. (2024). Inteligencia artificial y derechos humanos: desafíos y oportunidades en la era digital. Introducción al monográfico [Artificial intelligence and human rights]. *Deusto Journal of Human Rights*, (14). https://doi.org/10.18543/djhr.3202

López-Barajas Perea, I. (2010). La postulación y los derechos a la tutela y de defensa [Legal representation and the rights to judicial protection and defence]. *Revista de Derecho Político*, (79). https://doi.org/10.5944/rdp.79.2010.9131

Perdomo Torres, J. F., y Guerrero Osorio, C. F. (2025). ¿Es el secreto profesional del abogado una autorización para delinquir? [Is lawyer-client privilege a licence to commit crimes?]. *Via Inveniendi et Iudicandi, 20*(2). https://doi.org/10.15332/19090528.11588

Puerto, M. I., y Sferrazza Taibi, P. (2017). La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional [The Schrems judgment of the CJEU]. *Revista Derecho del Estado*, (40). https://doi.org/10.18601/01229893.n40.09

Ramírez Carvajal, D. M., y Paniagua Galeano, A. (2024). El juez de control de garantías y la reserva judicial en actuaciones que no requieren autorización previa [The guarantee judge and judicial reserve in measures not requiring prior authorisation]. *Revista Criminalidad, 66*(1). https://doi.org/10.47741/17943108.565

Ridaura Martínez, M. J. (2017). El legislador ausente del artículo 18.3 de la Constitución [The absent legislator of article 18.3 of the Spanish Constitution]. *Revista de Derecho Político*, (100), 347-404. https://doi.org/10.5944/rdp.100.2017.20702

Sarmiento Vallejo, G. H. (2022). Sitio web del derecho a la privacidad y a la intimidad en el contexto de la interceptación de las comunicaciones en el Ecuador [Privacy in the context of communications interception in Ecuador]. *Serie Científica de la Universidad de las Ciencias Informáticas, 15*(7), 242-261.

Seefeldt Pessoa, J. P., y Santos de Oliveira, R. (2019). «Big Brother Watch and Others v. The United Kingdom» [The ECtHR ruling on mass surveillance]. *Pensar, 24*(3), 1-12. https://doi.org/10.5020/2317-2150.2019.9528

Varona Jiménez, A. (2020). Aspectos relevantes de la interceptación de las comunicaciones telefónicas en el proceso penal español [Telephone interception in Spanish criminal proceedings]. *Ius Inkarri, 9*(9), 237-258. https://doi.org/10.31381/iusinkarri.v9n9.3687

Velásquez Arango, E. A., Otálvaro Ochoa, P. C., y Londoño Grajales, N. A. (2011). El derecho disciplinario frente a la interceptación de comunicaciones en Colombia [Disciplinary law and communications interception in Colombia]. *Nuevo Derecho, 6*(8). https://doi.org/10.25057/2500672X.697

Zoco Zabala, C. (2011). Interceptación de las comunicaciones electrónicas [Interception of electronic communications]. *InDret*.

Derechos de autor: 2026 Por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0)
https://creativecommons.org/licenses/by-nc-sa/4.0/