SUMILLA: LEY QUE ELIMINA EL ANONIMATO EN LÍNEAS MÓVILES Y APLICATIVOS DIGITALES PARA COMBATIR LA EXTORSIÓN Y PROTEGER A LA CIUDADANÍA.

Los Congresistas de la República que suscriben a iniciativa del congresista **Paul Silvio Gutiérrez Ticona**, miembro del grupo parlamentario "Somos Perú", en estricto cumplimiento de lo dispuesto en el artículo 107º de la Constitución Política del Estado y de conformidad con lo establecido en el literal c) del artículo 22° y los artículos 75° y 76° del Reglamento del Congreso de la República, presenta la siguiente propuesta legislativa:

EL CONGRESO DE LA REPÚBLICA;
Ha dado la Ley siguiente:

LEY QUE ELIMINA EL ANONIMATO EN LÍNEAS MÓVILES Y APLICATIVOS DIGITALES PARA COMBATIR LA EXTORSIÓN Y PROTEGER A LA CIUDADANÍA

Artículo 1.- Objeto de la Ley
La presente Ley tiene por objeto establecer un sistema nacional integral de identificación, verificación, trazabilidad y control del acceso al servicio público móvil y a los servicios digitales asociados, orientado a fortalecer la seguridad ciudadana y la lucha contra el crimen organizado, mediante la prevención del uso indebido de la conectividad digital, garantizando el respeto de los derechos fundamentales, la libertad de empresa, la neutralidad tecnológica y la protección de datos personales.

Artículo 2.- Finalidad
La presente Ley tiene por finalidad asegurar la identificación cierta y verificable de los usuarios de servicios de telecomunicaciones y servicios digitales, consolidar la trazabilidad del acceso y uso de dichos servicios, prevenir la suplantación de identidad, el uso fraudulento de líneas y plataformas digitales, y establecer mecanismos de control idóneos, necesarios y proporcionales que permitan reducir de manera efectiva la comisión de delitos a través de medios digitales.

Artículo 3.- Ámbito de aplicación
La presente Ley es aplicable a las empresas operadoras del servicio público móvil, a los proveedores de acceso a internet, a las personas naturales titulares de líneas móviles, a las personas jurídicas proveedoras de servicios digitales, aplicativos de mensajería, comunicación o interacción remota, así como a las entidades públicas competentes en materia de regulación, supervisión, fiscalización, seguridad y administración de justicia, conforme a sus competencias legalmente establecidas.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

Artículo 4.- Límite razonable y control de líneas móviles
La persona natural podrá contratar y mantener activas hasta diez (10) líneas móviles por empresa operadora, con un límite máximo acumulado de veinte (20) líneas a nivel nacional, comprendiendo todas las modalidades tecnológicas existentes o futuras.
Excepcionalmente, podrá autorizarse un número mayor cuando se acredite una necesidad objetiva, razonable y verificable, conforme al procedimiento administrativo especial establecido por el OSIPTEL, garantizando criterios objetivos, debida motivación y control posterior.
La activación del servicio se encuentra condicionada a la verificación de identidad del titular y a la consulta previa, obligatoria y en tiempo real del Registro Nacional de Líneas Activas por Usuario, siendo inválida toda activación que incumpla dichas condiciones.

Artículo 5.- Sistema integral de verificación de identidad y trazabilidad
Toda contratación, activación, reposición, migración, portabilidad, transferencia de titularidad o uso del servicio público móvil, así como la habilitación de tarjetas SIM, eSIM u otros mecanismos de acceso, requiere verificación previa, obligatoria y fehaciente de la identidad del usuario mediante mecanismos de autenticación biométrica interoperables con el Registro Nacional de Identificación y Estado Civil (RENIEC).
Dicha verificación constituye condición esencial de validez del acto y debe integrarse a un sistema nacional interoperable que garantice la trazabilidad integral, continua y verificable del servicio.

Artículo 6.- Registro Nacional de Líneas Activas por Usuario
El OSIPTEL implementa, administra y supervisa el Registro Nacional de Líneas Activas por Usuario como sistema único, interoperable, seguro y de consulta obligatoria en tiempo real.
Las empresas operadoras están obligadas a registrar, actualizar, validar y consultar permanentemente dicha información, constituyendo su verificación un requisito indispensable para toda activación o modificación del servicio.

Artículo 7.- Prohibición de contratación fraudulenta y numeración irregular
Se prohíbe la contratación, activación, uso o cesión del servicio público móvil mediante identidad falsa, inexistente, suplantada o no verificada, así como el uso de numeración virtual, automatizada, generada mediante sistemas informáticos o cualquier mecanismo destinado a eludir los procesos de identificación del titular.

Artículo 8.- Control de reposición y continuidad del servicio
La reposición, duplicado, sustitución o reactivación de mecanismos de acceso al servicio solo puede efectuarse previa verificación biométrica del titular, debiendo registrarse íntegramente la operación y conservarse evidencia digital suficiente que permita su auditoría conforme a los estándares establecidos por el OSIPTEL.

Artículo 9.- Condición de acceso a servicios digitales y uso de datos
El acceso, uso y provisión de servicios de comunicación digital, mensajería instantánea, redes sociales, servicios OTT y aplicativos equivalentes se encuentra condicionado a la existencia

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

de una línea del servicio público móvil activa, debidamente verificada y vinculada a la identidad del usuario conforme a la presente Ley.

Las empresas operadoras del servicio público móvil y los proveedores de acceso a internet deben garantizar que el servicio de transmisión de datos sea habilitado exclusivamente respecto de líneas cuya titularidad haya sido validada, debiendo bloquear, suspender o restringir el acceso a servicios digitales cuando la línea no cumpla con los requisitos de verificación, se encuentre inactiva o presente inconsistencias.

