CÁMARA DE DIPUTADOS
ÁREA DE TRÁMITE DOCUMENTARIO
RECIBIDO
PROPOSICIÓN LEGISLATIVA
00921-2026-2031-CD
RU 73473-CD
23 NOVIEMBRE 2026 04:37 p. m.
FIRMADO DIGITALMENTE: ASABARIAN

PROPOSICIÓN LEGISLATIVA QUE DEFINE, DESARROLLA Y REGULA EL MONITOREO DE COMUNICACIONES Y LOS DATOS DERIVADOS DE ESTAS, PREVISTO EN EL NUMERAL 1 DEL ARTÍCULO 230 DEL CÓDIGO PROCESAL PENAL

El grupo parlamentario **AHORA NACIÓN**, a iniciativa del Diputado de la República que suscribe, **HARVEY JULIO COLCHADO HUAMANÍ**, en ejercicio de la atribución que le confiere el artículo 107 de la Constitución Política del Perú y los artículos 98 y 107 del Reglamento de la Cámara de Diputados, presentan la siguiente **PROPOSICIÓN LEGISLATIVA**:

FÓRMULA LEGAL

LEY QUE DEFINE, DESARROLLA Y REGULA EL MONITOREO DE COMUNICACIONES Y LOS DATOS DERIVADOS DE ESTAS, PREVISTO EN EL NUMERAL 1 DEL ARTÍCULO 230 DEL CÓDIGO PROCESAL PENAL

Artículo 1.- Objeto de la ley

La presente proposición legislativa tiene por objeto definir y desarrollar el término monitoreo previsto en el numeral 1 del artículo 230 del Código Procesal Penal, y establecer las reglas para su autorización, ejecución y garantías que la rigen.

Artículo 2.- Finalidad

La presente ley tiene por finalidad garantizar que el monitoreo se ejecute con sujeción estricta al mandato judicial previo, escrito y motivado, y con pleno respeto a los derechos fundamentales en el marco de lo dispuesto en el numeral 10 del artículo 2 de la Constitución Política del Perú, asegurando la legalidad y eficacia de la investigación penal frente a las comunicaciones y los datos cuyo acceso no es posible mediante otras técnicas de investigación, incorporando a la regulación de la medida los avances tecnológicos en materia de telecomunicaciones e informática. El sistema y la capacidad técnica que hacen posible el monitoreo se destinan de manera exclusiva a su ejecución por mandato judicial dentro del proceso penal. No se habilitan, operan ni ponen al servicio de finalidades ajenas a aquel.

Artículo 3.- Definiciones

Para los efectos de la presente ley, se entiende por:

3.1. **Equipo.** Todo sistema informático utilizado por el investigado, cualquiera sea su forma o tecnología, tales como, de manera enunciativa y no limitativa, las computadoras personales, fijas o portátiles, los teléfonos móviles, las tabletas y los equipos equiparables, presentes o futuros.
3.2. **Acceso.** El ingreso o la conexión al equipo mediante cualquier técnica, programa, código, instrumento o procedimiento, presente o futuro.

3.3. **Comunicación en curso.** La comunicación cuyo proceso de transmisión se produce durante la ejecución de la medida, con independencia de que este se haya iniciado antes o durante dicha ejecución. Comprende las comunicaciones cursadas a través de canales de datos, servicios o aplicaciones de comunicación, incluidas las que emplean cifrado de extremo a extremo.

3.4. **Comunicaciones registradas en el equipo.** Las comunicaciones que, habiendo sido transmitidas o recibidas, permanecen registradas o almacenadas en el equipo, así como los datos derivados de estas.

3.5. **Datos derivados de las comunicaciones.** Los datos externos al contenido de la comunicación que forman parte de su proceso comunicativo o derivan de este, como el origen, el destino, la identidad de los interlocutores, la frecuencia, la hora, la duración, el servicio o la aplicación empleados, así como la localización asociada a la comunicación, entre otras equiparables.

3.6. **Ubicación en tiempo real.** La posición geográfica del equipo en el momento de su obtención, generada por este, por sus componentes o por los servicios de localización a los que accede.

3.7. **Historial de ubicaciones.** Las posiciones geográficas que permanecen registradas o almacenadas en el equipo o en las aplicaciones que este ejecuta.

3.8. **Información almacenada.** Los datos contenidos en el equipo que constituyan forma objetivada del contenido del pensamiento, sea cual fuere su formato o la aplicación que los genere.

3.9. **Servicios o plataformas en línea.** Los servicios de comunicación, correo, mensajería o almacenamiento que operan en infraestructura remota y a los que el equipo accede.

3.10. **Sistema informático y datos informáticos.** Los definidos como tales en la Novena Disposición Complementaria Final de la Ley N° 30096, Ley de Delitos Informáticos. El equipo tiene la condición de sistema informático.

3.11. **Monitoreo.** La medida prevista en el numeral 1 del artículo 230 del Código Procesal Penal que consiste en el acceso judicialmente autorizado al equipo utilizado por el investigado, a fin de captar y registrar:

a) Las comunicaciones en curso que el equipo cursa o recibe, a través de cualquier canal, servicio o aplicación, y su contenido;
b) Las comunicaciones que permanecen registradas en el equipo con su contenido;
c) Los datos derivados de las comunicaciones, en curso o registradas;
d) La información almacenada en el equipo que constituya forma objetivada del contenido del pensamiento del investigado, se haya transmitido o no, en el alcance que especifique el mandato judicial;
e) La ubicación en tiempo real del equipo y su historial de ubicaciones;
f) La visualización de lo que se muestra en la pantalla del equipo y las capturas de pantalla que permanecen registradas en este, en cuanto manifiesten comunicaciones o su contenido objetivado; y
g) La información contenida en los servicios o plataformas en línea a los que el equipo acceda, únicamente en el alcance que especifique el mandato judicial.

El monitoreo se define por su objeto y por su efecto, y se aplica sea cual fuere la técnica, el programa, el código, el sistema o el procedimiento empleados para su ejecución, presentes o futuros.

Para los efectos de la presente ley, se aplican las definiciones de comunicación y de medio previstas en el artículo 2, numerales 1 y 2, de la Ley N° 27697, Ley que otorga facultad al

Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional. En consecuencia, el equipo, en cuanto soporte en el cual se porta o se transmite la comunicación, constituye medio y tiene el mismo régimen que la comunicación misma.

