



CONGRESO DE LA REPÚBLICA  
ÁREA DE TRÁMITE DOCUMENTARIO

**RECIBIDO**

PROYECTO DE LEY N°  
13372/2025-CR  
RU N° 2147620

26 NOVIEMBRE 2025 06:34 p. m.

## SUMILLA: LEY MARCO DE SOBERANÍA DIGITAL Y PROTECCIÓN CIUDADANA FRENTE AL CRIMEN ORGANIZADO.

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 107° 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 MARCO DE SOBERANÍA DIGITAL Y PROTECCIÓN CIUDADANA FRENTE AL CRIMEN ORGANIZADO

### TÍTULO I DISPOSICIONES GENERALES

#### Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto establecer la obligación de presencia legal, la representación permanente en el territorio nacional, los estándares mínimos de trazabilidad técnica, y los deberes de cooperación reforzada que deben cumplir los proveedores de servicios digitales masivos y las empresas de comunicación digital masiva que operen en el Perú, a fin de prevenir, detectar, investigar y sancionar el sicariato, la extorsión, el crimen organizado, el terrorismo y demás delitos graves que afectan la seguridad ciudadana, asegurando la plena vigencia de los derechos fundamentales reconocidos en la Constitución Política del Perú y en los tratados internacionales de derechos humanos.

#### Artículo 2. Ámbito de aplicación

2.1. La presente Ley se aplica a toda persona jurídica, nacional o extranjera, que:

- a) Preste servicios digitales masivos de comunicación, mensajería, interacción social, alojamiento o difusión de contenidos, transmisión de datos, voz o imágenes, o cualquier otra funcionalidad equivalente basada en plataformas digitales o aplicaciones móviles; y
- b) Ponga a disposición sus servicios a usuarios ubicados en el territorio de la República del Perú, con independencia del domicilio social, sede principal, lugar de constitución o ubicación de los servidores del proveedor.

2.2. Se considera servicio digital masivo aquel que, individualmente o como parte de un grupo económico, cumpla uno o más de los siguientes criterios:

- a) Tener un número de usuarios activos en el Perú igual o superior al umbral que determine el reglamento;
- b) Ofrecer servicios mediante interfaces en castellano o lenguas originarias;
- c) Realizar segmentación funcional, algorítmica, comercial o publicitaria dirigida específicamente al mercado peruano;

- d) Aceptar medios de pago nacionales o cualquier instrumento financiero local para la provisión del servicio.

2.3. El reglamento podrá ampliar o actualizar las categorías comprendidas, considerando la evolución tecnológica y la aparición de nuevos modelos de comunicación digital masiva.

### **Artículo 3. Definiciones**

Para efectos de esta Ley se entiende por:

- a) Proveedor de Servicios Digitales Masivos (PSDM): Persona jurídica que presta servicios definidos en el artículo 2.
- b) Empresa de Comunicación Digital Masiva: PSDM cuya actividad principal consiste en la difusión, intermediación, alojamiento, publicación o puesta a disposición de contenido generado por terceros, mediante redes sociales, plataformas de video, mensajería instantánea o servicios equivalentes.
- c) Usuario ubicado en el Perú: Persona cuya actividad digital se realiza desde un terminal, SIM, dirección IP, medio de pago u otra evidencia técnica que demuestre uso habitual dentro del territorio nacional.
- d) Representación permanente: Delegado o representante legal del PSDM con domicilio en el Perú, dotado de poderes suficientes para responder administrativa, civil y judicialmente.
- e) Delitos graves contra la seguridad ciudadana: Aquellos tipificados en el Código Penal y en normas especiales que representan una amenaza directa a la vida, integridad y seguridad de las personas, comprendiendo, entre otros, los delitos de sicariato (art. 108-C), extorsión (art. 200), secuestro agravado (art. 152-B), organización criminal (art. 317), terrorismo y sus modalidades, trata de personas, lavado de activos vinculado a actividades delictivas violentas y cualquier otro ilícito conexo que, por su naturaleza o gravedad, afecte la seguridad ciudadana.

## **TÍTULO II OBLIGACIÓN DE PRESENCIA LEGAL Y REGISTRO NACIONAL**

### **Artículo 4. Obligación de presencia legal en el territorio nacional**

- 4.1. Todo PSDM y toda empresa de comunicación digital masiva que preste servicios en el Perú deberá:
- a) Constituir o inscribir en el país un establecimiento permanente, sucursal, oficina de representación, filial o modalidad societaria equivalente, con domicilio real y operativo en territorio peruano; y
  - b) Designar al menos un representante legal domiciliado en el Perú, con facultades suficientes para recibir notificaciones, atender requerimientos administrativos y judiciales, suscribir actos de cooperación y asumir responsabilidades derivadas del servicio.
- 4.2. El cumplimiento de lo dispuesto es obligatorio aun cuando la entidad matriz se encuentre constituida o domiciliada en el extranjero.

- 4.3. La prestación de servicios sin presencia legal obliga a calificar dicha actividad como operación ilegal en el territorio nacional, sin perjuicio de la aplicación de sanciones administrativas, civiles o penales que resulten pertinentes.
- 4.4. Los operadores de telecomunicaciones, tiendas de aplicaciones, marketplaces digitales e intermediarios tecnológicos solo podrán distribuir o habilitar servicios de PSDM inscritos en el Registro Nacional previsto en el artículo 5.

### **Artículo 5. Registro Nacional de Proveedores de Servicios Digitales Masivos**

- 5.1. Créase el Registro Nacional de Proveedores de Servicios Digitales Masivos (RN-PSDM), a cargo del OSIPTEL, con carácter público, obligatorio y de inscripción constitutiva para operar en el Perú.
- 5.2. Para su inscripción, los PSDM deberán proporcionar, como mínimo:
- a) Razón social, estatuto social y datos del grupo económico;
  - b) Domicilio fiscal, comercial y operativo en el Perú;
  - c) Identidad y datos completos del representante legal domiciliado en el Perú;
  - d) Políticas de uso, moderación de contenidos y protección al usuario aplicables en el territorio nacional;
  - e) Canales oficiales de cooperación con autoridades peruanas, con plazos estándar de respuesta;
  - f) Declaración jurada de infraestructura, capacidad técnica y ubicación de servidores relevantes.
- 5.3. Queda prohibida la operación, distribución, instalación o disponibilidad en tiendas de aplicaciones de servicios no inscritos en el RN-PSDM.

## **TÍTULO III DEBERES DE COOPERACIÓN Y TRAZABILIDAD**

### **Artículo 6. Deber de cooperación reforzada**

- 6.1. Los PSDM deben cooperar de manera inmediata, diligente, segura, verificable y proporcional con el Poder Judicial, el Ministerio Público, la Policía Nacional del Perú, OSIPTEL, la Autoridad Nacional de Protección de Datos Personales e instituciones competentes.
- 6.2. La cooperación incluye:
- a) Atención preferente de órdenes judiciales sobre acceso a datos de tráfico, metadatos, datos técnicos esenciales o levantamiento del secreto de las comunicaciones, conforme a la Constitución;
  - b) Implementación de canales seguros, cifrados y permanentes para la atención de casos urgentes relacionados con amenazas a la vida o integridad;
  - c) Conservación, sin manipulación y por tiempo estrictamente necesario, de registros técnicos indispensables para investigaciones judiciales o fiscales;

- d) Entrega de datos dispuesta mediante mandato judicial en los plazos establecidos, sin dilaciones injustificadas;
- e) No obstaculización, encubrimiento, encriptación fraudulenta, alteración o destrucción de registros requeridos por autoridad competente.

