



Firmado digitalmente por:
RAMIREZ GARCIA Tania
Estefany FAU 20161749126 soft
Initivo Soy el autor del
documento
Fecha: 09/01/2026 14:36:41-0500
CONGRESO
REPUBLICA

MARTHA MOYANO DELGADO
Congresista de la República

*Decenio de la Igualdad de Oportunidades para mujeres y hombres
Año de la recuperación y consolidación de la economía peruana*

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
RECIBIDO
PROYECTO DE LEY N°
13706/2025-CR RU 2186774
12 ENERO 2026 08:35 a. m.
FIRMADO DIGITALMENTE: CMEDINA

PROYECTO DE LEY

La Congresista de la República **MARTHA LUPE MOYANO DELGADO**, integrante del Grupo Parlamentario **FUERZA POPULAR**, en el ejercicio de las facultades que le confiere el artículo 107° de la Constitución Política del Perú, y de conformidad con lo establecido en los artículos 75° y 76° del Reglamento del Congreso, presenta la siguiente iniciativa legislativa:

FORMULA LEGAL

“Ley que prohíbe la comercialización, difusión y uso indebido de datos personales de ciudadanos en redes sociales y plataformas digitales y Protege los Datos Personales frente al Scraping Automatizado”

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto de la ley

La presente ley tiene por objeto prohibir y sancionar la recolección automatizada no autorizada, así como la comercialización y uso indebido de datos personales obtenidos sin consentimiento, en redes sociales y plataformas digitales, mediante técnicas de scraping automatizado u otras técnicas.

La presente ley promueve el fortalecimiento de la seguridad de los sistemas de identificación y registros públicos administrados por el Estado, en especial aquellos gestionados por el Registro Nacional de Identificación y Estado Civil - RENIEC, a fin de prevenir el acceso automatizado no autorizado y garantizar la protección reforzada de los datos personales.

Artículo 2. Ámbito de aplicación

Aplica a toda persona natural o jurídica, pública o privada, nacional o extranjera, que intervenga en el tratamiento automatizado de datos personales desde plataformas digitales accesibles en territorio nacional. Abarca a todas las plataformas digitales, redes sociales, empresas, organizaciones y ciudadanos que gestionen, obtengan, utilicen, transmitan o difundan datos personales en territorio nacional y en plataformas internacionales que operen en Perú.

Artículo 3. – Datos de interés estratégico

Se consideran de interés estratégico para la seguridad nacional y la protección de la identidad ciudadana los datos personales gestionados por entidades públicas que administren registros de identificación, procesos electorales, registros jurídicos, tributarios, migratorios y de seguridad ciudadana, incluyendo a los administrados por RENIEC, ONPE, JNE, SUNARP, SUNAT, Migraciones, Policía Nacional y otros que se enmarquen en estas funciones. El tratamiento de estos datos estará sujeto a medidas reforzadas de seguridad y control que el reglamento determinará

Artículo 4. Definiciones

- a. *Scraping Automatizado*: técnica que utiliza bots o software para extraer datos masivos o no de sitios web sin autorización del titular ni de la plataforma.
- b. *Anonimización*: es el proceso de eliminar o modificar los datos personales identificables para que no puedan ser asociados con una persona específica. Proceso de transformación de datos que podrían revelar la identidad de alguien en datos que no permiten su identificación.
- c. *Dato personal sensible*: información que, por su naturaleza, puede afectar la intimidad del titular o generar discriminación. Cualquier información vinculada o que pueda asociarse a una persona identificada o identificable. Se consideran sensibles, de forma expresa, los datos de identidad emitidos por el Estado, se incluye el Código Único de Identificación (CUI), número de DNI, datos biométricos, faciales, dactilares, de iris, firma digital, dirección, estado civil, filiación y cualquier otro dato presente en registros oficiales, sin perjuicio de otras categorías que la ley o el reglamento determinen.
- d. *Plataformas digitales*: redes sociales, foros, aplicaciones móviles y demás entornos virtuales que permitan la interacción pública o privada.
- e. *Usuario Final*: Persona natural que utiliza plataformas digitales de manera directa, en calidad de destinataria del servicio o interacción, distinta de intermediarios o administradores.
- f. *Responsable del tratamiento*: Persona o entidad que decide sobre el tratamiento de datos personales.