Artículo 4.- Límites objetivos del monitoreo

4.1. El monitoreo no comprende la intervención de las comunicaciones en tránsito por la infraestructura de las empresas prestadoras de servicios de telecomunicaciones, cualquiera sea su naturaleza o tecnología, la cual procede por requerimiento del fiscal y según las reglas de su propio procedimiento.
4.2. La captación de audio o de video a través del micrófono o de la cámara del equipo solo está permitida durante una comunicación en curso, y se circunscribe al flujo de esa comunicación tal como es procesado por el canal, servicio o aplicación empleados, incluidas las imágenes o audios que formen parte de ella cuando esta comprenda video o envíos en mensajes. Está prohibido activar, controlar o leer de manera independiente el micrófono, la cámara u otro sensor del equipo para captar sonidos o imágenes del entorno del investigado o de terceros. Está prohibido el acceso o la activación del micrófono o de la cámara del equipo fuera de una comunicación en curso.
4.3. La captación se circunscribe al objeto autorizado en el mandato judicial y a lo relacionado con el hecho investigado. Está prohibida la captación genérica, masiva o prospectiva.

Artículo 5.- Autorización judicial

5.1. El monitoreo es autorizado por el Juez de la Investigación Preparatoria, a solicitud del Fiscal, de oficio o a requerimiento de la Policía Nacional del Perú en función de investigación. Rige lo dispuesto por el numeral 1 del artículo 230 del Código Procesal Penal.
5.2. El requerimiento se tramita y se resuelve conforme al numeral 4 del artículo 226 del Código Procesal Penal, mediante trámite reservado e inmediato. La denegatoria de la medida puede ser apelada por el Fiscal conforme a dicho numeral.
5.3. La medida puede dirigirse contra el investigado o contra las personas previstas en el numeral 2 del artículo 230 del Código Procesal Penal. El requerimiento y mandato contra dichas personas debe motivarse de manera específica considerando que el monitoreo del equipo del investigado puede ser insuficiente para los fines de la investigación.
5.4. Ante peligro inminente para la vida, la integridad o la libertad de las personas, el requerimiento se prioriza y se resuelve en el plazo más breve posible, que no excede de veinticuatro horas desde su recepción, conforme al numeral 3 del artículo 230 del Código Procesal Penal, por el juez de turno o competente y por medios electrónicos cuando sea necesario. En ningún supuesto la priorización habilita la ejecución del monitoreo antes de la resolución judicial.
5.5. Si durante la ejecución del mandato judicial de monitoreo, en tiempo real se tomara conocimiento, a través de nuevos números telefónicos, IMSI, IMEI o equipos, o por identificación de comunicaciones, sobre el peligro inminente para la vida, la integridad física de manera grave o la libertad de las personas en el marco de la comisión de cualquier delito, rige lo establecido en el numeral 5 del artículo 231 del Código Procesal Penal, siempre que el mandato judicial haya previsto y delimitado dicha eventualidad con criterios concretos. La disposición fiscal de urgencia no alcanza a equipos no comprendidos en tales criterios.

Artículo 6.- Contenido del requerimiento fiscal y del mandato judicial

6.1. El requerimiento fiscal y el mandato judicial indican:

a) El nombre y la dirección de la persona contra quien se dispone la medida, si se conociera;
b) La individualización del equipo o de los equipos objeto de la medida mediante los datos que permitan identificarlos de manera única y, cuando estos no se conozcan, mediante la información que permita determinar sus características únicas o distintivas;
c) El alcance de la medida, con indicación expresa de cuáles de los supuestos de captación previstos en el numeral 11 del artículo 3 son materia de autorización;
d) El delito investigado y los elementos de convicción que sustentan la medida;
e) La técnica, el programa, el código o el sistema autorizado para la ejecución de la medida, y su descripción;
f) La duración de la medida y su fecha de término;
g) La unidad autorizada para ejecutar la medida y la autoridad o dependencia destinataria de lo captado;
h) Las medidas de filtrado aplicables;
i) La obligación de generar el registro de la medida de monitoreo conforme lo previsto en la presente ley;
j) La periodicidad con la que se informa al Juez sobre la ejecución de la medida.

6.2. Son obligatorios los datos señalados en los literales b), c), d) y f), en concordancia con el numeral 3 del artículo 230 del Código Procesal Penal. La omisión de cualquiera de ellos determina la invalidez del mandato, y todo lo captado en virtud de él carece de efecto legal. La omisión de los demás elementos es subsanable y no acarrea invalidez, sin perjuicio de la responsabilidad funcional que corresponda.
6.3. El mandato judicial puede prever que durante la ejecución de la medida se presente la eventualidad de peligro inminente para la vida, la integridad física de manera grave o la libertad de las personas en el marco de la comisión de cualquier delito, en cuyo caso rige lo dispuesto en el numeral 5 del artículo 231 del Código Procesal Penal.

Artículo 7.- Motivación reforzada

7.1. La motivación del requerimiento fiscal y del mandato judicial debe indicar lo siguiente:

a) Por qué la captación de las comunicaciones materia de la medida no es posible de manera inteligible mediante la intervención de las comunicaciones ejecutada en la red del operador u otras técnicas de investigación, incluida, de ser el caso, la circunstancia de que estas emplean cifrado de extremo a extremo u otros mecanismos equivalentes;
b) Por qué resulta necesario el acceso al equipo determinado; y
c) Por qué cada uno de los supuestos de captación autorizados conforme al literal c) del numeral 1 del artículo 6 es idóneo y necesario para el esclarecimiento del hecho investigado, y por qué su extensión no excede de lo indispensable para ese fin.

7.2. La omisión de la motivación reforzada determina la invalidez del mandato. Lo captado en virtud de él carece de efecto legal.