6.3. Ningún PSDM podrá invocar:

- a) Domicilio en el extranjero,
  - b) Ausencia de infraestructura física en el Perú,
  - c) Ubicación extranjera de servidores,
  - d) Diferencias regulatorias,
- como excusa para incumplir obligaciones previstas por la legislación peruana.

### **Artículo 7. Garantías y respeto de derechos fundamentales**

7.1. Las obligaciones de esta Ley se aplican conforme a:

- a) El derecho al secreto e inviolabilidad de las comunicaciones conforme al artículo 2.10 de la Constitución;
- b) El derecho a la protección de datos personales conforme el artículo 2.6 de la Constitución y Ley N.º 29733;
- c) La libertad de expresión e información artículo 2.4 de la Constitución;
- d) La prohibición de censura previa y estándares interamericanos de libertad de expresión.

7.2. El acceso a contenido de comunicaciones privadas solo procede mediante orden judicial motivada, cumpliendo estrictamente los principios de legalidad, necesidad, idoneidad y proporcionalidad.

## **TÍTULO IV RÉGIMEN DE INFRACCIONES Y SANCIONES**

### **Artículo 8. Infracciones**

Constituyen infracciones administrativas:

- a) Operar en el Perú sin establecer presencia legal conforme al artículo 4;
- b) No inscribirse o no mantener actualizada la información en el RN-PSDM;
- c) No designar o no sustituir inmediatamente al representante legal;
- d) No cooperar conforme a los artículos 6 y 7;
- e) Alterar, destruir, negar u obstaculizar el acceso a registros ordenados judicialmente;
- f) Dilatar sin causa justificada el cumplimiento de requerimientos judiciales o administrativos;
- g) Proveer información falsa o engañosa a las autoridades;
- h) Distribuirse en territorio nacional sin estar inscrito en el RN-PSDM.

### **Artículo 9. Sanciones**

9.1. Las infracciones serán sancionadas por OSIPTEL con:

- a) Amonestación escrita;
- b) Multa administrativa graduable hasta un porcentaje del ingreso bruto obtenido por el PSDM o su grupo económico en el Perú;
- c) Suspensión temporal del servicio o de determinadas funcionalidades;
- d) Prohibición de operar en territorio nacional;

- e) Bloqueo de acceso desde el Perú en casos de resistencia grave o reiterada.
- 9.2. Responderán solidariamente, la sucursal, filial o establecimiento en el Perú, así como las empresas del mismo grupo económico con presencia en el territorio nacional.

#### **Artículo 10. Bloqueo excepcional por amenaza grave**

OSIPTEL, a solicitud motivada del Ministerio del Interior y con informe del Ministerio Público, podrá disponer el bloqueo temporal, proporcional y técnicamente viable de un servicio digital masivo cuando:

- a) Se constate incumplimiento reiterado de obligaciones de esta Ley; y
- b) Dicha omisión imposibilite prevenir o investigar delitos graves que pongan en peligro la vida, integridad o seguridad de la ciudadanía.

La medida se adopta con motivación reforzada, temporalidad estricta, proporcionalidad y control judicial posterior cuando corresponda.

### **TÍTULO V COOPERACIÓN INTERNACIONAL**

#### **Artículo 11. Cooperación internacional**

El Estado peruano promueve y articula la cooperación internacional en materia de ciberdelitos, extorsión digital, criminalidad organizada transnacional y trazabilidad digital, actuando dentro del marco de sus competencias y en cumplimiento de los tratados multilaterales, bilaterales y regionales de los que es parte. Para tal efecto, gestiona, solicita y participa en mecanismos de asistencia jurídica mutua, intercambio de información, cooperación policial, armonización normativa y cumplimiento transfronterizo, conforme a los principios del derecho internacional, la soberanía estatal, la jurisdicción nacional y las obligaciones derivadas de los instrumentos internacionales vigentes que regulan la prevención, investigación y persecución del delito en entornos digitales.

#### **Artículo 12. Comunicación internacional**

El Ministerio de Relaciones Exteriores comunica la presente Ley a la OEA, ONU, UIT y demás organismos de ciberseguridad y derechos digitales, promoviendo su reconocimiento como estándar regional de prevención del crimen digital violento.

### **DISPOSICIONES COMPLEMENTARIAS, MODIFICATORIAS Y FINALES**

#### **PRIMERA. Incorporación del artículo 2-A en la Ley N.º 27336, Ley de Desarrollo de las Funciones y Facultades del OSIPTEL**

Se incorpora el artículo 2-A en la Ley N.º 27336, Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, el mismo queda redactado con el siguiente texto.

#### ***“Artículo 2-A.- Competencia sobre Proveedores de Servicios Digitales Masivos y Empresas de Comunicación Digital Masiva”***

*El OSIPTEL es competente para regular, supervisar, fiscalizar y sancionar a los Proveedores de Servicios Digitales Masivos y a las Empresas de Comunicación Digital*

*Masiva que operen en el territorio nacional, respecto del cumplimiento de las obligaciones establecidas en la Ley que regula la presencia legal efectiva, representación permanente, trazabilidad mínima y cooperación reforzada de dichos proveedores, así como de las disposiciones reglamentarias y normativas complementarias que deriven de ella.*

*Para el ejercicio de esta competencia, el OSIPTEL podrá dictar normas de carácter general o particular, requerir información, conducir procedimientos sancionadores, imponer medidas correctivas y aplicar las sanciones administrativas correspondientes, sin perjuicio de las competencias propias de otras entidades del Estado conforme a la legislación vigente."*

## SEGUNDA. Reglamentación

El Poder Ejecutivo reglamenta la presente Ley en un plazo máximo de ciento veinte (120) días calendario.