Los proveedores de servicios digitales están obligados a implementar mecanismos de validación e interoperabilidad en tiempo real con las empresas operadoras, a fin de verificar la autenticidad, vigencia y titularidad de la línea asociada a cada cuenta, quedando prohibida la habilitación o mantenimiento de cuentas vinculadas a numeración no verificada, virtual, automatizada o desvinculada de una línea activa.
El uso de funcionalidades multidispositivo o acceso remoto solo puede mantenerse mientras subsista la verificación activa de la línea titular.

Artículo 10.- Interoperabilidad y cooperación interinstitucional
El sistema nacional de registro y verificación es interoperable con las entidades competentes en materia de seguridad, inteligencia y administración de justicia, permitiendo el acceso a la información exclusivamente para fines de prevención, investigación y persecución de delitos, conforme a los principios de legalidad, necesidad, proporcionalidad y control.

Artículo 11.- Protección de datos personales
El tratamiento de datos personales y biométricos se realiza conforme a los principios de legalidad, finalidad, proporcionalidad, minimización, seguridad y responsabilidad, limitándose estrictamente a los fines de identificación, trazabilidad y prevención del uso indebido del servicio.

Artículo 12.- Obligaciones de las empresas operadoras, proveedores de acceso a internet y proveedores de servicios digitales
Las empresas operadoras, proveedores de acceso a internet y proveedores de servicios digitales deben implementar y garantizar sistemas técnicos idóneos que aseguren la verificación de identidad en tiempo real, la trazabilidad del servicio, la interoperabilidad de los sistemas, el bloqueo automático de accesos irregulares, la detección de patrones de uso indebido y la conservación de registros auditables conforme a los estándares establecidos por el OSIPTEL.

Artículo 13.- Régimen sancionador
Constituyen infracciones muy graves el incumplimiento de los mecanismos de verificación de identidad, la activación de servicios sin validación, la habilitación de líneas o cuentas vinculadas a identidades fraudulentas, la omisión de controles de trazabilidad, el incumplimiento de la interoperabilidad y la habilitación de servicios digitales sobre numeración no verificada.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

El OSIPTEL impone las sanciones correspondientes conforme a su régimen, pudiendo aplicar medidas adicionales como la suspensión temporal de operaciones en caso de reincidencia o afectación grave a la seguridad pública.

Artículo 14.- Garantías del debido procedimiento
Toda medida de suspensión o baja del servicio debe adoptarse mediante decisión debidamente motivada, con notificación previa y plazo razonable de regularización, salvo en supuestos de suplantación de identidad o riesgo grave e inminente debidamente acreditado, en los cuales podrá disponerse de forma inmediata con control posterior.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Reglamentación
El Ministerio de Transportes y Comunicaciones, reglamenta la presente Ley en un plazo no mayor de noventa (90) días.

SEGUNDA.- Adecuación progresiva
Las empresas operadoras, proveedores de acceso a internet y proveedores de servicios digitales deben adecuarse a la presente Ley en un plazo máximo de noventa (90) días.

TERCERA.- Implementación tecnológica
El OSIPTEL, en coordinación con el RENIEC y las entidades competentes, garantiza la interoperabilidad, seguridad y funcionamiento del sistema nacional de verificación.

CUARTA.- Vigencia de la Norma
La presente Ley, entra en vigencia a partir del día siguiente de la publicación en el Diario Oficial El Peruano.

Lima, 29 de Abril de 2026

FIRMA DIGITAL
Firmado digitalmente por: ZEGARRA SABOYA Ana Zadith FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 30/04/2026 15:55:55-0500

FIRMA DIGITAL
Firmado digitalmente por: GUTIERREZ TICONA Paul Silvio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 30/04/2026 09:29:42-0500

FIRMA DIGITAL
Firmado digitalmente por: PAREDES GONZALES Alex Antonio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 04/05/2026 12:40:30-0500

FIRMA DIGITAL
Firmado digitalmente por: PAZO NUNURA Jose Bernardo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 04/05/2026 10:00:10-0500

FIRMA DIGITAL
Firmado digitalmente por: VALER PINTO Hector FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 30/04/2026 12:45:36-0500

FIRMA DIGITAL
Firmado digitalmente por: VALER PINTO Hector FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 30/04/2026 12:45:49-0500

FIRMA DIGITAL
Firmado digitalmente por: MEDINA HERMOSILLA Elizabeth Sara FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 04/05/2026 10:19:33-0500

FIRMA DIGITAL
Firmado digitalmente por: ZEA CHOQUECHAMBI Oscar FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 30/04/2026 13:19:41-0500

EXPOSICIÓN DE MOTIVOS

I.- INTRODUCCIÓN DE LA PROPUESTA LEGISLATIVA

La transformación digital de las comunicaciones ha generado un escenario en el que la conectividad móvil y los servicios digitales asociados se han convertido en herramientas esenciales para el desarrollo social, económico y democrático; sin embargo, este mismo entorno ha sido progresivamente instrumentalizado por organizaciones criminales para la comisión de delitos como la extorsión, el fraude y la suplantación de identidad, aprovechando la ausencia de mecanismos eficaces de identificación y trazabilidad en el uso de líneas móviles y aplicativos digitales. En este contexto, el presente proyecto de ley parte de reconocer que el anonimato funcional en las telecomunicaciones constituye uno de los principales facilitadores de la criminalidad contemporánea, en la medida en que dificulta la identificación de los autores y debilita la capacidad de respuesta del Estado frente a estas conductas ilícitas, lo cual ha sido ampliamente advertido por la literatura especializada en ciberseguridad y gobernanza digital, que señala que los entornos digitales sin mecanismos robustos de identificación favorecen la expansión de economías ilícitas y redes criminales transnacionales[1].