Artículo 8.- Ejecución de la medida

8.1. La ejecución del monitoreo corresponde a la unidad especializada del sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú, bajo la supervisión del Fiscal. Sólo el personal autorizado en el mandato judicial accede al equipo o a lo captado, según el componente que corresponda.
8.2. Quien autoriza la medida no la ejecuta; quien configura o prepara el acceso al equipo no accede a lo captado; y quien accede a lo captado no decide su utilización. La evaluación y la decisión sobre la relevancia y la utilización de lo captado corresponden al Fiscal del caso, bajo control judicial.
8.3. La ejecución del monitoreo se organiza en dos componentes separados, conforme al modelo del sistema de intervención y control de las comunicaciones: el componente a cargo del Ministerio Público configura o prepara el acceso sin recibir lo captado, y el componente a cargo de la Policía Nacional del Perú realiza el acceso, la captación y la custodia de lo captado. La distribución y asignación de funciones entre ambos componentes se detalla en el protocolo correspondiente.
8.4. La ejecución de la medida no altera el funcionamiento, la configuración ni los mecanismos de seguridad del equipo más allá de lo estrictamente indispensable para la captación autorizada.
8.5. El sistema y la capacidad técnica empleados en el monitoreo operan únicamente para la ejecución de las medidas autorizadas judicialmente y bajo el régimen de registro y auditoría de esta ley. Su uso para cualquier otra finalidad está prohibido, así como su operación fuera del entorno autorizado para su ejecución.

Artículo 9.- Duración, prórroga, interrupción y cese

9.1. La duración del monitoreo, su prórroga y su interrupción se rigen por los numerales 5 y 6 del artículo 230 del Código Procesal Penal.
9.2. El cese de la medida se comunica al Juez y se deja constancia en el registro previsto en el artículo 11.

Artículo 10.- Pertinencia de lo captado y filtrado

10.1. El monitoreo es inadmisible cuando existan fundados motivos para prever que su ejecución obtendrá únicamente información que no guarda relación con el hecho investigado.
10.2. Durante la ejecución del monitoreo se adoptan, en la medida técnicamente posible, medidas de filtrado o de prevención que impidan captar información ajena al objeto autorizado.

Artículo 11.- Registro inalterable y auditabilidad

11.1. El sistema empleado en la ejecución del monitoreo registra, de manera íntegra y protegida contra toda alteración o supresión, las operaciones realizadas, entre ellas el inicio y el término de la medida, los accesos, las captaciones, las activaciones del micrófono, de la cámara o de la pantalla, las reproducciones, las copias, las

impresiones y la eliminación del instrumento utilizado para la ejecución del monitoreo, con identificación del personal responsable, la fecha y la hora de cada una.

11.2. El sistema asegura la integridad de lo captado mediante valores de verificación que permiten comprobar que no ha sido alterado. El instrumento empleado es susceptible de verificación técnica por un órgano independiente del que ejecuta la medida, cuyos resultados quedan a disposición del Juez y del Fiscal.

11.3. El registro está a disposición del Juez y del Fiscal. Toda consulta al registro o acción que involucre su uso queda asentada en él. El Juez puede requerir informes técnicos y disponer verificaciones sobre el funcionamiento del sistema.

11.4. El registro se conserva conforme a lo establecido en el numeral 2 del artículo 231 del Código Procesal Penal.

Artículo 12.- Actas, entrega y conservación

12.1. Lo captado se registra y asegura, se entrega directamente al Fiscal y se documenta conforme a los numerales 1 y 2 del artículo 231 del Código Procesal Penal, en lo compatible con la naturaleza de la medida.

12.2. El acta de recolección y control se suscribe por el Fiscal y por el personal de la unidad especializada encargada de la ejecución.

Artículo 13.- Reevaluación

13.1. La reevaluación de lo captado durante todo el proceso, por orden del Juez competente, y su destino, se rigen por el numeral 2 del artículo 231 del Código Procesal Penal. De descubrirse indicios de otros hechos delictivos, rige el inciso 11 del artículo 2 de la Ley N° 27697.

13.2. En el ámbito de aplicación de la Ley N° 30077, Ley contra el Crimen Organizado, rige en lo pertinente el artículo 10 de esa ley.

Artículo 14.- Reexamen judicial

14.1. Ejecutada la medida y realizadas las investigaciones relacionadas con su resultado, se pone en conocimiento del afectado todo lo actuado de acuerdo con lo establecido en el numeral 3 del artículo 231 del Código Procesal Penal y rige el reexamen judicial previsto en el numeral 4 del artículo 231 del Código Procesal Penal.

14.2. Contra la resolución que autoriza el monitoreo procede el recurso de apelación; los resultados de su ejecución se impugnan mediante el reexamen judicial. El secreto de las actuaciones requiere resolución judicial motivada y está sujeto a plazo.

Artículo 15.- Término de la medida

15.1. Producido el cese, la interrupción o el vencimiento de la medida, se procede de inmediato a:

a) Eliminar el software, el programa, el código, el agente o cualquier otro instrumento desplegado o instalado en el equipo objeto de la medida para la ejecución del monitoreo; y
b) Restaurar el funcionamiento del equipo, eliminando de este todo rastro asociado a la medida.

15.2. La eliminación y la restauración se documentan en acta suscrita por el personal autorizado y se comunican al Juez. No afectan la conservación de lo captado ni la del registro previsto en el artículo 11, conforme a la presente ley.

Artículo 16.- Inaplicabilidad de los regímenes de ejecución sin mandato previo

La ejecución del monitoreo no puede iniciarse ni mantenerse sin mandato judicial previo, escrito y motivado. No es aplicable al monitoreo ningún régimen de convalidación, confirmación o ratificación judicial posterior, con excepción del supuesto de apremio previsto en el numeral 5.5 del artículo 5 de la presente ley, que incorpora el numeral 5 del artículo 231 del Código Procesal Penal con todos sus requisitos.

Artículo 17.- Responsabilidad y eficacia de lo captado

17.1. La ejecución del monitoreo al margen de la presente ley configura, según el caso, los delitos previstos en los artículos 162, 162-A y 162-B del Código Penal, sin perjuicio de las responsabilidades funcionales y administrativas correspondientes.
17.2. La información captada en contravención de la presente ley carece de efecto legal, conforme al artículo VIII del Título Preliminar del Código Procesal Penal y al numeral 10 del artículo 2 de la Constitución Política del Perú.