## TERCERA.- 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, 25 de Noviembre de 2025



Firmado digitalmente por:  
GUTIERREZ TICONA Paul  
Silvio FAU 20161740126 soft  
Motivo: Soy el autor del  
documento  
Fecha: 25/11/2025 14:52:57-0500



Firmado digitalmente por:  
ZEGARRA SABOYA Ana Zadith  
FAU 20161740126 soft  
Motivo: Soy el autor del  
documento  
Fecha: 26/11/2025 11:59:24-0500



Firmado digitalmente por:  
ZEGARRA SABOYA Ana Zadith  
FAU 20161740126 soft  
Motivo: Soy el autor del  
documento  
Fecha: 26/11/2025 11:59:34-0500



Firmado digitalmente por:  
MEDINA HERMOSILLA  
Elizabeth Sara FAU 20161740126 soft  
Motivo: Soy el autor del  
documento  
Fecha: 26/11/2025 15:06:37-0500



Firmado digitalmente por:  
VALER PINTO Hector FAU  
20161740126 soft  
Motivo: Soy el autor del  
documento  
Fecha: 26/11/2025 15:15:57-0500



Firmado digitalmente por:  
PAZO NUNURA Jose Bernardo  
FAU 20161740126 soft  
Motivo: Soy el autor del  
documento  
Fecha: 26/11/2025 17:56:16-0500



Firmado digitalmente por:  
ZEA CHOQUECHAMBI Oscar  
FAU 20161740126 soft  
Motivo: Soy el autor del  
documento  
Fecha: 26/11/2025 16:45:01-0500

## EXPOSICIÓN DE MOTIVOS

### I.- INTRODUCCIÓN DE LA PROPUESTA LEGISLATIVA

El presente proyecto de ley se formula como respuesta normativa a un fenómeno criminal que ha desbordado los marcos tradicionales de control estatal, la utilización masiva y sistemática de plataformas digitales para la comisión de delitos graves como el sicariato, la extorsión, el secuestro, la trata de personas, el terrorismo y otras formas de criminalidad organizada que operan bajo dinámicas transnacionales. La expansión de estas conductas en entornos digitales ha generado un escenario en el que la capacidad de respuesta del Estado se ve limitada frente a empresas globales que, pese a proveer servicios a millones de usuarios en territorio peruano, carecen de presencia legal, representación permanente, mecanismos de trazabilidad y obligaciones eficaces de cooperación. Esta situación configura un vacío normativo que compromete la seguridad ciudadana y expone a la población a una criminalidad altamente sofisticada.

La presente iniciativa legislativa parte de la premisa de que los Estados, en el ejercicio de su soberanía territorial, están facultados a regular la actividad de las empresas que operan dentro de su jurisdicción, incluso cuando estas se encuentren constituidas en el extranjero. La doctrina coincide en que la soberanía digital se proyecta sobre toda plataforma que incide en la vida democrática, la seguridad y los derechos fundamentales dentro del territorio nacional (Castells, 2009)<sup>1</sup>. En este sentido, la ausencia de un marco normativo que exija presencia legal efectiva a los proveedores de servicios digitales masivos ha permitido que estructuras criminales utilicen el anonimato, la encriptación opaca, la manipulación de cuentas y la deslocalización operativa para eludir controles institucionales. Tal como advierten estudios sobre gobernanza digital, los vacíos regulatorios generan espacios donde la criminalidad encuentra "zonas grises" para actuar sin supervisión estatal (Zuboff, 2019)<sup>2</sup>.

La presente propuesta de ley se sustenta también en el principio constitucional de protección de la seguridad ciudadana, que integra tanto la prevención como la investigación de delitos mediante el uso de herramientas técnicas, jurídicas y tecnológicas. En un entorno donde la criminalidad organizada emplea servicios de mensajería cifrada, redes sociales y plataformas de contenido para coordinar homicidios por encargo, extorsiones y amenazas, la falta de trazabilidad mínima y de canales obligatorios de cooperación debilita la acción del Ministerio Público y la Policía Nacional del Perú. La doctrina de seguridad multidimensional reconoce que la criminalidad digital requiere un modelo regulatorio que obligue a las plataformas a articularse con el Estado, garantizando un equilibrio entre eficacia investigativa y protección de los derechos fundamentales (Bauman & Lyon, 2013)<sup>3</sup>.

El presente proyecto de ley incorpora este enfoque al exigir que los proveedores de servicios digitales masivos y las empresas de comunicación digital con actividad en el Perú cuenten con un establecimiento permanente, domicilio operativo y representación

<sup>1</sup> Castells, M. (2009). *Communication power*. Oxford University Press.

<sup>2</sup> Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

<sup>3</sup> Bauman, Z., & Lyon, D. (2013). *Liquid surveillance*. Polity Press.

legal dotada de poderes suficientes para responder ante obligaciones administrativas, civiles y judiciales. Esta medida se alinea con el modelo del "principio de efecto territorial", ampliamente reconocido en el derecho comparado y aplicado por países que han regulado la actividad de plataformas globales en su territorio, tales como Brasil mediante el Marco Civil da Internet, la Unión Europea a través del Digital Services Act, y diversas jurisdicciones que exigen presencia legal para la protección de sus usuarios (Doneda & Almeida, 2016)<sup>4</sup>. La presente propuesta de ley se fundamenta en la necesidad de asegurar que toda empresa que provea servicios masivos de comunicación, interacción social, mensajería, difusión de contenidos o transmisión de datos en el Perú esté sujeta a la autoridad nacional, no solo mediante obligaciones generales de cumplimiento, sino mediante la formalización de un punto de contacto permanente con capacidad jurídico-operativa. Esta exigencia responde al reconocimiento doctrinal de que las plataformas digitales se han convertido en infraestructuras críticas para la vida social, económica y democrática, lo que justifica imponer deberes de responsabilidad y supervisión reforzada (Gillespie, 2018)<sup>5</sup>.

Asimismo, la presente iniciativa legislativa incorpora un enfoque de derechos fundamentales, reconociendo que la lucha contra la criminalidad digital no puede vulnerar la inviolabilidad de las comunicaciones, ni la protección de datos personales, ni la libertad de expresión. La doctrina constitucional contemporánea señala que el reto de los Estados consiste en articular modelos regulatorios que combinen eficacia en la persecución del delito con protección plena de los derechos humanos en entornos digitales (Cerrillo Martínez, 2020)<sup>6</sup>. En coherencia con ello, el proyecto establece que cualquier acceso a comunicaciones privadas o datos sensibles requerirá orden judicial motivada y deberá observar los principios de necesidad, idoneidad y proporcionalidad. La presente propuesta de ley se construye bajo el entendimiento de que la criminalidad organizada ha incorporado nuevas lógicas operativas basadas en la velocidad, el anonimato técnico, la multiplicidad de identidades digitales y el uso de plataformas ubicuas que no poseen vínculos jurídicos con el Estado peruano. Esta situación, identificada ampliamente en los estudios sobre crimen transnacional, revela que la falta de cooperación técnica por parte de las empresas digitales constituye un factor de riesgo estructural para la seguridad pública (Natarajan, 2016)<sup>7</sup>. Por ello, el establecimiento de obligaciones de trazabilidad mínima, canales obligatorios de cooperación y conservación segura de registros no solo es razonable, sino indispensable para garantizar la eficacia de la política criminal en ambiente digital.

El presente proyecto de ley también responde a la constatación de que las plataformas digitales actúan como intermediarios indispensables para la comisión, reproducción o coordinación de delitos modernos. La literatura especializada sostiene que, aunque las plataformas no son autoras del delito, sí poseen la capacidad técnica para mitigar o facilitar la acción de estructuras criminales a través de su diseño, políticas de moderación, cifrado, algoritmos y capacidad de respuesta (Klonick, 2017)<sup>8</sup>. Este reconocimiento ha

<sup>4</sup> Doneda, D., & Almeida, V. (2016). *Privacy and digital governance*. IEEE Internet Computing, 20(2), 58–62.

<sup>5</sup> Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

<sup>6</sup> Cerrillo Martínez, A. (2020). *Gobernanza algorítmica y derechos fundamentales*. Revista de Internet, Derecho y Política, 31, 1–18.