CAPÍTULO II

PROHIBICIONES

Artículo 5. Conductas prohibidas.

Se consideran conductas prohibidas:

- La extracción de datos personales mediante scraping automatizado en redes sociales.
- La comercialización, intercambio, transferencia, difusión, publicación, o divulgación de datos personales obtenidos sin el consentimiento del titular víctima, mediante cualquier medio, incluyendo el scraping automatizado.
- La creación de plataformas o grupos virtuales con fines de venta de datos.
- El scraping, comercialización o difusión de datos provenientes de sistemas o plataformas de identidad y registros públicos administrados por el Estado, cuya afectación será considerada infracción muy grave.

Artículo 6: Uso indebido mediante scraping automatizado

Se prohíbe el uso de bots, scripts o cualquier sistema automatizado que acceda a plataformas digitales para recoger, almacenar o tratar datos personales sin la autorización expresa del titular o sin cumplir requisitos previstos en la presente ley.

Cuando el scraping automatizado recaiga sobre bases de datos estatales o registros de identidad administrados por el Estado, la conducta se considerará infracción muy grave y será sancionada con las medidas previstas para tales supuestos en el régimen sancionador.

CAPÍTULO III

DERECHOS DE LOS TITULARES DE DATOS

Artículo 7: Consentimiento informado

El responsable del tratamiento obtiene el consentimiento explícito, informado y verificable del titular antes de recolectar y tratar sus datos.

Los mecanismos para la obtención de consentimiento interoperan con los sistemas de verificación de identidad del RENIEC u otras entidades competentes, conforme a lo que establezca el reglamento.

Artículo 8: Derecho a la oposición y revocación

El titular puede oponerse al tratamiento de sus datos y revocar su consentimiento en cualquier momento, mediante solicitud al responsable. Las plataformas garantizan los mecanismos seguros de verificación de identidad, interoperan con los sistemas del RENIEC u otras entidades competentes, según lo que establezca el reglamento, a fin de prevenir suplantaciones en el ejercicio de estos derechos.

Artículo 9: Derecho a la eliminación

El responsable debe facilitar la eliminación de los datos personales cuando el titular lo solicite, siempre que no exista un interés legítimo en mantenerlos.

CAPÍTULO IV

NORMAS PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS

Artículo 10: Medidas de seguridad

Se implementan medidas técnicas, físicas y organizativas apropiadas para proteger los datos contra acceso no autorizado, manipulación, pérdida o difusión indebida.

Las entidades públicas, mantienen registros y medidas de seguridad de todos los accesos a datos personales. Establecer sistemas de monitoreo para detectar patrones anómalos de scraping. Las plataformas digitales adoptan barreras técnicas para prevenir el scraping automatizado, conforme a lo que disponga el reglamento.

Artículo 11: Transparencia y responsabilidad

Los responsables deben informar a los usuarios sobre el tratamiento de sus datos y mantener registros de las acciones realizadas.

CAPÍTULO V

RÉGIMEN SANCIONADOR

Artículo 12: Sanciones administrativas

Las infracciones a esta ley serán sancionadas con multas, suspensión de actividades, inhabilitación, siguiendo una escala proporcional a la gravedad de la infracción.

Las infracciones son:

- a. *Infracciones Leves*, cuando hay utilización de técnicas de scraping para fines académicos sin anonimización.
- b. *Infracciones Graves*: cuando la recolección y uso sin autorización de datos personales es para fines comerciales.
- c. *Infracciones Muy graves*: cuando las infracciones leves y graves son reiteradas. Incluye a la conducta que afecte datos de identidad emitidos por el Estado o datos biométricos, así como la información personal de operadores de justicia, fiscales, policías y demás autoridades que, por la naturaleza de sus funciones, estén expuestas a alto riesgo, lo que se determinará en el reglamento respectivo.

Artículo 13. Sanciones

Las sanciones incluyen:

- a. Multas que oscilan entre 100 y 500 UIT según la gravedad.
- b. Suspensión de licencias tecnológicas en caso de empresas.
- c. Inhabilitación en casos de reincidencia o uso doloso.