Artículo 18.- Concordancias

18.1. El término monitoreo previsto en el numeral 1 del artículo 230 del Código Procesal Penal se interpreta conforme a la presente ley.
18.2. La presente ley no modifica la intervención de las comunicaciones ejecutada a través de las empresas prestadoras de servicios de telecomunicaciones, que se rige por el numeral 4 del artículo 230 del Código Procesal Penal. La unidad especializada del sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú ejecuta tanto dicha intervención como el monitoreo, cada una conforme a su propio régimen.
18.3. La presente ley no modifica el régimen de revisión de equipos informáticos previsto en el artículo 230-A del Código Procesal Penal, el cual se rige por sus propios términos. A diferencia de la presente ley que regula el acceso remoto al equipo utilizado por el investigado con mandato judicial previo, el artículo 230-A regula el acceso a la información contenida en equipos hallados o incautados con confirmación judicial posterior.
18.4. La ubicación en tiempo real y el historial de ubicaciones generados por el equipo y obtenidos mediante el acceso a este se rigen por la presente ley. El acceso a los datos de localización o geolocalización en poder de las empresas operadoras se rige por su propio régimen. A diferencia de la medida de monitoreo regulada por la presente ley, el Decreto Legislativo N° 1182 no habilita el acceso al equipo.
18.5. El acceso remoto al equipo que tenga por objeto las comunicaciones y la ubicación generada por el equipo o la visualización de la pantalla se rigen por la presente ley, al igual que los datos derivados de las comunicaciones obtenidos del equipo; los datos obtenidos de las empresas operadoras se rigen por el régimen que les es propio.
18.6. La presente ley se aplica sin perjuicio de las demás técnicas especiales de investigación previstas en el Código Procesal Penal y en la Ley 30077, Ley contra el Crimen Organizado.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Protocolos de ejecución

Dentro de los noventa (90) días hábiles siguientes a la publicación de la presente ley, el Ministerio Público y la Policía Nacional del Perú, con acuerdo del Poder Judicial, aprueban el protocolo de requerimiento, ejecución, registro, auditoría y culminación del monitoreo, que comprende la organización de los dos componentes prevista en el numeral 8.3 del artículo 8 y los estándares de integridad y de verificación técnica del instrumento empleado. El protocolo asegura que la ejecución del monitoreo opere de manera centralizada, bajo acceso único y controlado, sin habilitación de accesos distribuidos o remotos ajenos al entorno autorizado.

SEGUNDA.- Reserva y confidencialidad

Los jueces, fiscales, personal policial, peritos y demás personas que intervengan en el monitoreo están obligados a guardar reserva sobre la información a la que accedan, bajo responsabilidad penal, civil y administrativa. En lo que resulte pertinente rige el artículo 15 de la Ley N° 30077, Ley contra el Crimen Organizado.

TERCERA.- Financiamiento

La implementación de la presente ley se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

CUARTA.- Vigencia

La presente ley entra en vigencia al día siguiente de su publicación en el diario oficial El Peruano. La ejecución del monitoreo procede una vez aprobado el protocolo de ejecución.

Lima 20 de noviembre de 2026

EXPOSICIÓN DE MOTIVOS

La presente propuesta legislativa se sustenta sobre la base de los siguientes fundamentos y evidencias, conforme se desarrolla a continuación:

I. Planteamiento del problema público

En los últimos años, el Perú ha experimentado un incremento de la incidencia delictiva, acompañado de una transformación en las dinámicas y modalidades de actuación de las organizaciones criminales. Este escenario se encuentra asociado a la expansión de economías ilegales y a la diversificación de delitos que generan una elevada afectación social, entre los que destaca la extorsión. Dicho fenómeno se manifiesta a través de diversas modalidades, como el cobro de cupos a transportistas y comerciantes, las amenazas y exigencias económicas mediante canales digitales, los préstamos extorsivos bajo la modalidad del denominado "gota a gota" y su vinculación con otras expresiones de violencia criminal, como el sicariato. La magnitud de esta problemática se refleja en el incremento de las denuncias por extorsión. Según cifras del Ministerio Público, durante el 2025 se registraron 28 948 denuncias, frente a las 22 835 reportadas en 2024, lo que representa un incremento del 26,8 % en un solo año, evidenciando la expansión sostenida de este fenómeno delictivo[1].

En paralelo, las organizaciones criminales han adoptado un proceso acelerado de tecnologización de sus operaciones. La planificación, coordinación y ejecución de las conductas ilícitas han migrado de los canales de telefonía convencional o el contacto presencial hacia el uso masivo de redes sociales y plataformas de mensajería instantánea. Dado que la gran mayoría de las comunicaciones e intercambios cotidianos -incluyendo las coordinaciones extorsivas- se desarrollan actualmente en entornos digitales, la capacidad de respuesta del Estado enfrenta desafíos significativos. La persecución penal tradicional, diseñada predominantemente para esquemas de telefonía analógica o de red fija, resulta insuficiente frente a una delincuencia organizada que opera protegida por el anonimato tecnológico.

Tal es el caso del Código Procesal Penal que presenta un vacío que limita el empleo de herramientas técnicas idóneas para hacer frente a esta realidad. El numeral 1 del artículo 230 del mencionado código autoriza al Juez de la Investigación Preparatoria, a solicitud del Fiscal, "la intervención, monitoreo o grabación de comunicaciones telefónicas, radiales, internet o de otras formas de comunicación, así como los registros de los datos derivados de las comunicaciones". No obstante, la norma emplea el término monitoreo sin ofrecer una definición legal, un objeto delimitado ni un procedimiento técnico para su desarrollo, omisión que ninguna otra disposición resuelve.

[1] Ministerio Público. (2026). Reporte de delitos denunciados según distrito fiscal y tipo de delito a nivel nacional. https://app.powerbi.com/view?r=eyJrIjoiNzQ3OWE5NTAtODAxMS00NGRmLTllM2QtYWM2ZDk5MTQxNDMwIiwidCI6IjU1OGU5ZDlhLWMzZmMtNGJkOC1hZjgwLWM0MzAwZmZlZTZjNSIsImMiOjR9

Esta omisión puede acarrear consecuencias jurídicas. El monitoreo habilita una injerencia en el secreto de las comunicaciones, derecho que el numeral 10 del artículo 2 de la Constitución Política del Perú reserva al mandato motivado del juez "con las garantías previstas en la ley". El fiscal que requiere, el juez que autoriza y el personal que ejecuta trabajan sobre una palabra sin contenido formal. En síntesis, el problema tiene tres dimensiones:

1) **Inseguridad jurídica de la prueba.** Los datos o información captada al amparo de un término indefinido como el de monitoreo, queda expuesta a ser declarada sin efecto legal por aplicación del artículo VIII del Título Preliminar del Código Procesal Penal y del numeral 10 del artículo 2 de la Constitución Política del Perú. Una medida de monitoreo ejecutada hoy puede ser cuestionada en juicio dentro de tres años, cuando la defensa sostenga que "monitoreo" no autorizaba lo que se hizo por falta de amparo legal o por indicación expresa de la ley. El costo o consecuencias de una decisión sin ese respaldo, recaería sobre la investigación, con efectos adversos como la pérdida de elementos de convicción, repetición de diligencias y, en suma, procesos que se debilitan no por los hechos sino por la indeterminación de la norma que los sostuvo.