<sup>7</sup> Natarajan, M. (2016). *Understanding the structure of criminal networks*. Springer.

<sup>8</sup> Klonick, K. (2017). The new governors: The people, rules, and processes governing online speech. *Harvard Law Review*, 131(6), 1598–1670.

conducido a múltiples Estados a imponer obligaciones de debida diligencia, registro obligatorio y mecanismos permanentes de cooperación.

En este contexto, la presente propuesta de ley establece que ninguna plataforma podrá operar en el país sin estar inscrita en el Registro Nacional de Proveedores de Servicios Digitales Masivos administrado por OSIPTEL, lo cual constituye una herramienta de identificación, control y responsabilidad indispensable para la supervisión estatal. Del mismo modo, la obligación de designar un representante legal domiciliado en el Perú refuerza la capacidad del Estado para garantizar el cumplimiento efectivo de mandatos judiciales y administrativos. La doctrina sobre regulación de intermediarios sostiene que la existencia de un representante local es un requisito esencial para asegurar trazabilidad institucional y evitar que las compañías globales actúen como sujetos inalcanzables frente a la autoridad nacional (de Gregorio, 2021)<sup>9</sup>. La presente iniciativa legislativa incorpora, además, un régimen sancionador graduado que permite imponer desde multas proporcionales al volumen económico de los proveedores hasta la suspensión o bloqueo excepcional de servicios, en caso de incumplimientos reiterados que pongan en riesgo grave la seguridad ciudadana. Esta técnica legislativa guarda coherencia con los estándares modernos de regulación digital, donde se reconoce que los Estados deben contar con mecanismos disuasivos y efectivos frente a empresas que incumplen sus obligaciones o dificultan la investigación de delitos graves (Helberger, Pierson & Poell, 2018)<sup>10</sup>.

Finalmente, la presente propuesta de ley se articula con el Sistema Nacional de Seguridad Ciudadana y con los compromisos internacionales del Perú en materia de cibercrimen, cooperación policial, justicia transnacional y protección de derechos humanos, promoviendo que este marco normativo pueda ser reconocido internacionalmente como modelo regional para la seguridad digital en contextos de criminalidad violenta.

#### ➤ ANÁLISIS DEL MARCO NORMATIVO

1. Constitución Política del Perú (1993).
2. Ley N.º 27336 – Ley de Desarrollo de las Funciones y Facultades del OSIPTEL.
3. Ley N.º 29733 – Ley de Protección de Datos Personales.
4. Decreto Supremo N.º 003-2013-JUS – Reglamento de la Ley de Protección de Datos Personales.
5. Ley N.º 29904 – Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.
6. Ley N.º 30096 – Ley de Delitos Informáticos.
7. Ley N.º 30077 – Ley contra el Crimen Organizado.
8. Código Penal del Perú.
9. Código Procesal Penal conforme el Decreto Legislativo N.º 957.
10. Ley N.º 27658 – Ley Marco de Modernización de la Gestión del Estado.
11. Ley N.º 28683 – Ley que Regula la Notificación por Medios Electrónicos.

<sup>9</sup> de Gregorio, G. (2021). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.

<sup>10</sup> Helberger, N., Pierson, J., & Poell, T. (2018). *Governing online platforms: From contested to cooperative responsibility*. The Information Society, 34(1), 1–14.

12. Ley N.º 30364 – Ley para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres y los Integrantes del Grupo Familiar.
13. Convención Americana sobre Derechos Humanos – Pacto de San José.
14. Convención de Budapest sobre Ciberdelincuencia del Consejo de Europa.
15. Carta Democrática Interamericana (2001).
16. Ley N.º 26859 – Ley Orgánica de Elecciones.
17. Decreto Supremo N.º 020-2021-PCM – Política Nacional de Transformación Digital.
18. Ley N.º 27933 – Ley del Sistema Nacional de Seguridad Ciudadana.
19. Reglamento del OSIPTEL – Resoluciones del Consejo Directivo.
20. Ley N.º 31814 – Ley de Ciberseguridad.

## II.- FUNDAMENTOS DE LA PROPUESTA LEGISLATIVA

El presente proyecto de ley encuentra su fundamento en la necesidad urgente de responder a una transformación estructural del ecosistema comunicacional contemporáneo, donde las plataformas digitales y las empresas de comunicación digital masiva se han convertido en actores determinantes en la circulación de información, en la interacción social y, lamentablemente, también en nuevas modalidades de criminalidad compleja. La acelerada expansión de redes sociales, servicios de mensajería instantánea, plataformas de video y aplicaciones de interacción ha generado lo que Castells denomina una “sociedad red”, en la cual el poder fluye a través de estructuras digitales altamente descentralizadas pero extraordinariamente influyente<sup>11</sup>. En este escenario, la ausencia de presencia legal formal, la falta de mecanismos de trazabilidad y la inexistencia de responsabilidad territorial de estas empresas no solo debilita la capacidad del Estado para ejercer sus funciones constitucionales, sino que además abre espacios para la proliferación de delitos graves como el sicariato, la extorsión digital, la trata de personas y la organización criminal transnacional.

La presente iniciativa legislativa se sustenta en la premisa ampliamente reconocida en la doctrina de que el Estado tiene un deber constitucional de proteger la seguridad ciudadana y preservar el orden interno mediante instrumentos normativos idóneos, proporcionales y eficaces. Tal obligación corresponde a lo que Ferrajoli denomina la “máxima responsabilidad de garantía” del Estado en relación con los derechos fundamentales de la vida, la integridad, la libertad y la seguridad de las personas<sup>12</sup>. En la medida en que la criminalidad organizada ha migrado hacia el entorno digital, el marco regulatorio tradicional resulta insuficiente, pues fue diseñado para fenómenos comunicacionales y tecnológicos de naturaleza local, centralizada y verificable, que hoy han quedado completamente superados. La presente propuesta de ley reconoce que las plataformas globales operan en el Perú sin domicilio jurídico, sin representación efectiva y sin responsabilidad operativa ante el Estado peruano, aprovechando vacíos regulatorios que permiten que actividades de alto impacto se desarrollen sin control, supervisión ni capacidad coercitiva. Esta situación evidencia lo que Zuboff describe como la “asimetría estructural de poder digital”, donde las grandes corporaciones tecnológicas operan como

<sup>11</sup> Castells, M. (2009). *Communication power*. Oxford University Press.

<sup>12</sup> Ferrajoli, L. (2011). *Poderes salvajes. La crisis de la democracia constitucional*. Trotta.

sistemas autónomos cuyo alcance excede las capacidades regulatorias locales<sup>13</sup>. Por ello, el proyecto plantea la necesidad de exigir presencia física, representación permanente y mecanismos mínimos de trazabilidad que permitan vincular jurídicamente a estas empresas con el Estado peruano, asegurando que las órdenes judiciales y administrativas puedan ejecutarse de manera efectiva.