CAPÍTULO VI

SUPERVISIÓN Y FISCALIZACIÓN

Artículo 14. Autoridad competente.

La Autoridad General de Protección de Datos Personales, adscrita al Ministerio de Justicia, será la encargada de fiscalizar, recibir denuncias y aplicar las sanciones correspondientes.

El RENIEC, la ONPE, el JNE, la SUNARP, la SUNAT, la Oficina de Migraciones, la Policía Nacional, serán entidades colaboradoras obligatorias de la autoridad competente y, conforme a lo que disponga el reglamento, podrán ejecutar medidas cautelares temporales de bloqueo de contenidos o perfiles que difundan datos personales obtenidos ilegalmente, sujetas a revisión posterior por la autoridad competente.

Artículo 15. Cooperación internacional.

El Estado promoverá convenios con plataformas digitales y entes internacionales para detectar e intervenir redes de scraping transnacional.

Se priorizará la suscripción de convenios con plataformas digitales para implementar mecanismos técnicos que bloqueen el scraping automatizado sobre fuentes oficiales, entendiéndose por estas aquellas administradas o autorizadas por el Estado, conforme a lo que establezca el reglamento.

DISPOSICIONES FINALES

Primera. Reglamentación de la Ley.

El Poder Ejecutivo, a través del Ministerio Justicia, a través de la Autoridad Nacional de Datos Personales, en coordinación con el Registro Nacional de Identificación y Estado Civil RENIEC y el Ministerio del Interior, reglamentará la presente ley en un plazo no mayor a noventa (90) días calendario desde su publicación.

En el reglamento se establecerán lineamientos técnicos mínimos obligatorios para la prevención de scraping, que podrán incluir, entre otras medidas, la anonimización de datos públicos indexados, la tokenización y las auditorías de acceso, así como cualquier otra práctica que garantice un nivel adecuado de protección, de conformidad con la evolución tecnológica.

Segunda. Integración normativa.

Las disposiciones de esta ley se integran con lo establecido en la Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento aprobado por Decreto Supremo N° 003-2013-JUS, y el Decreto Supremo N° 016-2024-JUS, así como con las normas que regulan el acceso y tratamiento de información en el Poder Judicial, Ministerio Público, Policía Nacional del Perú y otras entidades vinculadas.

Tercera. Carácter prevalente.

En caso de conflicto normativo, las disposiciones contenidas en esta ley prevalecerán sobre aquellas que regulen de manera general el tratamiento de datos personales, cuando se refiera específicamente a operadores de justicia en situación de riesgo o función sensible.

DISPOSICIÓN TRANSITORIA ÚNICA

Las entidades públicas y privadas comprendidas en el ámbito de aplicación de la presente ley deberán adecuar sus sistemas informáticos, protocolos de acceso y



Firmado digitalmente por:
LOPEZ MORALES Jeny Lu
FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/01/2026 16:53:06-0500

MARTHA MOYANO DELGADO
Congresista de la República

*Decenio de la Igualdad de Oportunidades para mujeres y hombres
Año de la recuperación y consolidación de la economía peruana*

procesos de consulta de información en un plazo máximo de ciento ochenta (180) días calendario desde la entrada en vigencia de esta norma.

Durante este período, la Dirección Nacional de Protección de Datos Personales del Ministerio del Interior, emitirá lineamientos técnicos mínimos y brindará asistencia especializada a las entidades responsables del tratamiento, en coordinación con la Autoridad Nacional de Protección de Datos Personales.

Para las entidades críticas, como el RENIEC, ONPE, JNE, Migraciones, Policía Nacional y Poder Judicial, el plazo máximo de adecuación será de noventa (90) días calendario, debiendo presentar a la Dirección Nacional de Protección de Datos Personales, dentro de los primeros treinta (30) días, un plan de implementación detallado que considere fases, recursos y responsables. Dicho plazo podrá ajustarse excepcionalmente, previa evaluación técnica, cuando la complejidad del cambio así lo justifique.