2) **Ineficacia frente a la comunicación cifrada.** Las aplicaciones de mensajería y llamadas de uso masivo cifran su contenido de extremo a extremo. El contenido viaja ilegible por la ruta de la comunicación y solo se vuelve legible en los dos extremos: el equipo que envía y el que recibe. La intervención ejecutada en la red del operador, que es el procedimiento del numeral 4 del artículo 230 del Código Procesal Penal, capta en esos casos el texto cifrado, es decir, nada utilizable. De ese modo, la persecución penal queda desigual según el canal que elija el investigado: eficaz contra quien usa telefonía tradicional, pero ciega contra quien usa cifrado. Esa desigualdad favorece precisamente a la criminalidad organizada que migró hace años a los canales cifrados, siendo la alternativa de monitoreo regulada en la presente ley una vía técnica y legal para hacerle frente.

3) **Exposición de los operadores jurídicos.** El Ministerio Público, la Policía Nacional del Perú y los jueces carecen de un parámetro normativo cierto para requerir, autorizar, ejecutar y documentar la medida. Cada decisión se adopta sobre un término sin contenido, con el riesgo funcional que ello acarrea para quien la toma.

Finalmente, el problema, entendido como la ausencia de una definición clara para el monitoreo de las comunicaciones, afecta a tres grupos: i) a los investigados, que no tienen certeza sobre los límites de la injerencia que pueden sufrir; ii) a las víctimas y a la ciudadanía, que ven cómo la eficacia de la persecución depende de la tecnología del delincuente y no de la gravedad del delito; y, iii) a las instituciones del sistema de justicia, que operan sobre una base que cualquier litigante podría cuestionar e invalidar.

II. Evidencia que sustenta el problema

El sustento de esta iniciativa es normativo, técnico y jurisprudencial. Por tanto, la evidencia es más de orden cualitativo que estadístico, lo que no implica que no sea abundante y verificable conforme se describe a continuación.

- **Evidencia normativa interna.** El numeral 1 del artículo 230 del Código Procesal Penal menciona explícitamente el término monitoreo y no lo define. Y lo mismo ocurrió con las sucesivas modificaciones a ese mismo artículo, introducidas por la Ley N° 30077, Ley Contra el Crimen Organizado, Ley N° 30096, Ley de Delitos Informáticos, su modificatoria Ley N°30171, por el Decreto Legislativo N° 1605, y la reforma del numeral 3 por el Decreto Legislativo N° 1708. En ninguna de esas reformas el legislador definió ni desarrolló el término en cuestión, lo que fluye del propio texto vigente del artículo 230 del Código Procesal Penal.

- **Evidencia técnica.** Las comunicaciones cursadas por aplicaciones con cifrado de extremo a extremo transmiten su contenido cifrado a lo largo de toda la ruta[2]. El contenido es legible únicamente en el dispositivo emisor y en el receptor. Es una característica verificable del entorno tecnológico actual, no una hipótesis. De ella se sigue una consecuencia jurídica directa: la captación inteligible de esas comunicaciones solo es posible en el extremo, es decir, en el equipo.

- **Evidencia jurisprudencial del estándar de invalidez.** La jurisprudencia nacional ha fijado con claridad la consecuencia de ejecutar una medida de intervención en las comunicaciones sin el debido amparo legal. La sentencia del Tribunal Constitucional 847/2021 del expediente N° 02324-2020-PHC/TC [3] declaró prueba ilícita la información de un correo electrónico al que se tuvo acceso antes de la autorización judicial, pese a que tal autorización llegara en fecha posterior. En ese mismo sentido, el Acuerdo Plenario N° 4-2010/CJ-116[4] ordena excluir el material probatorio obtenido con violación del contenido esencial de los derechos fundamentales. Por su parte, la Sentencia de Casación N° 1251-2019/Lambayeque[5] estableció que el incumplimiento de los requisitos constitucionales de la intervención, exclusividad jurisdiccional, motivación, intervención indiciaria, proporcionalidad y especialidad torna la intervención en constitucionalmente ilícita.

  Estas decisiones no versan sobre el monitoreo, porque el monitoreo no tiene desarrollo que litigar; versan sobre lo que ocurre cuando una intervención o injerencia en las comunicaciones se ejecuta sin el debido amparo legal. En caso se presenten pruebas bajo la figura del monitoreo en un proceso judicial, estas quedarían completamente expuestas a ser invalidadas, pues no tienen un desarrollo jurídico que las defina.

- **Evidencia de oportunidad y práctica institucional.** Existe una unidad policial especializada que gestiona el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú, prevista en el numeral 4 del artículo 230 y en el numeral 2 del artículo 231 del Código Procesal Penal, con experiencia administrativa, operativa y de cadena de custodia acreditada. Sobre esa unidad y ese sistema, recaería hoy la ejecución del monitoreo de los equipos de comunicación, lo que representa una gran oportunidad y especial potencial para fortalecer las

[2] Electronic Frontier Foundation. (s. f.). End-to-end encryption. Surveillance Self-Defense. https://ssd.eff.org/glossary/end-to-end-encryption
[3] Pleno. Sentencia 847/2021. (2021). Tribunal Constitucional. https://jurisprudencia.sedetc.gob.pe/sentencia/02324-2020-hc-847-2021
[4] Acuerdo Plenario N° 4-2010/CJ-116. (2010). Corte Suprema de Justicia de la República. https://static.legis.pe/wp-content/uploads/2018/12/Acuerdo-Plenario-4-2010-CJ-116.pdf
[5] Sentencia de Casación N° 1251-2019/Lambayeque. (2022). Corte Suprema de Justicia de la República. https://img.lpderecho.pe/wp-content/uploads/2022/07/Casacion-1251-2019-Lambayeque-LPDerecho.pdf

herramientas de lucha contra la criminalidad, siendo por eso necesario dotar el termino de definición y desarrollo legal.