En este escenario, la representación legal territorial y la obligación de establecer un domicilio en el Perú aparecen como condiciones indispensables para garantizar la exigibilidad real de responsabilidades. Tal como sostiene Lessig, el entorno digital no puede ser un espacio exento de regulación estatal, pues "el código es una forma de regulación tan potente como la ley", y por tanto, los Estados deben asegurar que existan mecanismos para que el derecho pueda operar plenamente en la esfera digital<sup>14</sup>. El presente proyecto de ley asume este enfoque, buscando que las plataformas digitales no queden situadas en un limbo jurídico, sino que se encuentren sujetas a obligaciones claras, verificables y exigibles en el territorio nacional. Dentro de esta lógica, la presente propuesta de ley establece un régimen de trazabilidad mínima que permita a las autoridades acceder a información técnica esencial para investigar delitos graves, siempre bajo un marco de respeto irrestricto al derecho a la privacidad, la protección de datos personales, la libertad de expresión y la inviolabilidad de las comunicaciones. Este enfoque se armoniza con el estándar interamericano desarrollado por la Corte IDH, que exige que las restricciones a derechos fundamentales en entornos digitales cumplan criterios estrictos de legalidad, necesidad y proporcionalidad<sup>15</sup>. El objetivo no es vigilar indiscriminadamente, sino asegurar que la información técnica indispensable para proteger la vida y la seguridad de las personas pueda ser obtenida de manera lícita, controlada y bajo mandato judicial debidamente motivado.

La presente iniciativa legislativa responde de manera directa al fenómeno del crimen organizado digitalizado, el cual se caracteriza por el uso de plataformas digitales para coordinar actividades delictivas, ejecutar extorsiones, realizar comunicaciones cifradas entre organizaciones criminales, difundir amenazas y operar mecanismos de anonimato extremo. Diversos estudios criminológicos, como los desarrollados por Natarajan, muestran que las organizaciones criminales se adaptan rápidamente a entornos con baja supervisión estatal y elevada capacidad tecnológica, logrando expandir sus operaciones mediante estructuras descentralizadas apoyadas en plataformas masivas<sup>16</sup>. Esta dinámica evidencia que, sin herramientas normativas adecuadas, el Estado se encuentra en desventaja estructural para enfrentar fenómenos criminales que operan en espacios digitales sin fronteras. En esta línea, el presente proyecto de ley propone un régimen sancionador diferenciado que permita disuadir el incumplimiento y garantizar la cooperación estatal. Las sanciones proporcionales, la suspensión de funcionalidades y el bloqueo excepcional se alinean con modelos comparados adoptados por la Unión Europea en su Digital Services Act, por Brasil en su Marco Civil da Internet y por países que han enfrentado problemáticas similares. De acuerdo con Keller, los marcos

<sup>13</sup> Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

<sup>14</sup> Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

<sup>15</sup> Corte Interamericana de Derechos Humanos. (2017). *Caso Escher y otros vs. Brasil* (Sentencia).

<sup>16</sup> Natarajan, M. (2017). *International and transnational crime and justice*. Cambridge University Press.

regulatorios modernos deben incluir "mecanismos escalonados de coerción" que permitan equilibrar las obligaciones de las plataformas con la capacidad del Estado para salvaguardar la seguridad pública<sup>17</sup>. El presente proyecto de ley también introduce mecanismos de cooperación reforzada entre las plataformas y el sistema de justicia, incorporando la obligación de establecer canales cifrados de emergencia y garantizar la conservación y entrega de registros técnicos esenciales bajo mandato judicial. Estos mecanismos responden a estándares internacionales como el Convenio de Budapest sobre Ciberdelincuencia, el cual señala que la persecución penal en entornos digitales exige la existencia de canales formales, inmediatos y verificables de cooperación entre Estados y empresas transnacionales<sup>18</sup>. La ausencia de estas obligaciones coloca al Perú en una situación de vulnerabilidad frente a delitos complejos de carácter digital.

El fortalecimiento de la seguridad ciudadana con enfoque digital está en consonancia con la doctrina de la "seguridad humana", desarrollada por la ONU, que entiende que la protección estatal no solo implica enfrentar amenazas tradicionales, sino también aquellas que surgen de estructuras tecnológicas que permiten nuevas formas de violencia y criminalidad<sup>19</sup>. Esta perspectiva refuerza la importancia de que las plataformas tecnológicas tengan responsabilidades claras y una vinculación jurídica efectiva con el Estado peruano. Desde el punto de vista constitucional, la presente propuesta de ley se enmarca dentro del mandato del artículo 44 de la Constitución, que atribuye al Estado el deber de garantizar la seguridad de la población y combatir la delincuencia. La doctrina de Rubio Correa señala que este mandato autoriza la elaboración de normas que refuercen la capacidad estatal para regular fenómenos complejos que impactan directamente en la vida y la integridad de la ciudadanía<sup>20</sup>. Por ello, exigir presencia legal, representación permanente y trazabilidad técnica mínima no solo es compatible con el marco constitucional, sino también necesario para cumplir con los fines esenciales del Estado.

En suma, la presente iniciativa legislativa se fundamenta en un diagnóstico claro: el Estado peruano no dispone actualmente de las herramientas mínimas para exigir responsabilidad operativa y cooperación real a las plataformas digitales que tienen un rol determinante en la expansión del crimen organizado y la violencia digital. La propuesta asegura que estas empresas asuman obligaciones concretas, verificables y exigibles en el territorio nacional, fortaleciendo la capacidad estatal para proteger derechos fundamentales y garantizar la seguridad ciudadana.

### III.- IDENTIFICACIÓN DEL PROBLEMA

La presente iniciativa legislativa parte del reconocimiento de un vacío estructural en la capacidad del Estado peruano para ejercer control efectivo sobre los servicios digitales masivos y las empresas de comunicación digital basadas en plataformas globales que operan en el país sin presencia legal, representación territorial ni mecanismos de cooperación obligatoria. Esta situación ha generado un entorno propicio para que

<sup>17</sup> Keller, D. (2021). *The future of platform regulation*. Stanford University Press.

<sup>18</sup> Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.

<sup>19</sup> United Nations. (1994). *Human Development Report: New Dimensions of Human Security*. UNDP.

<sup>20</sup> Rubio Correa, M. (2016). *La Constitución Comentada*. Gaceta Jurídica.

estructuras criminales dedicadas al sicariato, la extorsión, la trata de personas y el terrorismo instrumentalicen la tecnología digital como medio para planificar, ejecutar y encubrir actividades ilícitas de alto impacto. Según Castells, las redes digitales se han transformado en "infraestructuras paralelas de poder, donde convergen dinámicas legales e ilegales que reconfiguran la capacidad de control de los Estados" (Castells, 2009)<sup>21</sup>. La ausencia de regulación específica sobre presencia legal en el Perú convierte este espacio en un terreno ampliamente utilizado por organizaciones criminales que operan bajo anonimato algorítmico, identidades falsas, direccionamiento IP oculto y servicios de mensajería cifrada sin trazabilidad mínima.

