

PROYECTO DE LEY QUE REFUERZA LA PROTECCIÓN DE LOS DATOS PERSONALES FRENTE A SU RECOLECCIÓN Y COMERCIALIZACIÓN INDEBIDA EN PLATAFORMAS DIGITALES

El congresista de la República que suscribe, **ALEJANDRO SOTO REYES**, integrante del **Grupo Parlamentario Alianza para el Progreso**, en ejercicio del derecho de iniciativa legislativa que le confiere el artículo 107 de la Constitución Política y los artículos 74 y 75 del Reglamento, propone el siguiente **PROYECTO DE LEY**:

FÓRMULA LEGAL

LEY QUE REFUERZA LA PROTECCIÓN DE LOS DATOS PERSONALES FRENTE A SU RECOLECCIÓN Y COMERCIALIZACIÓN INDEBIDA EN PLATAFORMAS DIGITALES

Artículo 1. Objeto de la Ley

La presente ley tiene por objeto reforzar la protección de los datos personales frente a prácticas de recolección automatizada, oferta, comercialización, intercambio o difusión indebida de información personal obtenida sin consentimiento, especialmente cuando dichas conductas se realizan a través de plataformas digitales, redes sociales o servicios de mensajería.

Artículo 2. Finalidad

La finalidad de la presente ley es prevenir y desincentivar el mercado ilegal de datos personales, proteger la identidad y privacidad de los ciudadanos, y fortalecer la responsabilidad de quienes obtienen, negocian o difunden datos personales sin consentimiento.

Artículo 3. Incorpórese el artículo 28-A a la Ley 29733, Ley de Protección de Datos Personales

Se incorpora el artículo 28-A a la Ley 29733, Ley de Protección de Datos Personales, con el siguiente texto:

"Artículo 28-A.- Recolección y comercialización indebida de datos personales

Constituye una modalidad de tratamiento ilícito de datos personales la recolección, extracción, almacenamiento, oferta, comercialización, intercambio, publicación o difusión de datos personales, realizada mediante técnicas automatizadas o no, cuando dicha información haya sido obtenida sin el consentimiento del titular o sin habilitación legal expresa, aun cuando los datos se encuentren disponibles en entornos digitales de acceso público.

Se encuentra comprendida en esta prohibición la oferta o venta de datos personales a través de plataformas digitales, redes sociales, servicios de



mensajería instantánea, marketplaces virtuales o cualquier otro medio digital, con fines comerciales o de lucro.

Cuando estas conductas recaigan sobre datos personales contenidos en registros o sistemas administrados por entidades públicas, especialmente aquellos vinculados a la identidad, registros civiles, electorales, tributarios, migratorios o de seguridad ciudadana, la infracción será considerada de carácter muy grave para efectos del régimen sancionador."

Artículo 4. Modifíquese el artículo 154-A del Decreto Legislativo 635, Código Penal

Se modifica el artículo 154-A del Decreto Legislativo 635, Código Penal, con el siguiente texto:

"Artículo 154-A.- Tráfico ilegal de datos personales

*El que ilegítimamente **recolecta, obtiene, ofrece, comercializa, vende, intercambia o difunde** información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.*

La misma pena se aplicará a quien adquiere, compra o utiliza información no pública de datos personales, con conocimiento de su origen ilícito o sin consentimiento del titular, aun cuando no haya participado en su recolección o comercialización inicial.

*Si el agente comete el delito como integrante de una organización criminal, **o cuando la conducta se realice a través de plataformas digitales, redes sociales o servicios de mensajería**, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en **los párrafos anteriores.**"*

Lima, 12 de enero del 2026

ALEJANDRO SOTO REYES
Congresista de la República

EXPOSICIÓN DE MOTIVOS

La protección de los datos personales constituye en la actualidad uno de los principales desafíos jurídicos del Estado frente a la acelerada digitalización de los servicios públicos y privados. El desarrollo de plataformas digitales, redes sociales y servicios de mensajería instantánea ha permitido una circulación masiva de información personal, generando nuevos riesgos para la identidad, la privacidad y la seguridad de los ciudadanos, especialmente cuando dicha información es recolectada, comercializada o difundida sin el consentimiento de sus titulares.

El marco constitucional reconoce expresamente el derecho fundamental a la protección de los datos personales, conforme al artículo 2, inciso 6, de la Constitución Política del Perú, el cual garantiza que toda persona tenga control sobre la información que le concierne. Este derecho se desarrolla normativamente a través de la Ley 29733, Ley de Protección de Datos Personales, cuyo objeto es regular el tratamiento de la información personal y establecer obligaciones para quienes la administran. No obstante, la evolución tecnológica ha generado modalidades de afectación que no se encontraban plenamente previstas al momento de su promulgación.