La presente iniciativa legislativa se sustenta en la necesidad de establecer un modelo normativo que permita restituir el principio de trazabilidad en el ecosistema digital, entendiendo que la identificación verificable del usuario no constituye una restricción arbitraria, sino una condición necesaria para garantizar la seguridad pública en entornos altamente digitalizados. En esa línea, diversos estudios han demostrado que los sistemas de identificación digital y autenticación robusta reducen significativamente los riesgos de fraude y actividades ilícitas, al generar un entorno de responsabilidad verificable en el uso de servicios tecnológicos[2]. Bajo esta premisa, la presente propuesta de ley introduce la verificación biométrica obligatoria en todas las fases del servicio móvil, no como un mecanismo de control desproporcionado, sino como una herramienta técnica orientada a asegurar la correspondencia entre identidad y uso efectivo del servicio.

Asimismo, el presente proyecto de ley reconoce que la problemática no se limita al ámbito de las telecomunicaciones tradicionales, sino que se ha desplazado hacia los servicios digitales y aplicativos de mensajería que operan sobre la infraestructura de conectividad, los cuales, en ausencia de mecanismos de validación interoperable, permiten la creación y uso de cuentas desvinculadas de una identidad real. Esta situación ha sido identificada como un factor crítico en la proliferación de delitos digitales, dado que los servicios OTT (over-the-top) pueden operar al margen de los controles propios de los operadores de telecomunicaciones, generando espacios de anonimato estructural[3]. En atención a ello, la presente iniciativa legislativa propone un modelo de interoperabilidad obligatoria entre operadores y plataformas digitales, con el propósito de garantizar que el acceso y uso de dichos servicios se encuentre condicionado a la existencia de una línea activa y debidamente verificada.

[1] Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
[2] World Bank. (2019). *ID4D Global Dataset: Digital Identification for Development*. World Bank Publications.
[3] GSMA. (2020). *The Mobile Economy 2020*. GSMA Intelligence.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

Desde una perspectiva de política pública, la presente propuesta de ley se alinea con los enfoques contemporáneos de seguridad digital que promueven la integración de sistemas de identificación, trazabilidad y control como elementos esenciales para la prevención del delito en entornos digitales. En efecto, la evidencia internacional demuestra que la implementación de registros integrados y sistemas de validación en tiempo real fortalece la capacidad del Estado para detectar patrones de comportamiento ilícito y actuar de manera oportuna frente a amenazas emergentes[4]. En ese sentido, la creación de un registro nacional interoperable administrado por el organismo regulador no solo responde a una necesidad técnica, sino que constituye una herramienta estratégica para la articulación de acciones entre entidades públicas y privadas.

Del mismo modo, la presente iniciativa legislativa incorpora un enfoque de equilibrio entre seguridad y derechos fundamentales, reconociendo que cualquier intervención estatal en el ámbito digital debe respetar los principios de legalidad, proporcionalidad y protección de datos personales. La regulación propuesta no busca controlar el contenido de las comunicaciones ni restringir el acceso a la tecnología, sino establecer condiciones mínimas de identificación y responsabilidad en su uso, en concordancia con estándares internacionales que sostienen que la gobernanza digital debe basarse en mecanismos de confianza, seguridad y rendición de cuentas[5]. En tal sentido, el diseño normativo del presente proyecto de ley integra garantías como el debido procedimiento, la limitación de la finalidad del tratamiento de datos y la supervisión institucional, asegurando que las medidas adoptadas sean compatibles con el orden constitucional.

En este marco, la presente propuesta de ley configura un modelo integral de control del ecosistema digital que articula la verificación de identidad, la trazabilidad del servicio, la interoperabilidad de sistemas y la responsabilidad de los actores involucrados, con el objetivo de cerrar las brechas que actualmente permiten el uso delictivo de la conectividad. Su adopción responde a la necesidad urgente de actualizar el marco normativo frente a las nuevas dinámicas del crimen organizado, que han migrado hacia entornos digitales aprovechando vacíos regulatorios, y constituye una respuesta estructural orientada a recuperar la capacidad del Estado para garantizar la seguridad ciudadana en la era digital.

➢ ANÁLISIS DEL MARCO NORMATIVO

- Constitución Política del Perú.
- Ley N.º 27336, Ley de Desarrollo de las Funciones y Facultades del OSIPTEL.
- Ley N.º 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.
- Decreto Supremo N.º 013-93-TCC, Texto Único Ordenado de la Ley de Telecomunicaciones.
- Decreto Supremo N.º 020-2007-MTC, Reglamento General de la Ley de Telecomunicaciones.
- Ley N.º 29733, Ley de Protección de Datos Personales.
- Decreto Supremo N.º 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales.

[4] OECD. (2015). *Digital Security Risk Management for Economic and Social Prosperity*. OECD Publishing.
[5] Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

- Ley N.º 27269, Ley de Firmas y Certificados Digitales.
- Decreto Supremo N.º 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Legislativo N.º 1182, Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación.
- Decreto Legislativo N.º 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad (RENTESEG).
- Ley N.º 30096, Ley de Delitos Informáticos.
- Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Ley N.º 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.
- Ley N.º 27933, Ley del Sistema Nacional de Seguridad Ciudadana.
- Ley N.º 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas.
- Decreto Legislativo N.º 957, Código Procesal Penal.
- Ley N.º 26859, Ley Orgánica de Elecciones (en lo relativo al uso de medios tecnológicos y verificación de identidad).
- Resoluciones del Consejo Directivo del OSIPTEL sobre registro, validación y control de líneas móviles.
- Normativa del Registro Nacional de Identificación y Estado Civil (RENIEC) sobre verificación biométrica e identidad digital.