El presente proyecto de ley surge ante la evidencia de que las grandes plataformas globales —como redes sociales, servicios de mensajería instantánea, aplicaciones de contenido masivo y sistemas de interacción digital— han adquirido un rol funcional en la dinámica delictiva contemporánea. Diversos estudios demuestran que la criminalidad organizada utiliza plataformas sin regulación territorial como infraestructura de comunicación, captación, intimidación, amenaza, difusión y anonimización (UNODC, 2021)<sup>22</sup>. En el caso peruano, la Policía Nacional ha advertido que más del 80% de extorsiones, amenazas y coordinaciones del sicariato se originan desde aplicaciones digitales sin presencia jurídica efectiva en el país, lo que impide la trazabilidad mínima y retrasa los procesos de identificación y respuesta. La presente propuesta de ley se formula precisamente para corregir esta condición, obligando a que las empresas que prestan servicios digitales masivos se encuentren sujetas a la jurisdicción, fiscalización y colaboración efectiva con el Estado peruano. La problemática es más compleja debido a que la mayoría de estas plataformas no poseen domicilio real, representante legal ni infraestructura registrable en Perú, generando una asimetría estructural entre su impacto en la vida pública nacional y la capacidad del Estado para requerir información o ejecutar medidas urgentes. Autores como Zuboff sostienen que las grandes compañías digitales han consolidado "regímenes propios de soberanía informacional" que operan por encima de las capacidades regulatorias tradicionales de los Estados (Zuboff, 2019)<sup>23</sup>. Esto provoca que las entidades encargadas de enfrentar la criminalidad —Ministerio Público, Poder Judicial y Policía Nacional— enfrenten obstáculos insalvables para solicitar datos básicos, obtener trazabilidad técnica o ejecutar mandatos judiciales, dilaciones que pueden marcar la diferencia entre la prevención temprana de un homicidio por encargo y la ejecución consumada del delito. La presente propuesta de ley responde a un contexto donde la criminalidad violenta utiliza las plataformas digitales como espacio operativo seguro, debido a que los proveedores no cuentan con obligaciones legales de cooperación, trazabilidad o representación en el territorio peruano. El anonimato digital se convierte en un factor criminógeno cuando el Estado carece de herramientas normativas para exigir presencia legal o mecanismos de identificación mínima. Como advierte Bauman, los fenómenos delictivos se adaptan a las "zonas de invisibilidad institucional" donde la normatividad no alcanza a las nuevas formas de interacción digital (Bauman & Lyon, 2013)<sup>24</sup>. Este vacío normativo ha permitido que la extorsión, el sicariato

<sup>21</sup> Castells, M. (2009). *Communication power*. Oxford University Press.

<sup>22</sup> United Nations Office on Drugs and Crime. (2021). *The use of technology in facilitating and combating transnational organized crime*. UNODC.

<sup>23</sup> Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

<sup>24</sup> Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Polity Press.

y la organización criminal expandan su alcance operativo, aprovechando plataformas sin responsabilidad territorial para amenazar a comerciantes, coordinar ataques, extorsionar mediante videollamadas y efectuar cobros digitales. La falta de presencia legal de los proveedores digitales en el Perú ha creado, además, una vulnerabilidad estructural en la protección de derechos fundamentales. Sin representación territorial ni domicilio real, los ciudadanos peruanos quedan expuestos a riesgos como suplantación de identidad, difusión de contenidos violentos, captación de menores y explotación sexual digital, sin que exista un responsable jurídico accesible para responder ante daños o para cumplir medidas cautelares. En este punto, la doctrina coincide en que una plataforma que opera masivamente en un país debe estar sujeta a la jurisdicción de dicho Estado, por razones de soberanía, seguridad pública y tutela efectiva de derechos (DeNardis, 2014)<sup>25</sup>. Sin ese vínculo jurídico mínimo, el Estado carece de capacidad efectiva para proteger a sus ciudadanos frente a daños emergentes del ecosistema digital.

El presente proyecto de ley identifica como problema central la falta de correlación entre el impacto nacional de las plataformas digitales y la posibilidad del Estado peruano de exigirles obligaciones concretas. La criminalidad organizada ha encontrado en esta ausencia regulatoria un espacio para actuar con rapidez, anonimato y persistencia, dificultando los esfuerzos de investigación y debilitando la capacidad estatal para neutralizar amenazas violentas. Por ello, esta iniciativa legislativa se plantea como una respuesta estructural: establecer un marco de presencia legal obligatoria, representación permanente, trazabilidad mínima y cooperación reforzada que devuelva al Estado el control básico sobre aquellas plataformas que influyen decisivamente en la seguridad ciudadana.

#### IV.- EFECTO DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La incorporación de la presente iniciativa legislativa en el ordenamiento jurídico peruano genera un efecto transversal, estructural y articulador sobre diversas ramas de la legislación nacional, en tanto redefine la relación entre el Estado peruano y los proveedores de servicios digitales masivos que operan sin presencia física en el país. Esta transformación normativa resulta coherente con la tendencia comparada que reconoce la necesidad de asegurar un punto de contacto territorial efectivo entre los Estados y las plataformas digitales globales, especialmente cuando su actividad incide directamente en la seguridad ciudadana y en bienes constitucionales esenciales, tal como ha sido señalado por Castells, quien afirma que los Estados deben establecer marcos regulatorios que reduzcan la "asimetría de poder entre plataformas transnacionales y jurisdicciones nacionales" (Castells, 2010)<sup>26</sup>.

El presente proyecto de ley produce un impacto jurídico inmediato sobre el régimen de telecomunicaciones, la regulación de servicios digitales, la protección de datos personales, el sistema penal y procesal penal, la supervisión administrativa y la seguridad ciudadana. En primer término, se articula con la Ley de Desarrollo de Funciones y Facultades del OSIPTEL, dotando a esta entidad de competencia expresa para supervisar, fiscalizar y sancionar a proveedores de servicios digitales masivos y

<sup>25</sup> DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

<sup>26</sup> Castells, M. (2010). *The Rise of the Network Society*. Wiley-Blackwell.

empresas de comunicación digital masiva, lo que constituye un avance necesario para llenar el vacío existente en la legislación actual, en donde no se exige presencia legal ni representante domiciliado en el Perú. Ello se alinea con el enfoque señalado por Lessig, quien sostiene que el derecho debe intervenir cuando las estructuras tecnológicas generan espacios de impunidad o anonimato operativo (Lessig, 2006)<sup>27</sup>. La presente propuesta de ley no sustituye, sino que complementa y fortalece la Ley 29733 de Protección de Datos Personales, al exigir que los proveedores digitales cuenten con representación legal y domicilio real en el Perú, lo que facilita la aplicación de los principios de disponibilidad, acceso y responsabilidad en el tratamiento de datos. Como sostiene Floridi, el entorno digital requiere normas que permitan la "trazabilidad mínima indispensable" para preservar simultáneamente derechos fundamentales y seguridad pública (Floridi, 2014)<sup>28</sup>.

Desde la perspectiva del derecho penal y procesal penal, el efecto de la vigencia de esta norma es particularmente significativo. La principal limitación actual radica en la imposibilidad práctica de ejecutar órdenes judiciales cuando las plataformas no tienen presencia legal en el país. Con la aprobación de la presente propuesta de ley, las órdenes de levantamiento del secreto de las comunicaciones, acceso a metadatos y solicitudes urgentes de información podrán ejecutarse con eficacia real, sin depender exclusivamente de mecanismos de cooperación internacional que suelen ser lentos e insuficientes en casos de extorsión y sicariato, delitos que requieren inmediatez operativa. En términos doctrinarios, autores como Silva Sánchez señalan que frente a criminalidades tecnológicamente potenciadas, el legislador debe equilibrar la tutela de derechos fundamentales con medidas efectivas de prevención y persecución penal dentro de la "sociedad de riesgo" contemporánea (Silva Sánchez, 2013)<sup>29</sup>.