DISPOSICIÓN COMPLEMENTARIA DE ENTRADA EN VIGENCIA

La presente ley entra en vigencia a los treinta (30) días calendario siguientes a su publicación en el diario oficial *El Peruano*, con excepción de lo dispuesto en la Disposición Final Primera, que rige desde al día siguiente de la publicación



Firmado digitalmente por:
REVILLA VILLANUEVA Cesar
Manuel FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/01/2026 11:43:58-0500

EXPOSICIÓN DE MOTIVOS



Firmado digitalmente por:
MOYANO DELGADO Martha
Lupe FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 07/01/2026 13:12:28-0500

I. ANTECEDENTES

En la era digital contemporánea, el uso y tratamiento de los datos personales se ha convertido en un elemento fundamental para la ciudadanía, las empresas y las instituciones públicas. La creciente automatización y el avance tecnológico han optimizado la recopilación, análisis y utilización de la información individual, generando beneficios, pero también abriendo nuevas vulnerabilidades y riesgos para la protección de los derechos y libertades de los titulares de los datos.

Uno de los fenómenos que más ha puesto en evidencia estas vulnerabilidades es el uso del scraping automatizado, una técnica que permite extraer de manera masiva y no autorizada datos de plataformas digitales, redes sociales y sitios web. Esta práctica, si bien tiene aplicaciones legítimas en ciertos contextos, cuando se realiza sin consentimiento y en perjuicio de la privacidad de las personas, constituye una grave violación a sus derechos fundamentales.

El presente proyecto de ley surge como respuesta a estas problemáticas, con la finalidad de establecer un marco normativo claro y efectivo que prohíba la recolección, difusión, comercialización y uso indebido de datos personales mediante técnicas de scraping automatizadas sin la debida autorización o cumplimiento de la normativa vigente. La ley busca también fortalecer los mecanismos de protección de los derechos de los titulares, garantizando el acceso, la rectificación, la cancelación y la oposición en el tratamiento de sus



Firmado digitalmente por:
CHACON TRUJILLO Nilza
Merly FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/01/2026 12:53:33-0500



Firmado digitalmente por:
HUAMAN CORONADO Raul
20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 09/01/2026 12:57:17-0500



Firmado digitalmente por:
AGUINAGA RECUENCO
Alejandro Aurelio FAU 20161749126
soft
Motivo: Soy el autor del
documento
Fecha: 09/01/2026 15:29:58-0500

datos, así como la implementación de medidas de seguridad que eviten accesos no autorizados y la explotación ilícita de la información.

Asimismo, es imperativo regular y sancionar las conductas ilícitas relacionadas con la comercialización y difusión de datos personales, particularmente en un contexto donde los delitos cibernéticos y las prácticas abusivas en línea han aumentado en magnitud y sofisticación. La incorporación de sanciones administrativas, penales y la creación de órganos de supervisión especializados contribuirán a disuadir estas conductas y a proteger el interés público.

En resumen, esta ley constituye un paso decisivo hacia una regulación moderna, efectiva y coherente que respeta los derechos de los ciudadanos, promueve la confianza en las plataformas digitales y establece un importante precedente en la protección de datos personales frente a las amenazas del scraping automatizado y del comercio ilícito de información.

Por ello, es deber del Estado garantizar la protección efectiva de los derechos fundamentales en el ámbito digital, adaptándose a los nuevos desafíos planteados por las Tecnologías de la Información y las Comunicaciones (TIC), y promoviendo una cultura de respeto y responsabilidad en el tratamiento de los datos personales.

En los últimos años se ha incrementado la **comercialización ilegal de datos personales** en redes sociales, foros clandestinos y plataformas digitales. Entre los casos más críticos encontramos elementos como:

- Las filtraciones de bases de datos públicas con información sensible (DNI, direcciones, teléfonos).
- El ofrecimiento de servicios de búsqueda masiva por número de documento o nombre en grupos de redes sociales.
- El uso de *bots* para extraer datos de plataformas estatales sin autorización.
- La publicación de datos de autoridades judiciales, policiales o fiscales, poniendo en riesgo su seguridad.

Estas prácticas vulneran el derecho fundamental a la privacidad, generan un riesgo de extorsión, estafa, suplantación de identidad y delitos informáticos, y deterioran la confianza del ciudadano en el Estado.