III. Objetivos generales y específicos

Objetivo general:

Regular el alcance y las condiciones de aplicación del término *monitoreo* del numeral 1 del artículo 230 del Código Procesal Penal, para garantizar una herramienta de persecución penal eficaz y respetar la protección de los derechos fundamentales de las personas involucradas.

Objetivos específicos:

1) Desarrollar la medida de monitoreo, el requerimiento, autorización y ejecución de la medida de monitoreo del equipo del investigado, supuestos de invalidez y de motivación reforzada.
2) Establecer las garantías que exige la ejecución de la medida judicial de acceso al equipo del investigado, en resguardo de sus derechos fundamentales.
3) Fijar concordancias con otros regímenes vigentes, regulados por los artículos 226, 230, 230-A y 231 del Código Procesal Penal, la Ley 27697, el Decreto Legislativo 1182 y la Ley 30077, de manera que el monitoreo no se superponga ni colisione con la intervención en la red del operador, con la revisión de equipos incautados ni con el acceso a datos de localización gestionados por las operadoras.

IV. Fundamentación de la iniciativa

El numeral 10 del artículo 2 de la Constitución Política del Perú no se agota en reservar la decisión de una medida de intervención de las comunicaciones al juez; exige además que la intervención se realice "con las garantías previstas en la ley". Esa cláusula convierte a la ley en condición de validez de la medida, conforme al principio según el cual toda limitación de un derecho fundamental debe provenir de una ley (STC 2235-2004-AA/TC[6], fundamento 3). Sin una ley que defina el objeto, el alcance, los límites y el procedimiento del monitoreo, el mandato que lo autorice se apoya en un término carente de contenido, con el consiguiente riesgo de nulidad. La presente proposición no crea la medida, que el propio Código Procesal Penal ya contempla, sino que define y desarrolla el término con el que la denomina, dando cumplimiento a esa exigencia constitucional.

En esa línea, el estándar interamericano recogido por el Tribunal Constitucional exige que la ley que habilita la interceptación sea precisa e indique reglas claras y detalladas sobre la materia (STC 00655-2010-PHC/TC[7], que recoge el Caso Escher y otros vs. Brasil, Corte Interamericana de Derechos Humanos, sentencia del 6 de julio de 2009). La presente proposición satisface ese estándar: define la medida por lo que hace, acceder al equipo del investigado para captar un catálogo determinado de supuestos, y la declara aplicable sea cual fuere la técnica empleada, presente o futura. La precisión queda asegurada por la determinación del objeto y por el mandato judicial que individualiza el equipo y el alcance en

[6] Sentencia del Expediente N.° 2235-2004-AA/TC. (2005). Tribunal Constitucional del Perú. https://www.tc.gob.pe/jurisprudencia/2005/02235-2004-AA.pdf
[7] Sentencia del Expediente N.° 00655-2010-PHC/TC. (2010). Tribunal Constitucional del Perú. https://www.tc.gob.pe/jurisprudencia/2010/00655-2010-HC.html

cada caso, en línea con el estándar análogo de la jurisprudencia constitucional alemana, que exige delimitar el objeto de la medida y fijar sus garantías en la propia ley.

Precisamente, Alemania reguló el registro remoto de equipos para captar comunicaciones en los parágrafos 100a y siguientes de su Ordenanza Procesal Penal, con protección expresa del ámbito reservado de la vida privada en el parágrafo 100d. El Tribunal Constitucional Federal alemán, en la resolución N° 1 BvR 180/23[8] del 24 de junio de 2025, declaró inconstitucionales varios aspectos de esa regulación por falta de precisión en la delimitación de los derechos afectados y de sus garantías. De allí que la lección sea doble y directa para el Perú: la medida es admisible, pero exige que la ley declare con precisión qué afecta y con qué garantías. En la misma línea, el Tribunal de Justicia de la Unión Europea, en el asunto C-548/21[9] del 4 de octubre del 2024 y en el asunto C-746/18[10] del 2 de marzo del 2021, exigió control previo de un juez o autoridad independiente para el acceso a datos de esta naturaleza, con una excepción acotada para la urgencia debidamente justificada y control inmediato posterior. En definitiva, una estructura normativa que precisa el control previo de ese tipo de intervenciones, así como estrictos supuestos de excepción que es el modelo garantista que recoge la presente proposición.

Es preciso señalar que el objeto de la medida guarda armonía con la definición legal de comunicación, aspecto que es necesario aclarar y resaltar. La presente proposición legislativa autoriza captar no solo comunicaciones en tránsito, sino también comunicaciones registradas, esto es, información almacenada que constituya forma objetivada del pensamiento del investigado, como las comunicaciones o contenidos diversos que se muestran en la pantalla del equipo. Se podría objetar que esto excede el concepto de comunicación, en tanto implica acceder al registro del contenido del dispositivo, pero esta objeción encuentra respuesta en el derecho positivo peruano. Así, el numeral 1 del artículo 2 de la Ley N° 27697 define comunicación como "cualquier forma de transmisión del contenido del pensamiento, o de una forma objetivada de éste, por cualquier medio"; y precisa, que "no interesa que el proceso de transmisión de la comunicación se haya iniciado o no". Por tanto, la ley peruana ya considera comunicación a la forma objetivada del pensamiento, se haya transmitido o no.

En ese sentido, un mensaje redactado y no enviado, el borrador de un mensaje o un audio grabado para enviar son comunicación en los términos de la referida ley. El numeral 2 del mismo artículo añade que el medio, el soporte en el que se porta o transmite la comunicación, tiene el mismo régimen que la comunicación misma, y ese medio es, precisamente, el equipo del investigado. Por eso la proposición ancla en esa definición la captación de comunicaciones y de su contenido objetivado. La información almacenada que exceda ese contenido se capta únicamente en el alcance que especifique el mandato judicial y con exclusión de todo lo ajeno al hecho investigado, conforme al numeral 3 del artículo 4, de modo que la medida nunca autoriza la extracción indiscriminada de todo el contenido del equipo. De lo expuesto se concluye que el objeto del monitoreo queda delimitado por el concepto de comunicación que fija la ley peruana y, en lo que lo excede, por el mandato judicial y su vínculo con el hecho investigado.