II.- FUNDAMENTOS DE LA PROPUESTA LEGISLATIVA

La presente iniciativa legislativa se sustenta en la necesidad de responder a una transformación estructural del fenómeno delictivo, particularmente de la extorsión, que ha migrado desde formas tradicionales hacia esquemas altamente sofisticados basados en el uso de tecnologías de la información y comunicación. En este nuevo contexto, el anonimato digital se configura como un factor determinante que facilita la comisión de delitos, reduce los costos de operación de las organizaciones criminales y dificulta significativamente la identificación y persecución de los responsables. Diversos estudios han evidenciado que la capacidad de operar bajo identidades no verificadas en entornos digitales incrementa la incidencia de delitos como la extorsión, el fraude y la suplantación de identidad, al eliminar barreras de trazabilidad y control estatal (Wall, 2007)[6].

El presente proyecto de ley plantea una intervención normativa estructural orientada a restablecer el principio de identificación cierta en el uso de los servicios de telecomunicaciones y aplicativos digitales, bajo el entendimiento de que la anonimidad irrestricta en entornos digitales no constituye un derecho absoluto, sino una condición susceptible de regulación cuando entra en tensión con bienes jurídicos superiores como la seguridad ciudadana y el orden público. Desde la perspectiva de la criminología contemporánea, la trazabilidad de las comunicaciones constituye un elemento esencial para la prevención del delito, en tanto incrementa el riesgo percibido por los potenciales

[6] Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

infractores y fortalece la capacidad de respuesta del sistema de justicia penal (Clarke, 1997)[7].

La presente propuesta de ley incorpora como eje central la verificación obligatoria de identidad mediante mecanismos biométricos interoperables, lo cual responde a estándares internacionales de seguridad digital que reconocen la autenticación fuerte como herramienta clave para mitigar riesgos de fraude y suplantación. En ese sentido, la autenticación biométrica, cuando se implementa bajo principios de proporcionalidad y protección de datos, constituye un mecanismo idóneo para garantizar la correspondencia entre la identidad física del usuario y su actividad digital, reduciendo significativamente los espacios de anonimato funcional utilizados con fines ilícitos (Jain, Ross & Prabhakar, 2004)[8].

Asimismo, la presente iniciativa legislativa reconoce que la regulación del fenómeno delictivo en entornos digitales no puede limitarse a la infraestructura de telecomunicaciones, sino que debe extenderse a la capa de servicios digitales, particularmente a los aplicativos de mensajería y comunicación que hoy constituyen el principal medio para la comisión de extorsiones. En esa línea, se establece la obligación de vincular el acceso y funcionamiento de dichos aplicativos a líneas móviles previamente verificadas, cerrando el circuito entre identidad, conectividad y uso de plataformas digitales. Este enfoque integral se encuentra alineado con las tendencias regulatorias que buscan responsabilizar a los distintos actores del ecosistema digital en la prevención de riesgos sistémicos asociados al uso de tecnologías (Kuner, 2013)[9].

Por otro lado, el presente proyecto de ley incorpora la creación de un registro nacional interoperable en tiempo real, lo cual permite consolidar información relevante para la supervisión y control del servicio, así como para la investigación de delitos. La interoperabilidad entre entidades públicas y privadas, bajo estándares de legalidad y protección de datos, ha sido identificada como un componente crítico en los sistemas modernos de seguridad digital, en tanto permite una respuesta coordinada y eficiente frente a amenazas complejas (Brenner, 2010)[10]. La presente propuesta de ley ha sido diseñada bajo un enfoque de constitucionalidad reforzada, garantizando que las medidas adoptadas sean idóneas, necesarias y proporcionales, evitando restricciones arbitrarias a derechos fundamentales como la libertad de empresa o la protección de datos personales. En ese sentido, el establecimiento de mecanismos de verificación de identidad, trazabilidad y control del acceso a servicios digitales se encuentra justificado en la necesidad de proteger a la ciudadanía frente a formas contemporáneas de criminalidad que se aprovechan de vacíos regulatorios y tecnológicos.

III.- IDENTIFICACIÓN DEL PROBLEMA

El presente proyecto de ley parte de un problema público concreto: la expansión de la extorsión y otras formas de criminalidad organizada mediante el uso anónimo o irregular

[7] Clarke, R. V. (1997). *Situational crime prevention: Successful case studies*. Harrow and Heston.
[8] Jain, A. K., Ross, A., & Prabhakar, S. (2004). *An introduction to biometric recognition*. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.
[9] Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.
[10] Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

de líneas móviles, servicios de internet y aplicativos digitales de mensajería. En la actualidad, la conectividad digital se ha convertido en una herramienta indispensable para la vida social, económica y productiva; sin embargo, también ha sido aprovechada por organizaciones criminales para ocultar su identidad, contactar víctimas, coordinar amenazas, exigir pagos y operar mediante cuentas vinculadas a números no verificados, numeración virtual, líneas obtenidas fraudulentamente o servicios digitales que no aseguran la identificación real del usuario. Esta situación evidencia una brecha entre el sistema tradicional de regulación de telecomunicaciones y la nueva realidad delictiva, donde el crimen ya no actúa únicamente a través de llamadas telefónicas, sino también mediante aplicativos, cuentas digitales, mensajería instantánea y mecanismos de acceso remoto.