En los últimos años, se ha evidenciado la proliferación de prácticas ilícitas consistentes en la recolección automatizada de datos personales, así como su oferta, venta e intercambio a través de plataformas digitales abiertas, como redes sociales, servicios de mensajería y marketplaces virtuales. Diversos reportajes periodísticos han documentado la existencia de mercados informales donde se negocian bases de datos que contienen números de DNI, direcciones, teléfonos, información financiera y otros datos sensibles de ciudadanos peruanos.

Un claro ejemplo de la magnitud del problema se observó en investigaciones realizadas sobre redes sociales, donde El Comercio¹ constató que más de 160 cuentas en Facebook Marketplace ofrecían datos personales verificados y reales a partir de 5 soles, incluyendo información sensible como números de documento de identidad, direcciones, números de teléfono y registros patrimoniales de ciudadanos peruanos, en algunos casos extendiéndose también a servicios de mensajería como Telegram. Esta oferta masiva de información personal en espacios digitales abiertos demuestra que los datos de los ciudadanos circulan en un mercado informal y lucrativo sin control ni supervisión, lo que incrementa los riesgos de

¹ <https://elcomercio.pe/lima/sucesos/mas-de-160-cuentas-de-marketplace-venden-datos-personales-verificados-y-reales-desde-10-soles-noticia/>

fraude, suplantación de identidad y otras conductas delictivas en perjuicio de la privacidad y seguridad individual.

Estas prácticas no se limitan a actos aislados de acceso indebido, sino que configuran verdaderas redes de comercialización de datos personales, en las que participan recolectores, intermediarios y compradores finales. La experiencia reciente demuestra que plataformas de uso cotidiano, como grupos de WhatsApp, Telegram y espacios de compraventa digital, son utilizados para ofertar información personal con fines comerciales, fraudulentos o delictivos, sin que exista una tipificación suficientemente clara que abarque toda la cadena de responsabilidad.

Casos de alta repercusión pública, como las investigaciones por filtraciones de datos en entidades estatales como la ONPE y el RENIEC, han puesto en evidencia la magnitud del problema y la necesidad de reforzar la tutela jurídica sobre la información personal administrada tanto por el Estado como por el sector privado. Estas filtraciones no solo afectan a millones de ciudadanos, sino que generan un impacto directo en la confianza pública y en la seguridad jurídica del sistema.

Si bien la Ley 29733 establece obligaciones claras en su artículo 28 respecto al consentimiento, la licitud y la finalidad del tratamiento de datos personales, no desarrolla de manera expresa la recolección automatizada masiva ni la comercialización de datos obtenidos ilícitamente, especialmente cuando estas conductas se realizan aprovechando entornos digitales de acceso público. Esta omisión ha permitido interpretaciones restrictivas que dificultan la actuación efectiva de la Autoridad Nacional de Protección de Datos Personales.

La regulación vigente del artículo 154-A del Código Penal, si bien sancionaba el tráfico ilegal de datos personales, se encontraba limitada a supuestos tradicionales de comercialización directa, sin prever de manera expresa las nuevas dinámicas del mercado digital ni abarcar toda la cadena de conductas que hoy configuran el negocio ilícito de datos personales. En particular, la redacción anterior no contemplaba la oferta pública, el intercambio ni la difusión sistemática de información personal a través de plataformas digitales y servicios de mensajería, ni tampoco atribuía responsabilidad penal al adquirente o comprador de datos que, con conocimiento de su origen ilícito, incentiva y sostiene dicho mercado. La presente modificación subsana estos vacíos normativos, adecuando el tipo penal a la realidad tecnológica actual y permitiendo una respuesta penal más completa, eficaz y coherente frente al tráfico ilegal de datos personales en entornos digitales. Por eso que la presente propuesta plantea esta modificación:



“Artículo 154-A.- Tráfico ilegal de datos personales

*El que ilegítimamente **recolecta, obtiene, ofrece, comercializa, vende, intercambia o difunde** información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.*

La misma pena se aplicará a quien adquiere, compra o utiliza información no pública de datos personales, con conocimiento de su origen ilícito o sin consentimiento del titular, aun cuando no haya participado en su recolección o comercialización inicial.