II. OBJETIVOS

2.1. Objetivo General

El proyecto busca establecer un marco normativo que prohíba y sancione la comercialización y difusión ilegal de datos personales en redes sociales.

2.2. Objetivos específicos

Los objetivos específicos que se identifica son los siguientes:

- Proteger la privacidad e integridad digital de los ciudadanos.
- Fortalecer la seguridad de las bases de datos del Estado.
- Promover una cultura de respeto y responsabilidad en el uso de datos.
- Coordinar con plataformas digitales la eliminación de contenidos ilícitos.
- Prevenir y sancionar el uso indebido por servidores públicos o terceros.
- Proteger a colectivos vulnerables y datos de especial protección (identidad oficial, biométricos, menores, autoridades en funciones de alto riesgo).

III. FUNDAMENTO LEGAL

Las bases normativas son las siguiente:

- **Constitución Política del Perú:** Art. 2 inciso 6 (derecho a la intimidad personal y familiar).
- **Ley N° 29733 – Protección de Datos Personales:** Principios de consentimiento, finalidad, proporcionalidad y seguridad.
- Tratados internacionales sobre derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos.

IV. ANTECEDENTES

- Denuncias e informes de la Autoridad Nacional de Protección de Datos¹ sobre consultas masivas desde IPs no autorizadas.
- Propuestas previas del MININTER (Dirección de Protección de Datos del Ministerio del Interior²) y RENIEC para considerar las bases de datos del Estado como activos críticos.³
- Casos internacionales similares que impulsaron leyes de scraping y uso indebido de datos (ej. GDPR en Europa y CCPA en EE.UU.).⁴

1 La Ley N.º 29733 establece el marco legal para la protección de datos personales en Perú, definiendo los principios, derechos y obligaciones relacionados con el tratamiento de datos personales. En su título VI.

2 La norma que crea la Dirección General de Protección de Datos Personales (DGPDP) dentro del Ministerio del Interior (MININTER) es el Decreto Supremo N.º DS 003-2021-IN, según la Plataforma del Estado Peruano. Este decreto supremo fue publicado el 9 de abril de 2021. El Decreto Supremo N.º DS 003-2021-IN establece la creación de la DGPDP como un órgano de línea del MININTER, encargado de la protección de datos personales dentro del ámbito de sus competencias. Además, este decreto define las funciones y estructura de la dirección.

3 Decreto Supremos N° 004-2028-IN Que aprueba la "Directiva Nacional de Orden Interno para la Protección de los Activos Críticos Nacionales ACN" Noticia. "Filtran datos de más de 15 millones de peruanos desde el Mininter" <https://smartdata.com.pe/filtran-datos-de-mas-de-15-millones-de-peruanos-desde-el-mininter/>

4 Ver: "Situación jurídica del Web Scraping en 2025".

[https://proxyseller.com/es/blog/es_legal_el_web_scraping_en_2024/#:~:text=Situaci%C3%B3n%20jur%C3%ADdica%20del%20Web%20Scraping%20en%202025,Platforms%20Inc%20contra%20Bright%20Data%20Ltd%20\(2024\)](https://proxyseller.com/es/blog/es_legal_el_web_scraping_en_2024/#:~:text=Situaci%C3%B3n%20jur%C3%ADdica%20del%20Web%20Scraping%20en%202025,Platforms%20Inc%20contra%20Bright%20Data%20Ltd%20(2024))

"¿Es legal el web scraping? Abarcando todos los aspectos". <https://medium.com/@datajournal/is-web-scraping-legal-0df27c2e2ec6>

V. JUSTIFICACIÓN

La naturaleza masiva y transnacional de las redes sociales facilita la diseminación de datos personales sin ningún tipo de control. La ciudadanía no está debidamente informada ni protegida frente al riesgo digital permanente.

Por tanto, esta propuesta de ley, busca:

- Fortalecer el rol del Estado como garante de los derechos fundamentales.
- Limitar el uso de tecnologías automatizadas para extraer datos sin autorización.
- Sancionará con claridad conductas que hasta hoy operan en un vacío legal.
- Impulsará alianzas tecnológicas con redes sociales para bloquear contenidos ilícitos.