---

[8] Resolución N° 1 BvR 180/23. (2025). Tribunal Constitucional Federal de Alemania. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2025/06/rs20250624_1bvr018023en.html

[9] Sentencia del Tribunal de Justicia (Gran Sala) en el asunto C-548/21. (2024). Tribunal de Justicia de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62021CJ0548

[10] Sentencia del Tribunal de Justicia (Gran Sala) en el asunto C-746/18. (2021). Tribunal de Justicia de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62018CJ074

Por otro lado, en lo que respecta al control judicial de la medida, la proposición exige que la autorización del juez anteceda al acceso al equipo, pues la revisión judicial posterior no podría impedir que la injerencia exceda lo estrictamente necesario para la investigación. En esa línea, la jurisprudencia nacional ha resuelto que lo accedido antes de la autorización judicial constituye prueba ilícita, aunque la autorización llegue con posterioridad (STC 02324-2020-PHC/TC[11]). La proposición recoge esa regla con claridad: no admite que el acceso al equipo se legitime mediante un régimen de convalidación, confirmación o ratificación posterior. El supuesto de apremio del numeral 5 del artículo 231 del Código Procesal Penal, que la proposición incorpora por remisión, no es una excepción a esa exigencia: solo opera cuando el propio mandato judicial previó y delimitó la eventualidad, de modo que la autorización del juez ya existe, anticipada y condicionada, antes de que el Fiscal actúe en apremio para conjurar una amenaza inminente a la vida, la integridad o la libertad de las personas. Lo que en ese supuesto sobreviene no es la autorización, que es previa, sino una convalidación que opera como control adicional de la ejecución urgente, con todos sus requisitos: previsión de la eventualidad en el mandato, apremio, plazo máximo de setenta y dos horas, y cuenta y solicitud de convalidación al juez competente con la máxima celeridad. De ese modo, ni aun en el apremio se accede al equipo sin autorización judicial previa; la proposición sigue el modelo que el propio derecho positivo peruano ya había trazado.

En cuanto a la motivación reforzada que debe justificar el monitoreo, encuentra pleno asidero en la existencia del cifrado de extremo a extremo, supuesto en el que la intervención resulta "absolutamente necesaria" en los términos del numeral 1 del artículo 230 del Código Procesal Penal. La proposición convierte esa premisa en carga concreta, al exigir que el requerimiento y el mandato motiven: i) por qué la captación no es posible de manera inteligible por la vía del operador u otras técnicas; ii) por qué es necesario el acceso al equipo determinado; y iii) por qué lo es el alcance solicitado. La omisión de esa motivación invalida el mandato. La proposición no presume la imposibilidad técnica: obliga a acreditarla ante el juez, caso por caso. Se asegura así que la intensidad de la injerencia se corresponda con el rigor de su justificación y con la motivación del juez que la autoriza.

La proposición delimita con claridad los ámbitos en los que la medida se aplica y aquellos que quedan fuera de su alcance. Establece dos exclusiones, la primera: las comunicaciones en tránsito por la infraestructura del operador, cualquiera sea su naturaleza, no forman parte del monitoreo y se rigen por los artículos 230 y 231 del Código Procesal Penal; si una investigación requiere ambas vías, se trata de dos medidas distintas, cada una con su régimen. La segunda, más delicada, concierne al micrófono y a la cámara del equipo: solo pueden usarse mientras existe una comunicación en curso y únicamente para captar esa comunicación, no el entorno. Fuera de una comunicación, activar el micrófono o la cámara para captar el entorno está prohibido en términos absolutos. La razón es que, durante una llamada, el micrófono capta lo que el investigado transmite, que es la comunicación misma, lo único que el artículo 230.1 autoriza; captar el domicilio, los terceros ajenos a la comunicación queda fuera de esa autorización.

Sobre la ejecución de la medida, la proposición distribuye las responsabilidades para evitar su concentración. Sigue, en esto, el modelo del sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú, que opera con dos componentes en

[11] Sentencia del Tribunal Constitucional N.° 02324-2020-PHC/TC. (2021). Tribunal Constitucional. https://jurisprudencia.sedetc.gob.pe/sentencia/02324-2020-hc-847-2021

entidades distintas, de modo que ninguna controle la medida por completo. Esa separación responde a una razón concreta: reducir el riesgo de uso indebido de la herramienta, lógica que se traslada al monitoreo. Por ello, la proposición organiza la ejecución en dos componentes separados, uno a cargo del Ministerio Público y otro de la Policía Nacional, y añade la separación funcional clásica: quien autoriza no ejecuta, quien configura no accede y quien accede no decide la utilización. Ningún actor concentra todas las funciones, y cada tránsito entre ellas deja rastro en el registro.

Otra salvaguarda para la seguridad y la protección de la información es la trazabilidad de toda la operación, que la proposición exige como condición de validez. El sistema debe registrar toda operación de manera íntegra y protegida contra alteración, y asegurar la integridad de lo captado mediante valores de verificación comprobables. Ese aseguramiento responde a las sospechas de manipulación habituales en esta clase de medidas. Así, cuando la defensa alegue que lo captado fue alterado o que algo se suprimió, la respuesta no será una afirmación de buena fe, sino un registro verificable y un instrumento sujeto a verificación técnica por un órgano independiente del que ejecuta la medida. Sin esa trazabilidad, la medida no resistiría el control; con ella, lo resiste y consolida su validez.

Una vez que la medida concluye, por cumplirse el objeto para el que fue autorizada, por interrupción o por vencimiento del plazo, la injerencia sobre el equipo cesa por completo. Ello implica que el instrumento instalado se elimina y el equipo se restaura, lo que debe constar en acta y comunicarse al juez. Lo captado, en cambio, se conserva bajo el régimen del artículo 231 del Código Procesal Penal. El cese produce así dos efectos que no se contradicen y cumplen funciones distintas: i) la eliminación del instrumento, que cierra la injerencia; y ii) la conservación de lo captado, que preserva la prueba y el derecho de defensa.

Cabe señalar que se han registrado antecedentes institucionales orientados a abordar la problemática de la prueba en entornos digitales. En esa línea, el 7 de noviembre de 2025, el Consejo Nacional de Política Criminal (CONAPOC), bajo la presidencia del Ministerio de Justicia y Derechos Humanos, aprobó una propuesta legislativa sobre preservación, obtención y aseguramiento de la evidencia digital en el proceso penal. Aunque dicho texto planteaba el acceso remoto a equipos informáticos bajo reserva judicial, la Autoridad Nacional de Protección de Datos Personales —mediante el Informe Jurídico N.° 060-2025-JUS/DGTAIPD del 24 de diciembre de 2025— advirtió la inviabilidad de su formulación al admitir la captación de datos de tráfico y geolocalización sin control judicial previo y bajo un esquema de convalidación posterior. Asimismo, pese a modificar el artículo 230 e incorporar el artículo 230-B al Código Procesal Penal, la referida iniciativa omitió definir el término monitoreo y delimitar sus alcances, manteniendo incólume el vacío normativo que la presente proposición busca resolver.