La presente iniciativa legislativa identifica que el anonimato operativo en el ecosistema digital debilita la capacidad del Estado para prevenir, investigar y perseguir delitos. INTERPOL ha advertido que los criminales utilizan tecnologías que refuerzan el anonimato y dificultan la investigación, especialmente cuando la evidencia digital es volátil y se encuentra dispersa entre plataformas, operadores y jurisdicciones distintas (INTERPOL, 2026)[11]. Esta realidad guarda relación directa con el fenómeno de la extorsión, pues cuando una cuenta de mensajería o un aplicativo funciona sin una línea activa, verificada y vinculada a una identidad real, el sistema permite que el agresor o la organización criminal actúe con una ventaja indebida frente a la víctima y frente a la autoridad.

El problema no se agota en la existencia de líneas móviles registradas, sino en la falta de trazabilidad efectiva entre la persona, la línea, el acceso a internet y el aplicativo utilizado. Por ello, la presente propuesta de ley no se limita a exigir identificación en la contratación de una línea, sino que busca cerrar el circuito completo de uso del servicio digital. La experiencia comparada demuestra que el registro de tarjetas SIM, por sí solo, no resulta suficiente si no se acompaña de controles de calidad, actualización permanente, interoperabilidad y mecanismos efectivos de verificación de identidad. La GSMA ha señalado que las políticas de registro de SIM deben diseñarse con criterios de efectividad, proporcionalidad y capacidad real de implementación, pues un registro deficiente puede generar mercados paralelos, suplantación o uso fraudulento de identidades (GSMA, 2016)[12]. En ese sentido, el problema central no es únicamente cuántas líneas puede tener una persona, sino si cada línea, cada reposición, cada cuenta digital y cada acceso a datos están efectivamente vinculados a un titular verificable.

La presente iniciativa legislativa también reconoce que la extorsión digital se beneficia de la fragmentación institucional y tecnológica. Si una empresa operadora verifica la línea, pero el aplicativo permite operar con números virtuales, cuentas automatizadas, bots o accesos multidispositivo sin validación permanente, la finalidad de seguridad pública queda debilitada. De igual forma, si los proveedores de internet habilitan conectividad sin asegurar que el abonado se encuentre debidamente identificado, se mantiene una zona de opacidad que puede ser explotada por el crimen organizado. La UNODC ha advertido

[11] INTERPOL. (2026). *INTERPOL report warns of increasingly sophisticated global financial fraud threat*. INTERPOL.
[12] GSMA. (2016). *Mandatory registration of prepaid SIM card users: Considerations for policymakers*. GSMA.

que la delincuencia organizada en entornos digitales se adapta rápidamente a las oportunidades tecnológicas, utilizando infraestructuras de comunicación, anonimato y coordinación transnacional para ampliar su capacidad operativa (UNODC, 2025)[13]. Por ello, la respuesta normativa debe ser integral y no parcial.

La presente propuesta de ley se justifica porque el Estado tiene el deber de proteger a la ciudadanía frente a nuevas modalidades de criminalidad que utilizan la conectividad como medio de amenaza, intimidación y obtención ilícita de beneficios. No se trata de restringir arbitrariamente el acceso a internet ni de controlar contenidos, sino de establecer una regla mínima de responsabilidad digital: toda línea, cuenta o servicio que permita comunicación con terceros debe estar asociado a una identidad real, validada y trazable. La OCDE ha sostenido que los sistemas de identidad digital confiables deben construirse sobre reglas de seguridad, interoperabilidad, confianza y protección de derechos, permitiendo que las personas interactúen en entornos digitales con mayores niveles de certeza (OCDE, 2021)[14]. Bajo esa lógica, la identificación digital no constituye una carga desproporcionada cuando se orienta a prevenir delitos graves, siempre que se respeten la finalidad, la proporcionalidad, la minimización de datos y las garantías del debido procedimiento. El problema identificado exige, además, evitar que la regulación sea meramente declarativa. La lucha contra la extorsión requiere que las obligaciones de verificación sean operativas, interoperables y exigibles en tiempo real. Si los aplicativos de mensajería pueden seguir funcionando con numeración no verificada o desvinculada de una línea activa, el anonimato criminal continuará. Si las empresas operadoras no bloquean activaciones irregulares, si los proveedores de servicios digitales no validan la titularidad de la línea, o si no existen sanciones efectivas frente al incumplimiento, el sistema seguirá permitiendo que la tecnología sea utilizada como instrumento de amenaza. En esa línea, la OCDE ha resaltado que los sistemas modernos de identidad digital deben ser seguros, interoperables, inclusivos y resilientes, de modo que permitan gestionar riesgos sin sacrificar derechos fundamentales (OCDE, 2024)[15].

La presente iniciativa legislativa enfrenta, por tanto, una falla estructural del ecosistema digital: la desconexión entre identidad real, línea móvil, acceso a internet y cuenta digital. Esa desconexión permite que una persona o una organización criminal oculte su identidad, utilice números virtuales, mantenga cuentas en aplicativos sin titularidad verificable y eluda la acción del Estado. Frente a ello, la presente propuesta de ley plantea un modelo de trazabilidad responsable, bajo control legal, con protección de datos personales y con garantías de debido procedimiento, orientado a cerrar los espacios de anonimato que hoy facilitan la extorsión, la suplantación de identidad, el fraude digital y otras formas de criminalidad organizada.

IV.- RAZONABILIDAD DE LA IDENTIFICACIÓN DE ABONADOS Y RESPONSABILIDAD DE LOS OPERADORES EN LA PREVENCIÓN DE LA EXTORSIÓN

[13] United Nations Office on Drugs and Crime. (2025). *Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia*. UNODC.
[14] Organisation for Economic Co-operation and Development. (2021). *G20 collection of digital identity practices*. OECD Publishing.
[15] Organisation for Economic Co-operation and Development. (2024). *G7 mapping exercise of digital identity approaches*. OECD Publishing.