VI. Contenido de la norma

La propuesta incluirá:

- 6.1. Definiciones técnicas:** scraping⁵, consulta masiva, difusión digital, datos sensibles.
- 6.2. Conductas sancionadas:** venta, publicación, acceso no autorizado, intercambio en redes.
- 6.3. Sanciones administrativas:** escaladas según gravedad y reincidencia.
- 6.4. Obligaciones del Estado:** registro de incidentes, monitoreo activo, auditorías digitales.
- 6.5. Medidas preventivas:** educación digital, fortalecimiento institucional, protocolos de emergencia.

VII. Análisis Estadístico del Problema

Es importante revisar los datos estadístico siguientes:

7.1. Filtraciones de datos personales en redes sociales

- En **2021**, se filtraron datos de **533 millones de usuarios de Facebook** en más de 100 países, incluyendo números de teléfono, correos electrónicos y ubicaciones.⁶

“¿Es legal el web scraping en EE. UU.? – Una guía completa”. <https://www.promptcloud.com/blog/is-web-scraping-legal-in-us-a-complete-guide/#:-:text=LinkedIn%20vs.,el%20scraping%20de%20datos%20p%C3%ABlicos>

5 El scraping, también conocido como web scraping o raspado web, es una técnica de extracción automatizada de datos de sitios web. Consiste en utilizar software para recopilar información específica de una página web y guardarla en un formato estructurado, como una hoja de cálculo o una base de datos. En esencia, el scraping imita la navegación humana para obtener datos de forma automatizada.

6 Filtran línea datos de 533 millones de usuarios de Facebook. <https://www.dw.com/es/filtran-datos-de-533-millones-de-usuarios-de-facebook-en-foro-de-ciberpiratas/a-57095450>

- En el caso de **LinkedIn**, se expusieron datos de **700 millones de usuarios** en 2021, lo que representó más del 90% de su base global.⁷
- En Perú, se han reportado casos de **venta de bases de datos** con información de ciudadanos en grupos de redes sociales, incluyendo nombres, DNI, direcciones y teléfonos.⁸

7.2. Riesgos asociados

- Según estudios internacionales, el **valor comercial de los datos personales** puede superar los **900 USD por usuario** al año en plataformas como Facebook.⁹
- El **Informe Anual 2022 de la Autoridad Nacional de Protección de Datos Personales (ANPD)** reportó un incremento de denuncias por uso indebido de datos en entornos digitales. INFORME N° 001-022-JUS/DGTAIPD¹⁰
- El **90,4% de los peruanos tiene acceso a internet**,¹¹ lo que los expone potencialmente a riesgos de scraping y comercialización de datos.

7.3. Percepción ciudadana

- En encuestas realizadas por medios como La República, más del 12% no sabe cómo las redes sociales usan sus datos.¹²

7 Scraping: "Robé los datos de 700 millones de usuarios de LinkedIn por diversión". <https://www.bbc.com/mundo/noticias-57835205>

8 Investigan a vendedores informales de chips que verificaban datos de ciudadanos sin autorización en Lima Norte. <https://www.gob.pe/institucion/reniec/noticias/994412-investigan-a-vendedores-informales-de-chips-que-verificaban-datos-de-ciudadanos-sin-autorizacion-en-lima-norte>

Filtran datos de más de 15 millones de peruanos desde el Mininter. <https://smartdata.com.pe/filtran-datos-de-mas-de-15-millones-de-peruanos-desde-el-mininter/>

9 ¿Cuántas personas usan las redes sociales? (Estadísticas de uso de 2025). <https://www.demandsage.com/social-media-users/#:~:text=Principales%20estad%C3%ADsticas%20de%20uso%20de,activas%20en%20las%20redes%20sociales>.

"Los datos de Facebook los pueden comprar todas las empresas, no sólo Cambridge Analytica" <https://www.lapoliticaonline.com/mexico/entrevista-mx/n-110437-los-datos-de-facebook-los-pueden-comprar-todas-las-empresas-no-solo-cambridge-analytica/>.