Por último, la medida se encauza en el numeral 10 del artículo 2 de la Constitución Política, que admite que las comunicaciones y sus instrumentos sean "abiertos, incautados, interceptados o intervenidos" por mandamiento motivado del juez. El acceso al equipo para captar comunicaciones queda habilitado por ese texto, pues el equipo es el instrumento en el que la comunicación se porta o transmite. Los derechos concurrentes de los numerales 7 y 9 del artículo 2, la intimidad personal y la inviolabilidad del domicilio se protegen no solo por esa habilitación legal, sino también por la prohibición absoluta de captación ambiental que la proposición incorpora. La regla general del mandato judicial previo, sin convalidación,

satisface la exigencia de control anterior; y la propia ley declara qué derechos afecta y con qué garantías los resguarda.

V. Antecedentes legislativos, investigaciones y fuentes

a. Marco legislativo vigente

La materia se asienta sobre un conjunto de normas que esta proposición invoca por remisión.

- Constitución Política, en el numeral 10 de su artículo 2, reserva la intervención de las comunicaciones al mandato motivado del juez con las garantías de ley.
- Código Procesal Penal, aprobado por Decreto Legislativo 957, contiene el artículo 226 sobre el trámite reservado, el artículo 230 que menciona el monitoreo sin definirlo y sus normas modificatorias que tampoco aportaron tal definición (Leyes 30077, 30096, 30171 y 32130 y por el Decreto Legislativo 1605; el numeral 3 fue modificado por el Decreto Legislativo 1708), el artículo 230-A (incorporado por el Decreto Legislativo 1698) que regula la revisión de equipos informáticos hallados o incautados, y el artículo 231 que fija el registro, la conservación, la reevaluación y el reexamen de la intervención.
- Ley 27697 aporta las definiciones de comunicación y de medio que esta proposición adopta.
- Ley 30096 aporta, en su Novena Disposición Complementaria Final, la terminología de sistema informático y datos informáticos conforme al Convenio sobre la Ciberdelincuencia.
- Ley 30077 aporta el régimen supletorio de su artículo 10 y la reserva de su artículo 15. El Código Penal sanciona en sus artículos 162, 162-A y 162-B la interferencia y la posesión de equipos de interceptación.
- Proyecto de Ley 11815/2024-CR regula la evidencia digital como medio de prueba y su cadena de custodia.
- Proyecto de Ley 12950/2025-CR autoriza la lectura de información de dispositivos hallados o incautados en establecimientos penitenciarios.

b. Jurisprudencia

- Del Tribunal Constitucional: Expedientes 00655-2010-PHC/TC, 01019-2017-PA/TC, 2235-2004-AA/TC y 02324-2020-PHC/TC.
- De la Corte Suprema: el Acuerdo Plenario 4-2010/CJ-116, la Casación 1251-2019/Lambayeque y la Casación 2089-2019/Arequipa.

c. Marco normativo internacional

- Del derecho internacional y comparado: la sentencia de la Corte Interamericana de Derechos Humanos en Escher y otros vs. Brasil (2009); las sentencias del Tribunal de Justicia de la Unión Europea en los asuntos C-548/21 (2024) y C-746/18 (2021); la resolución del Tribunal Constitucional Federal alemán 1 BvR 180/23 (2025); los parágrafos 100a, 100b y 100d de la Ordenanza Procesal Penal alemana; y el Convenio sobre la Ciberdelincuencia, aprobado por Resolución Legislativa 30913 y ratificado por Decreto Supremo 010-2019-RE, en particular su artículo 32 sobre acceso transfronterizo a datos almacenados

VI. Sectores comprendidos

- **El Poder Judicial,** a través de los Juzgados de Investigación Preparatoria, a quienes corresponde autorizar la medida, controlar su ejecución, conocer el reexamen y, con el Ministerio Público y la Policía Nacional, acordar el protocolo de ejecución.
- **El Ministerio Público**, que conduce la medida, formula el requerimiento, evalúa y utiliza lo captado, y asume uno de los dos componentes de la ejecución de la medida.
- **La Policía Nacional del Perú,** que ejecuta la medida a través de la unidad especializada del sistema de intervención y control de las comunicaciones y asume el otro componente de la ejecución de la medida.
- **Las empresas prestadoras de servicios de telecomunicaciones** quedan comprendidas de manera tangencial y sin nuevas obligaciones. Su participación se produce solo cuando la ejecución del monitoreo la requiera, bajo el numeral 4 del artículo 230 del Código Procesal Penal. El régimen de revisión de equipos del artículo 230-A y las demás técnicas especiales de investigación no se modifican.

VII. Normas que se modifican o derogan

La proposición no modifica el texto de ninguna norma vigente y tampoco propone la derogación de ninguna ley específica.

VIII. Análisis costo-beneficio

La presente proposición legislativa no genera gasto público adicional ni irroga el uso de recursos extraordinarios del Tesoro Público. La implementación de sus disposiciones será asumida de manera progresiva con cargo al presupuesto institucional normativamente asignado a las entidades del sistema de justicia involucradas en su ejecución. Asimismo, la medida no impone cargas financieras ni obligaciones tarifarias a los operadores de servicios de telecomunicaciones, así como tampoco establece beneficios ni exenciones de carácter económico, respetando estrictamente lo dispuesto en el inciso a) del artículo 107 del Reglamento del Congreso de la República.

Desde una perspectiva de impacto económico, la propuesta legislativa genera un efecto indirecto y altamente favorable para la administración de justicia. Al dotar de certeza y seguridad jurídica a la medida de monitoreo, se previenen dilaciones procesales, planteamientos de nulidad y la eventual repetición de diligencias derivadas de vacíos interpretativos. De este modo, la incorporación de salvaguardias técnicas y garantías para la protección de la información captada optimiza la eficiencia operativa de las investigaciones penales, reduciendo significativamente los costos procesales futuros, tanto institucionales como de las partes involucradas.

IX. Impacto ambiental

No aplica.