*Si el agente comete el delito como integrante de una organización criminal, **o cuando la conducta se realice a través de plataformas digitales, redes sociales o servicios de mensajería**, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en **los párrafos anteriores.**”*

La ausencia de sanción penal expresa para quien adquiere o utiliza datos personales sabiendo su origen ilícito genera un incentivo perverso que alimenta la demanda de información personal en el mercado negro digital. Sin compradores, no existiría un incentivo económico para la recolección y venta de datos personales, por lo que resulta jurídicamente necesario cerrar este vacío normativo desde una perspectiva integral de prevención del delito.

Un fenómeno alarmante que ilustra la urgencia de esta reforma normativa es la proliferación de bots² en plataformas de mensajería como Telegram que permiten a cualquier usuario acceder a datos personales de ciudadanos peruanos con solo introducir un número de documento o teléfono, desplegando información sensible como nombres, dirección, estado civil e incluso antecedentes judiciales o policiales, sin autorización ni control estatal efectivo. Esta realidad, reportada por organizaciones especializadas en derecho y tecnologías, evidencia que grupos organizados utilizan la infraestructura de plataformas digitales para traficar datos personales de manera automatizada, alimentando un mercado ilegal de información que no solo vulnera la privacidad y la autodeterminación informativa de las personas, sino que también facilita la comisión de delitos conexos como la suplantación de identidad, fraudes financieros y otros actos delictivos graves

² <https://tytl.com.pe/bots-en-telegram-que-trafican-nuestros-datos-personales-que-esta-ocurriendo-con-la-ciberseguridad-estatal/>

La gravedad del tráfico ilegal de datos personales se pone de manifiesto frente a hechos que ilustran la vulneración de la identidad y privacidad de los ciudadanos más vulnerables. Según denuncias realizadas por la jefa del Registro Nacional de Identificación y Estado Civil (Reniec)³, se ha detectado la comercialización de información personal incluso de menores de edad desde los dos años, incluyendo datos que permiten identificar sus vínculos familiares y otros detalles sensibles, a través de chats ilícitos en plataformas de mensajería como Telegram, utilizados por redes delictivas para extender circuitos de extorsión y otros ilícitos informáticos. Esta situación evidencia no solo la existencia de un mercado ilegal de datos personales, sino también la incapacidad de las regulaciones actuales para proteger de manera efectiva a los titulares frente a nuevos esquemas de explotación y comercio de información.

La presente iniciativa legislativa responde a esta realidad incorporando, por un lado, el artículo 28-A a la Ley 29733, con el fin de reconocer expresamente la recolección y comercialización indebida de datos personales como una modalidad agravada de tratamiento ilícito, sin duplicar las obligaciones ya reguladas en el artículo 28. De este modo, se fortalece el régimen administrativo sancionador frente a prácticas que hoy exceden el tratamiento tradicional de datos.

Por otro lado, la modificación del artículo 154-A del Código Penal permite actualizar el tipo penal conforme a las nuevas dinámicas delictivas, ampliando los verbos típicos e incorporando la responsabilidad penal del adquirente o comprador de datos personales, siempre que actúe con conocimiento del origen ilícito de la información o sin consentimiento del titular.

Debe resaltarse que esta reforma no crea un nuevo delito ni altera la estructura del sistema penal, sino que perfecciona un tipo existente, adecuándolo a la realidad tecnológica actual y a los estándares internacionales de protección de datos. En ese sentido, se alinea con las recomendaciones de organismos internacionales que advierten sobre el crecimiento del comercio ilegal de información personal como fenómeno transnacional vinculado a delitos informáticos, fraude y suplantación de identidad.

³ <https://lpderecho.pe/venden-hasta-datos-de-una-nina-de-2-anos-reniec-cerrara-telegram-app-no-censura-chats-ilicitos/>

Desde una perspectiva de política criminal, la modificación propuesta fortalece el carácter disuasivo del sistema penal frente al tráfico ilegal de datos personales, atacando no solo la oferta sino también la demanda de información ilícita. Ello contribuye a reducir la rentabilidad de estas conductas y a proteger de manera más efectiva la identidad y privacidad de los ciudadanos.

Finalmente, la importancia de esta iniciativa legislativa radica en que reconoce que la protección de los datos personales no puede limitarse a sanciones administrativas cuando el daño es masivo, sistemático y lucrativo. Al reforzar la responsabilidad administrativa y penal frente a la recolección y comercialización indebida de información personal, el Estado reafirma su compromiso con la defensa de los derechos fundamentales en el entorno digital y fortalece la confianza ciudadana en el uso seguro de las tecnologías de la información.

II. EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa tiene por objeto reforzar la protección jurídica de los datos personales de los ciudadanos frente a prácticas de recolección, oferta, comercialización, intercambio y difusión indebida de información personal obtenida sin consentimiento, mediante la incorporación de disposiciones específicas en la Ley de Protección de Datos Personales y la actualización del tipo penal de tráfico ilegal de datos personales previsto en el artículo 154-A del Código Penal. Su finalidad es dotar al ordenamiento jurídico de una respuesta más clara, eficaz y proporcional frente a un fenómeno que, en el contexto digital actual, afecta gravemente la privacidad, la identidad y la seguridad de las personas.

La propuesta se integra de manera armónica al sistema jurídico nacional, complementando las disposiciones constitucionales y legales vigentes en materia de protección de datos personales, delitos informáticos y derechos fundamentales. En ese sentido, la modificación propuesta no introduce un régimen paralelo ni altera la estructura del sistema sancionador existente, sino que perfecciona y actualiza normas ya vigentes para adecuarlas a las nuevas modalidades de afectación derivadas del uso intensivo de plataformas digitales y servicios de mensajería.

En consecuencia, la presente no contraviene el principio de legalidad ni implica una expansión irracional del ius puniendi del Estado, sino que responde a la necesidad de cerrar vacíos normativos frente a prácticas ilícitas que se han intensificado con la transformación digital.

III. ANÁLISIS COSTO BENEFICIO

La presente propuesta considera el siguiente cuadro de actores:

ACTORES	BENEFICIOS	COSTOS
Estado	<ul style="list-style-type: none"> Fortalece el marco normativo para combatir el mercado ilegal de datos personales, dotando de mayor claridad y eficacia a la actuación administrativa y penal. Mejora la capacidad sancionadora frente a prácticas de recolección, oferta y venta de datos personales en plataformas digitales y servicios de mensajería. 	No Aplica
Ciudadanía	<ul style="list-style-type: none"> Mayor protección frente a la exposición, comercialización y uso indebido de datos personales, reduciendo riesgos de fraude, suplantación de identidad y extorsión. Incremento de la confianza en el uso de plataformas digitales, redes sociales y servicios en línea. Salvaguarda reforzada de datos sensibles y de identidad, incluyendo los de niños, niñas y adolescentes. 	No aplica

Fuente: Elaboración propia

IV. RELACIÓN CON LA AGENDA LEGISLATIVA Y LAS POLÍTICAS DE ESTADO DEL ACUERDO NACIONAL

La presente propuesta guarda relación con la Política de Estado expresado en el acuerdo nacional: I Democracia y Estado de Derecho, punto 7 - Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana:

“Nos comprometemos a normar y fomentar las acciones destinadas a fortalecer el orden público y el respeto al libre ejercicio de los derechos y al cumplimiento de los deberes individuales.

Con este objetivo el Estado: (a) consolidará políticas orientadas a prevenir, disuadir, sancionar y eliminar aquellas conductas y prácticas sociales que pongan en peligro la tranquilidad, integridad o libertad de las personas así como la propiedad pública y privada; (b) propiciará una cultura cívica de respeto a la



ley y a las normas de convivencia, sensibilizando a la ciudadanía contra la violencia y generando un marco de estabilidad social que afiance los derechos y deberes de los peruanos; (c) pondrá especial énfasis en extender los mecanismos legales para combatir prácticas violentas arraigadas, como son el maltrato familiar y la violación contra la integridad física y mental de niños, ancianos y mujeres; (d) garantizará su presencia efectiva en las zonas vulnerables a la violencia; (e) fomentará una cultura de paz a través de una educación y una ética públicas que incidan en el respeto irrestricto de los derechos humanos, en una recta administración de justicia y en la reconciliación; (f) desarrollará una política de especialización en los organismos públicos responsables de garantizar la seguridad ciudadana; (g) promoverá los valores éticos y cívicos de los integrantes de la Policía Nacional, así como su adecuada capacitación y retribución; (h) promoverá un sistema nacional de seguridad ciudadana en la totalidad de provincias y distritos del país, presidido por los alcaldes y conformado por representantes de los sectores públicos y de la ciudadanía."

Asimismo, guarda relación con la Agenda Legislativa del Congreso de la República, aprobada mediante Resolución Legislativa del Congreso 006-2024-2025-CR, específicamente con la política de estado 28. Plena vigencia de la Constitución y de los Derechos Humanos y acceso a la justicia e independencia judicial, tema 97 sobre "Modernización y acceso en el sistema de justicia."