10 INFORME N° 001-022-JUS/DGTAIPD. <https://www.gob.pe/institucion/anpd/informes-publicaciones/6977883-informe-anual-2022-dgtaipd>

11 "El 90,4 por ciento de los hogares peruanos tienen conectividad fija o móvil, según lo relevó la Encuesta Residencial de Servicios de Telecomunicaciones (Erestel), a pedido del Organismo Supervisor de Inversión Privada en Telecomunicaciones (Osiptel)." <https://www.telesemana.com/blog/2023/11/02/se-achica-la-brecha-de-acceso-a-internet-en-peru-en-9-de-cada-10-de-hogares-hay-conectividad/#:~:text=El%2090%2C4%20por%20ciento%20de%20los%20hogares,todo%20un%20avance%20de%20casi%20un%20tre>
s

12 Otro aspecto que inquieta a los internautas de Perú es la información que ceden a las **redes sociales**: 12% de los peruanos asegura que no tiene idea de cómo estas plataformas utilizan sus datos personales y 33% señala que no confía en absoluto en el uso que dichas compañías hacen de su información. Peor aún, casi la mitad (48%) de las personas encuestadas afirmó que

- El Día Internacional de la Protección de Datos Personales (28 de enero)¹³ ha sido aprovechado por la ANPD para promover campañas de concientización, pero aún se requiere mayor alcance.

Este análisis respalda la necesidad de una ley que **regule, prevenga y sancione** la comercialización de datos personales en redes sociales.

VIII. Concordancias de la propuesta con la Ley N° 29733 – Ley de Protección de Datos Personales

8.1. Similitudes:

- **Consentimiento y derechos del titular:** La propuesta respeta los principios de consentimiento previo, informado y revocación que establece la Ley 29733.
- **Limitación del tratamiento sin autorización:** La prohibición de tratar datos sin autorización y la obligación de obtener el consentimiento previo y explícito guardan relación con los principios de la ley.
- **Medidas de seguridad:** La obligación de implementar medidas para proteger los datos en la propuesta se alinea con las obligaciones de seguridad y confidencialidad en la Ley 29733.
- **Derecho a la protección y eliminación:** La facultad del titular de solicitar la eliminación y oponerse al tratamiento está en línea con la normativa peruana

8.2. Diferencias

- La Ley 29733 regula el tratamiento de datos personales en los ámbitos público y privado, pero no contempla específicamente la problemática del scraping automatizado ni la comercialización ilícita, que la propuesta busca abordar expresamente.
- La ley peruana en general no contempla sanciones específicas por la obtención masiva de datos sin consentimiento mediante técnicas automatizadas, lo que la propuesta pretende incluir.

IX. Diferencias principales con la propuesta

tiene algún conocido cuyos datos personales han sido comprometidos en estas aplicaciones, según Kaspersky.
<https://andina.pe/agencia/noticia-usas-mucho-redes-sociales-sigue-estos-consejos-para-cuidar-tu-privacidad-876629.aspx>

¹³ El “Día Internacional de la Protección de Datos Personales” se celebra en esta fecha conmemorando la apertura a la firma del Convenio 108 en 1981, conocido como el primer tratado internacional sobre protección de datos y que fue una iniciativa del Consejo de Europa. En: “**28 de enero: Día Internacional de la Protección de Datos Personales**”.
<https://www.welivesecurity.com/es/privacidad/dia-internacional-proteccion-datos-personales/>

- 9.1. Enfoque en el scraping automatizado:** la propuesta introduce una regulación específica y proactiva contra el scraping automatizado, que actualmente no está claramente regulado en las leyes existentes.
- 9.2. Prohibición de la comercialización y difusión no autorizada:** La propuesta busca prohibir expresamente la venta y difusión de datos obtenidos sin consentimiento, aspecto que no está explícitamente regulado en las leyes actuales.
- 9.3. Normativa específica para plataformas digitales y redes sociales:** La propuesta crea obligaciones y restricciones directas a los responsables en plataformas digitales, con sanciones específicas para estos actores.
- 9.4. Sanciones más específicas y severas:** La propuesta busca establecer sanciones penales y administrativas específicas para las conductas relacionadas con el scraping ilegal y la difusión de datos no autorizados.