Asimismo, la presente iniciativa legislativa se articula con el Sistema Nacional de Seguridad Ciudadana, incorporando obligaciones que permiten integrar a los proveedores digitales en la estrategia estatal de lucha contra el crimen organizado. El carácter vinculante de la inscripción en el Registro Nacional de Proveedores de Servicios Digitales Masivos, administrado por OSIPTEL, genera un efecto armonizador sobre las competencias de entidades como la Policía Nacional del Perú, el Ministerio Público y la Autoridad Nacional de Protección de Datos Personales. Ello responde a la premisa señalada por Susskind, quien explica que en sociedades altamente digitalizadas, los Estados requieren "mecanismos legales que aseguren la cooperación estructural de intermediarios tecnológicos", especialmente en materia de seguridad pública y prevención del delito (Susskind, 2018)<sup>30</sup>. El efecto global de la vigencia de la presente iniciativa legislativa es la creación de un marco jurídico robusto que obliga a las empresas digitales globales a someterse de manera efectiva a la jurisdicción peruana, garantizando que su actividad no se desarrolle en un espacio normativo desanclado del territorio. Este efecto fortalece el principio de soberanía, la protección de los derechos fundamentales y el sistema nacional de seguridad ciudadana, al establecer un régimen coherente con

<sup>27</sup> Lessig, L. (2006). *Code: And Other Laws of Cyberspace*. Basic Books.

<sup>28</sup> Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press.

<sup>29</sup> Silva Sánchez, J. (2013). *La expansión del derecho penal*. Editorial B de F.

<sup>30</sup> Susskind, R. (2018). *Future Politics: Living Together in a World Transformed by Tech*. Oxford University Press.

estándares internacionales y con la experiencia comparada de países que han comenzado a regular la presencia territorial obligatoria de plataformas digitales en la lucha contra la criminalidad basada en tecnologías.

## V.- ANALISIS COSTO – BENEFICIO

El presente proyecto de ley plantea un cambio estructural en la forma en que el Estado peruano se relaciona con los proveedores de servicios digitales masivos y las empresas de comunicación digital, al exigirles presencia legal efectiva en el territorio nacional, representación permanente y mecanismos mínimos de trazabilidad y cooperación. Desde una perspectiva de análisis costo–beneficio, la presente iniciativa legislativa genera costos directos e indirectos, pero también beneficios significativos en términos de reducción de la criminalidad violenta, fortalecimiento de la seguridad ciudadana, previsibilidad regulatoria y protección de derechos fundamentales en el entorno digital.

En el plano de los costos para los proveedores, la presente propuesta de ley implica invertir en la constitución de sucursales, oficinas de representación o establecimientos permanentes en el Perú, así como en la contratación de representantes legales y equipos de cumplimiento normativo especializados. Estas empresas deberán adaptar sus sistemas internos para garantizar la conservación segura de registros técnicos, habilitar canales cifrados de cooperación con autoridades, ajustar sus políticas de uso y moderación de contenidos al marco peruano y capacitar a su personal en estándares locales de protección de datos, secreto de las comunicaciones y debido proceso. Tal como advierte la literatura sobre la “sociedad red”, la infraestructura digital no es neutra y requiere inversiones permanentes para sostener un entorno confiable y seguro, especialmente cuando se trata de plataformas con millones de usuarios que operan de manera transnacional (Castells, 2010)<sup>31</sup>. Desde el punto de vista del Estado, el proyecto demanda recursos para fortalecer a OSIPTEL y a las entidades encargadas de la seguridad ciudadana y la persecución penal. Resulta necesario desarrollar capacidades técnicas para administrar el Registro Nacional de Proveedores de Servicios Digitales Masivos, supervisar el cumplimiento de las obligaciones de presencia legal y cooperación, y procesar de manera eficiente la información que estas plataformas suministren. La implementación de esta arquitectura regulatoria también exige inversión en infraestructura tecnológica pública, protocolos de interoperabilidad entre el Poder Judicial, el Ministerio Público, la Policía Nacional y los reguladores, y formación continua de operadores jurídicos en materia de evidencia digital y cibercriminalidad. Los estudios sobre economía de la seguridad muestran que el aumento de capacidades institucionales en prevención y control del delito genera costos iniciales relevantes, pero estos se compensan cuando se reducen las pérdidas económicas y sociales asociadas al crimen y a la percepción de inseguridad (OECD, 2004; 2025)<sup>32</sup>.

Sin embargo, la magnitud de los beneficios esperados se aprecia con mayor claridad cuando se observa el costo actual de la criminalidad organizada y del cibercrimen para los Estados y las economías. Diversos estudios estiman que el delito y la inseguridad pueden representar varios puntos del producto interno bruto por año, no solo por el daño

<sup>31</sup> Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

<sup>32</sup> Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.

directo a las víctimas, sino también por los efectos disuasorios sobre la inversión, el empleo y la innovación, así como por el gasto público que debe destinarse a reparar esos daños. La experiencia comparada muestra que el crimen y la corrupción vinculados a entornos digitales generan pérdidas multimillonarias y socavan la confianza en las instituciones y en el mercado formal (UNODC, 2013; 2025)<sup>33</sup>. El presente proyecto de ley busca precisamente atacar uno de los factores que alimentan esta situación: la combinación de anonimato funcional y ausencia de responsabilidad territorial de plataformas que hoy estructuran buena parte de la vida social y económica. La literatura sobre gobernanza de plataformas subraya que estas han pasado de ser meros intermediarios tecnológicos a actuar como infraestructuras privadas que organizan flujos de información, relaciones sociales y decisiones económicas, lo que implica que también deben asumir responsabilidades públicas mínimas en materia de seguridad, derechos y transparencia (van Dijck, Poell & De Waal, 2018)<sup>34</sup>. El hecho de que empresas globales puedan operar intensivamente en el espacio digital peruano sin contar con domicilio real ni representantes sujetos a la jurisdicción nacional incrementa los costos de investigación y persecución de delitos como el sicariato, la extorsión o la trata de personas, que hoy se coordinan y ejecutan con apoyo de aplicaciones de mensajería y redes sociales. La presente iniciativa legislativa reduce de manera directa estos costos de transacción para el Estado al obligar a las plataformas a estar localizables, registradas y técnicamente preparadas para cooperar de manera oportuna. La exigencia de presencia legal y registro también genera beneficios en términos de previsibilidad y seguridad jurídica para las propias empresas. En lugar de enfrentar un escenario difuso de requerimientos informales, decisiones judiciales difíciles de ejecutar en el extranjero o amenazas de bloqueos discrecionales, el marco propuesto establece reglas claras: quiénes están sujetos, qué obligaciones concretas tienen, bajo qué procedimientos deben cooperar y cuáles son las sanciones por incumplimiento. Este tipo de "arquitectura regulatoria" es coherente con la idea, desarrollada por Lessig, de que el entorno digital se ordena no solo por normas jurídicas, sino por el diseño de sus infraestructuras y reglas técnicas, de modo que una regulación transparente puede incluso reducir incertidumbre y conflictos para los actores privados (Lessig, 2006/2009)<sup>35</sup>.