La razonabilidad de la identificación de abonados en el presente proyecto de ley se sustenta en que el servicio móvil y los aplicativos digitales han dejado de ser simples medios de comunicación para convertirse en instrumentos que pueden ser utilizados por organizaciones criminales para ejecutar extorsiones, amenazas, fraudes, suplantaciones y coordinaciones delictivas. Por ello, exigir que cada línea móvil, cuenta digital o acceso a servicios de mensajería esté vinculado a una identidad cierta, verificable y trazable no constituye una restricción arbitraria, sino una medida idónea para cerrar espacios de anonimato que hoy favorecen la impunidad. La Unión Internacional de Telecomunicaciones ha reconocido que la vinculación entre números móviles e identidad digital permite certificar que el abonado es quien afirma ser, fortaleciendo el acceso seguro a servicios electrónicos y reduciendo riesgos de uso indebido del ecosistema móvil (Unión Internacional de Telecomunicaciones, 2018)[16].

La presente iniciativa legislativa no busca limitar injustificadamente el acceso a las telecomunicaciones, sino ordenar su uso bajo criterios de identificación responsable, trazabilidad y control proporcional. En esa línea, la verificación biométrica, la consulta en tiempo real al registro nacional de líneas activas y la obligación de que los aplicativos funcionen únicamente sobre números verificados responden a una finalidad constitucionalmente legítima: proteger la seguridad ciudadana frente a la extorsión y el crimen organizado. El Grupo de Acción Financiera Internacional ha señalado que los sistemas de identidad digital confiables deben apoyarse en fuentes independientes y verificables, especialmente cuando se requiere prevenir abusos, reducir debilidades en controles humanos y fortalecer la autenticación permanente del usuario (Grupo de Acción Financiera Internacional, 2020)[17].

La responsabilidad de los operadores resulta razonable porque son los sujetos que habilitan el acceso inicial al sistema móvil, validan la identidad del abonado, asignan numeración, permiten la transmisión de datos y tienen capacidad técnica para bloquear activaciones irregulares o accesos vinculados a líneas no verificadas. En un modelo moderno de seguridad digital, no basta con sancionar al usuario que comete el delito; también debe exigirse diligencia reforzada a quienes administran la infraestructura que permite la conectividad. La OCDE ha desarrollado el enfoque de gestión del riesgo de seguridad digital, conforme al cual los operadores y actores del ecosistema deben adoptar medidas proporcionales para preservar la confianza, continuidad y seguridad de las actividades críticas sin impedir el desarrollo económico ni la innovación tecnológica (Organización para la Cooperación y el Desarrollo Económicos, 2015)[18].

La presente propuesta de ley también resulta razonable porque incorpora garantías frente a posibles excesos: exige finalidad legítima, proporcionalidad, protección de datos personales, debido procedimiento y responsabilidad subjetiva. Esto evita que el sistema se convierta en un mecanismo de vigilancia indiscriminada o censura digital. La medida no controla contenidos ni opiniones, sino que exige que el acceso a líneas, datos y

[16] Unión Internacional de Telecomunicaciones. (2018). *Digital identity in the ICT ecosystem: An overview*. ITU.
[17] Grupo de Acción Financiera Internacional. (2020). *Guidance on Digital Identity*. FATF/OECD.
[18] Organización para la Cooperación y el Desarrollo Económicos. (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. OECD Publishing.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

aplicativos se produzca sobre una identidad previamente verificada. La experiencia comparada en materia de identidad digital demuestra que los sistemas interoperables, seguros y basados en fuentes confiables permiten equilibrar inclusión, seguridad y protección de derechos, siempre que exista limitación de finalidad, minimización de datos y controles institucionales adecuados (Banco Mundial, 2019)[19].

Bajo esa lógica, la identificación obligatoria de abonados y la responsabilidad de operadores no deben entenderse como una carga desproporcionada, sino como una obligación de prevención frente a un riesgo socialmente grave. La extorsión digital se alimenta del anonimato, de la numeración falsa, de cuentas creadas con identidades inexistentes y de aplicativos que funcionan sin una línea activa realmente validada. Por ello, la presente iniciativa legislativa fortalece la seguridad ciudadana al cerrar el circuito de impunidad entre línea móvil, acceso a internet y cuenta digital, imponiendo a operadores, proveedores de internet y plataformas digitales deberes técnicos de verificación, interoperabilidad, trazabilidad y bloqueo de accesos irregulares. La GSMA ha señalado que las políticas de registro SIM y verificación de usuarios deben implementarse con reglas claras, enfoque de riesgo, protección de datos y cooperación entre Estado e industria para evitar usos indebidos del ecosistema móvil sin afectar indebidamente a los usuarios legítimos (GSMA, 2016)[20].

V.- EFECTO DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

El presente proyecto de ley genera un impacto transversal en el ordenamiento jurídico nacional al introducir un modelo normativo de control estructural del ecosistema digital que no sustituye el régimen vigente, sino que lo complementa y fortalece desde una lógica de seguridad pública y prevención del delito en entornos digitales. La presente iniciativa legislativa se articula directamente con el marco regulatorio de las telecomunicaciones, en particular con el Texto Único Ordenado de la Ley de Telecomunicaciones y la Ley N.º 27336, que regula las funciones del OSIPTEL, reforzando sus competencias en materia de supervisión mediante la incorporación de obligaciones de verificación en tiempo real, interoperabilidad y trazabilidad digital, lo cual transforma el enfoque tradicional de regulación, pasando de un modelo reactivo a uno preventivo sustentado en gestión de riesgos tecnológicos. Este tránsito responde a la necesidad de adaptar el derecho administrativo regulador a las nuevas dinámicas del delito digital, en donde la anonimización de las comunicaciones constituye un factor determinante para la expansión de la criminalidad organizada (Lessig, 2006).