X. Balance general

El análisis muestra que los beneficios de la ley en términos de protección de derechos, confianza, seguridad y alineamiento internacional superan con creces los costos asociados a su implementación y aplicación. La inversión en protección de datos y en medidas de seguridad digital favorece un entorno más seguro y confiable, promoviendo el desarrollo económico y social sostenible en la era digital.

Por otra parte, la adopción de medidas y la adecuada reglamentación pueden mitigar los costos relacionados con el cumplimiento, optimizando recursos y promoviendo la innovación responsable. Además, la ley puede facilitar la creación de un mercado digital más justo y competitivo, en que los derechos de los usuarios prevalezcan sobre prácticas abusivas

XI. Análisis de Impacto de la Vigencia de la Ley en la Legislación Nacional

11.1. Fortalezas e impactos positivos

- **Alineamiento con normativas existentes:** la ley complementará y reforzará la normativa vigente en materia de protección de datos personales, como la Ley N° 29733 – Ley de Protección de Datos Personales y sus reglamentos, estableciendo un marco específico para abordar las particularidades del scraping automatizado y la difusión ilícita de datos.
- **Modernización del marco legal:** al incorporar regulaciones específicas contra el scraping y la comercialización ilícita de datos, se adapta la legislación nacional a los desafíos tecnológicos contemporáneos, fortaleciendo la capacidad del sistema jurídico para responder a delitos digitales.
- **Mejor protección de derechos:** la vigencia de la ley promoverá una protección más efectiva de los derechos de los titulares de datos en el contexto digital, en especial frente a la vulneración de su privacidad y derechos fundamentales, generando mayor confianza en las plataformas digitales nacionales e internacionales.

- **Impulso a la cooperación internacional:** la ley facilitará la firma de convenios y mecanismos de colaboración con otros países en la lucha contra delitos transnacionales relacionados con el comercio ilícito de datos y prácticas de scraping no autorizadas.

11.2. Desafíos e impactos negativos

- **Periodo de adaptación y cumplimiento.** La vigencia de la ley implica que las entidades públicas y privadas deberán realizar inversiones y cambios en sus sistemas y procesos en un plazo definido (por ejemplo, 180 días para adecuarse). Esto puede generar costos y ajustes operativos, especialmente en organizaciones con recursos limitados.
- **Potencial duplicidad o conflicto normativo.** La incorporación de nuevas disposiciones puede generar conflictos o redundancias con leyes existentes, como la Ley de Protección de Datos Personales, requiriendo procesos de armonización y revisión legislativa que podrían demorar su plena efectividad.
- **Incremento en la carga regulatoria.** La nueva ley puede aumentar la carga regulatoria para las organizaciones, requiriendo la implementación de nuevas políticas y procedimientos, lo que en algunos casos podría afectar la agilidad o innovación en ciertas actividades digitales.
- **Posible resistencia o evasión.** La vigencia de la ley puede enfrentarse a actitudes de evasión por parte de actores que realizan prácticas ilícitas, además de la necesidad de fortalecer los recursos y capacidades de fiscalización para garantizar su cumplimiento efectivo.

11.3. Oportunidades derivadas de la vigencia

- La creación de un marco legal actualizado atraerá inversiones en tecnología y protección de datos, promoviendo un entorno digital más seguro y confiable.
- La ley facilitará la sanción de conductas ilícitas, fortaleciendo el Estado de Derecho en el ámbito digital y valorizando la protección de la ciudadanía frente a delitos cibernéticos.
- Promoverá la cultura de respeto a los derechos digitales, incentivando buenas prácticas en el tratamiento y protección de datos, tanto en el sector público como privado.

Por tanto, la vigencia de la ley, una vez aprobada, tendrá un impacto positivo en la legislación nacional, reforzando los marcos regulatorios existentes, adaptándose a los nuevos desafíos tecnológicos y mejorando la protección de los derechos de los ciudadanos en el entorno digital. Sin embargo, su efectividad dependerá del adecuado proceso de implementación, de la armonización normativa y de la fiscalización efectiva para evitar prácticas ilícitas y garantizar el cumplimiento.