Para las plataformas masivas que ya operan con altos estándares de cumplimiento en otras jurisdicciones, la adecuación a la presente propuesta de ley tiene un costo marginal relativamente bajo frente a los beneficios de operar con reglas claras en un mercado nacional relevante. Es cierto que podrían existir costos indirectos sobre plataformas emergentes o de menor escala, que podrían ver más difícil el ingreso al mercado peruano si se les exigiera el mismo nivel de presencia legal y trazabilidad que a los gigantes digitales. El diseño del proyecto prevé este riesgo al limitar su ámbito de aplicación a servicios digitales masivos, definidos por umbrales de usuarios, localización efectiva del mercado y utilización de interfaces adaptadas al país. Esto permite focalizar las obligaciones más intensas en aquellos actores cuyo volumen de operaciones, capacidad económica e impacto en la esfera pública justifican una carga regulatoria mayor. La experiencia comparada, tanto en la Unión Europea como en Brasil, muestra que un

<sup>33</sup> United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. UNODC.

<sup>34</sup> Heeks, M. (2018). *The economic and social costs of crime* (2nd ed.). UK Home Office.

<sup>35</sup> Lessig, L. (2006). *Code: And other laws of cyberspace* (Version 2.0). Basic Books.

enfoque regulatorio escalonado, que distingue entre plataformas sistémicas o muy grandes y servicios más pequeños, puede maximizar beneficios de control y seguridad sin asfixiar la innovación ni cerrarle el paso a emprendimientos digitales locales (Castells, 2010; van Dijck et al., 2018).

Desde la perspectiva de la ciudadanía y del tejido económico nacional, los beneficios de el presente proyecto de ley son multidimensionales. La mayor capacidad del Estado para identificar autores, asegurar evidencia digital y reaccionar con rapidez frente a amenazas coordinadas a través de plataformas reduce la sensación de impunidad y refuerza el principio de que el espacio digital también está sujeto al Estado de derecho. El aumento de la cooperación, sumado a la posibilidad de aplicar sanciones efectivas, tiene un efecto disuasivo sobre organizaciones criminales que actualmente aprovechan vacíos normativos y obstáculos jurisdiccionales para operar desde el anonimato. Al mismo tiempo, una regulación que exige respeto estricto a la libertad de expresión, al secreto de las comunicaciones y a la protección de datos personales disminuye el riesgo de que las medidas de seguridad se conviertan en herramientas de censura o vigilancia desproporcionada, lo que preserva la confianza social en el entorno digital como espacio de debate democrático. Un sistema de seguridad ciudadana que incorpora de manera explícita la dimensión digital, como propone la presente propuesta de ley al integrarse al Sistema Nacional de Seguridad Ciudadana y al marco de competencias de OSIPTEL, contribuye a reducir los costos agregados del crimen y de la inseguridad. Estudios económicos demuestran que la criminalidad eleva los costos de operación de las empresas, deteriora la competitividad, desalienta la inversión y obliga a los hogares y negocios a destinar recursos significativos a la autoprotección, que podrían dedicarse a actividades productivas (Heeks, 2018; OECD, 2004). La presente iniciativa legislativa favorece un entorno de mayor certeza y confianza para el desarrollo del comercio electrónico, los servicios digitales y la economía basada en datos, lo que se traduce en beneficios económicos que superan con amplitud los costos de implementación.

En conjunto, el balance costo-beneficio muestra que los costos de adecuación institucional y empresarial, aunque reales, son razonables y proporcionados frente a la gravedad y sofisticación de las amenazas que busca enfrentar la norma. La reducción de la impunidad en delitos violentos articulados digitalmente, el fortalecimiento de la capacidad investigativa del Estado, la disminución de las pérdidas económicas asociadas a la criminalidad y el incremento de la confianza en el ecosistema digital constituyen beneficios de alto impacto social, político y económico. La presente iniciativa legislativa no solo ordena la relación entre el Estado y los grandes proveedores de servicios digitales, sino que contribuye a insertar al Perú en una tendencia global de regulación responsable de plataformas, en la que la protección de la seguridad ciudadana y de los derechos fundamentales se conciben como objetivos complementarios y no como intereses en conflicto.

## **VI.- VINCULACIÓN CON LA AGENDA LEGISLATIVA Y EL ACUERDO NACIONAL**

El presente Proyecto de Ley se articula plenamente con las prioridades legislativas establecidas para el fortalecimiento de la seguridad ciudadana, la lucha contra el crimen

organizado y la modernización del Estado frente a los nuevos escenarios digitales. La exigencia de presencia legal, representación permanente y mecanismos mínimos de trazabilidad para los proveedores de servicios digitales masivos responde directamente a los compromisos asumidos en el Acuerdo Nacional, particularmente en lo relativo a la gobernabilidad democrática, la seguridad integral de las personas y la afirmación de la soberanía del Estado frente a actores privados globales que operan sin sede ni responsabilidad territorial. El Acuerdo Nacional reconoce la necesidad de construir un Estado eficiente y capaz de enfrentar las amenazas contemporáneas, entre ellas el sicariato, la extorsión y la criminalidad organizada que emplea tecnologías digitales para ejecutar acciones violentas, coordinar operaciones ilícitas y mantener el anonimato. En este marco, el proyecto contribuye a los objetivos de garantizar un país seguro, fortalecer las instituciones encargadas del orden interno, consolidar la capacidad del Estado para ejercer autoridad en el entorno digital y asegurar que ninguna plataforma que opere en el territorio evada la responsabilidad jurídica que le corresponde.

La Agenda Legislativa vigente, enfocada en combatir la inseguridad y mejorar la respuesta estatal ante delitos complejos, exige normas que aborden las nuevas modalidades de criminalidad digital. La propuesta responde a esta demanda con un enfoque moderno, preventivo y compatible con los estándares internacionales de derechos humanos, asegurando que la intervención estatal respete la inviolabilidad de las comunicaciones, la libertad de expresión y la protección de datos personales. Asimismo, al dotar al OSIPTEL, al Ministerio Público y a la Policía Nacional de herramientas efectivas de cooperación con plataformas digitales, se fortalece el Sistema Nacional de Seguridad Ciudadana y se impulsa la interoperabilidad institucional requerida para enfrentar delitos de alta complejidad.

En suma, la iniciativa se inserta de manera coherente en los lineamientos estratégicos del país, contribuye a los compromisos del Acuerdo Nacional en materia de seguridad, institucionalidad y lucha contra el crimen organizado, y alinea la legislación peruana con las mejores prácticas comparadas, consolidando un marco normativo que refuerza la soberanía digital y permite que el Estado recupere capacidad de acción frente a amenazas que hoy operan sin fronteras 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** 18. Medidas en favor de la seguridad ciudadana y el civismo 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 N° 002-2023-2024-CR.