La presente propuesta de ley incide también en la legislación sobre protección de datos personales, particularmente en la Ley N.º 29733, en la medida en que introduce el uso intensivo de mecanismos biométricos para la verificación de identidad. Sin embargo, lejos de generar una contradicción normativa, el proyecto establece una armonización funcional al incorporar principios de proporcionalidad, finalidad y seguridad en el tratamiento de datos, lo que permite encuadrar la medida dentro de los estándares constitucionales y del derecho comparado sobre gobernanza digital. En este contexto, el uso de datos biométricos se justifica como una medida idónea y necesaria frente a la

[19] Banco Mundial. (2019). *ID4D Practitioner's Guide*. World Bank Group.
[20] GSMA. (2016). *Mandatory registration of prepaid SIM cards: Addressing challenges through best practice*. GSM Association.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

magnitud del fenómeno delictivo, siempre que se limite a fines específicos de identificación y trazabilidad, lo cual resulta coherente con los criterios desarrollados en la doctrina especializada sobre regulación de tecnologías emergentes (Solove, 2004).

Asimismo, la presente iniciativa legislativa produce un efecto integrador respecto de la normativa vinculada a la seguridad ciudadana y la persecución del delito, al establecer mecanismos de interoperabilidad entre el sistema de telecomunicaciones y las entidades encargadas de la investigación penal, como la Policía Nacional del Perú y el Ministerio Público. Este elemento introduce una mejora sustantiva en la capacidad del Estado para responder frente a delitos como la extorsión, al permitir el acceso oportuno a información verificable sobre la titularidad y uso de líneas móviles, reduciendo significativamente los márgenes de impunidad derivados del anonimato digital. Este tipo de regulación se alinea con enfoques contemporáneos que reconocen la necesidad de integrar sistemas tecnológicos en la gestión de la seguridad pública, bajo esquemas de control legal y respeto de derechos fundamentales (Wall, 2007). De igual forma, el presente proyecto de ley impacta en la regulación del entorno digital al extender obligaciones a los proveedores de servicios digitales y aplicativos de comunicación, quienes, bajo el régimen vigente, operan con niveles limitados de exigencia en cuanto a verificación de identidad. La presente propuesta de ley introduce un estándar normativo que exige la vinculación entre cuenta digital y línea móvil verificada, lo que implica una reconfiguración del régimen de responsabilidad de estos actores, alineándolos con el principio de debida diligencia en la prestación de servicios digitales. Esta medida se sustenta en la necesidad de reducir los espacios de anonimato que facilitan la comisión de delitos, en concordancia con tendencias regulatorias internacionales que buscan equilibrar innovación tecnológica y seguridad pública (Kerr, 2010).

Finalmente, la vigencia de la norma proyecta efectos sobre el sistema jurídico en su conjunto al consolidar un nuevo paradigma de regulación basado en la identidad digital verificable como condición de acceso a servicios esenciales de comunicación. Este enfoque no restringe derechos, sino que los ordena bajo criterios de razonabilidad y proporcionalidad, garantizando que la libertad de empresa y la neutralidad tecnológica se ejerzan dentro de un marco de responsabilidad y trazabilidad que impida su instrumentalización con fines ilícitos. En ese sentido, la presente iniciativa legislativa se configura como una respuesta normativa coherente con la evolución del derecho frente a los desafíos de la criminalidad digital, fortaleciendo la capacidad del Estado para proteger a la ciudadanía sin desnaturalizar los principios constitucionales que rigen el ordenamiento jurídico.

VI.- ANALISIS COSTO – BENEFICIO

El presente proyecto de ley genera un beneficio público superior al costo regulatorio que impone, debido a que enfrenta uno de los principales factores que facilitan la extorsión y el crimen organizado: el anonimato operativo en líneas móviles, aplicativos digitales y servicios de conectividad. Desde una perspectiva económica del delito, la criminalidad se reduce cuando aumentan los costos de identificación, trazabilidad y sanción para el infractor, pues el delincuente evalúa la probabilidad de ser detectado frente al beneficio

esperado de su conducta ilícita (Becker, 1968)[21]. Bajo esa lógica, la presente iniciativa legislativa eleva el riesgo de detección de quienes utilizan líneas no verificadas, numeración virtual, cuentas falsas o aplicativos vinculados a identidades inexistentes, reduciendo los incentivos para emplear medios digitales en actos de extorsión, fraude, suplantación o amenaza. La presente propuesta de ley no debe entenderse como una carga aislada para las empresas operadoras, proveedores de internet o plataformas digitales, sino como una inversión obligatoria en seguridad del ecosistema digital. La experiencia comparada en prevención situacional del delito demuestra que las medidas más eficaces no siempre son las que actúan después del hecho criminal, sino aquellas que reducen la oportunidad material de cometerlo, dificultan el anonimato, incrementan la trazabilidad y eliminan espacios de impunidad tecnológica (Clarke, 1997)[22]. En ese sentido, exigir verificación biométrica, registro interoperable en tiempo real y bloqueo de accesos no validados no constituye una restricción arbitraria, sino una medida preventiva dirigida a cerrar las condiciones que hoy permiten que la extorsión se ejecute desde líneas, cuentas o aplicativos sin titularidad cierta.

El costo de implementación tecnológica será asumido principalmente por los agentes económicos que participan en el mercado de telecomunicaciones y servicios digitales, quienes ya cuentan con infraestructura de autenticación, registro de usuarios, gestión de tráfico, validación de líneas y cumplimiento regulatorio. La presente iniciativa legislativa ordena integrar y fortalecer dichos sistemas bajo estándares comunes de interoperabilidad, auditoría y trazabilidad. En materia de seguridad de la información, la literatura especializada advierte que los fallos de seguridad no derivan únicamente de problemas técnicos, sino también de incentivos económicos mal alineados, donde una empresa puede no asumir plenamente el costo social que genera una seguridad deficiente (Anderson & Moore, 2006)[23]. Por ello, imponer obligaciones legales de verificación y responsabilidad contribuye a corregir esa externalidad negativa, trasladando parte del deber de prevención a quienes habilitan la conectividad y los servicios digitales usados por terceros.

El beneficio social esperado es considerable, porque la extorsión no solo afecta a la víctima directa, sino que genera miedo colectivo, pérdida de confianza en el comercio, cierre de negocios, informalidad defensiva, costos de seguridad privada y presión adicional sobre la Policía, el Ministerio Público y el sistema judicial. La OCDE sostiene que la gestión del riesgo de seguridad digital debe integrarse en la toma de decisiones públicas y privadas, pues la confianza en el entorno digital es condición para el bienestar, la inclusión y la prosperidad económica (OCDE, 2015)[24]. Desde esa perspectiva, la presente propuesta de ley tiene impacto positivo no solo en la persecución penal, sino también en la estabilidad económica, la protección del usuario, la formalización de servicios digitales y la recuperación de confianza ciudadana frente al uso seguro de la conectividad.

[21] Becker, G. S. (1968). *Crime and punishment: An economic approach*. *Journal of Political Economy, 76*(2), 169–217.
[22] Clarke, R. V. (1997). *Situational crime prevention: Successful case studies* (2nd ed.). Harrow and Heston.
[23] Anderson, R., & Moore, T. (2006). *The economics of information security*. *Science, 314*(5799), 610–613.
[24] Organización para la Cooperación y el Desarrollo Económicos. (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. OECD Publishing.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284

El diseño normativo planteado mantiene equilibrio constitucional porque no prohíbe el acceso a telecomunicaciones ni restringe el contenido de las comunicaciones, sino que exige que el acceso a líneas móviles, internet móvil y aplicativos asociados se realice mediante identidad real, verificable y trazable. Este enfoque es compatible con los criterios modernos de identidad digital, que recomiendan procesos de prueba de identidad, autenticación y gestión del ciclo de vida de credenciales para reducir riesgos de fraude y uso indebido de servicios digitales (Grassi et al., 2017)[25]. De esta manera, el costo administrativo y tecnológico resulta razonable frente al beneficio de prevenir delitos graves, proteger a la ciudadanía, reducir la impunidad digital y fortalecer la capacidad estatal de respuesta frente a la extorsión y el crimen organizado.

VII.- VINCULACIÓN CON LA AGENDA LEGISLATIVA Y EL ACUERDO NACIONAL

La propuesta normativa se vincula de manera directa y coherente con la Agenda Legislativa del Congreso de la República, en tanto responde a una de las principales demandas ciudadanas vinculadas a la seguridad pública y a la lucha contra la criminalidad organizada, especialmente frente al incremento sostenido de delitos de extorsión que utilizan medios digitales y telecomunicaciones como principal canal de ejecución. En ese sentido, el proyecto se alinea con las prioridades legislativas orientadas a fortalecer el orden interno, modernizar los mecanismos de prevención del delito y cerrar brechas normativas que permiten el uso anónimo e impune de herramientas tecnológicas, contribuyendo a una política criminal más eficaz basada en la trazabilidad y la identificación real de los usuarios.

Asimismo, la iniciativa guarda plena concordancia con los lineamientos del Acuerdo Nacional, particularmente con las políticas de Estado orientadas a garantizar la seguridad ciudadana, el fortalecimiento del Estado de derecho, la lucha contra el crimen organizado y la promoción de un uso responsable y seguro de las tecnologías de la información. La implementación de un sistema nacional de identidad digital y control de acceso a servicios de telecomunicaciones y aplicativos digitales se inscribe en la necesidad de adaptar el marco jurídico a los nuevos escenarios de criminalidad digital, asegurando que el desarrollo tecnológico no sea aprovechado para la comisión de ilícitos, sino que se encuentre al servicio del bienestar general, la protección de la ciudadanía y la consolidación de una sociedad más segura, transparente y confiable en esa línea de ideas, la presente la iniciativa legislativa contenida en el Proyecto de Ley que se presenta, está alineada con los objetivos del **numeral** I. "Democracia y Estado de Derecho", del Acuerdo Nacional y vinculados con las Políticas de Estado en el **numeral** 7. Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana, y concordante con el **tema** 19. Medidas de seguridad ciudadana vinculadas al transporte de la Agenda Legislativa del Congreso para el período Anual de Sesiones 2021-2022, aprobada por Resolución Legislativa del Congreso N° 002-2021-2022-CR y Resolución Legislativa del Congreso N° 002-2022-2023-CR, Resolución Legislativa del Congreso Nº 002-2023-2024-CR.

[25] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines* (NIST Special Publication 800-63-3). National Institute of Standards and Technology.

Edificio Juan Santos Atahualpa Jr. Ancash y Av. Abancay s/n Ofic. 501 – Lima - Perú Tlfs: (51) 311 7777 – Anexo 7284