"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
RECIBIDO
PRESENTADO EL 26/01/2026 A LAS 6:56 P. M. CON RU 2201187
27 ENERO 2026 04:09 p. m.
FIRMADO DIGITALMENTE: NGUILLEN

Lima, 26 de enero de 2026

OFICIO Nº 033 -2026 -PR

Señor
FERNANDO MIGUEL ROSPIGLIOSI CAPURRO
Primer Vicepresidente
Encargado de la Presidencia del Congreso de la República
Presente. -

Tenemos el agrado de dirigirnos a usted, de conformidad con lo dispuesto por el artículo 104º de la Constitución Política del Perú, con la finalidad de comunicarle que, al amparo de las facultades legislativas delegadas al Poder Ejecutivo mediante Ley N° 32527, y con el voto aprobatorio del Consejo de Ministros, se ha promulgado el Decreto Legislativo N° 1700 que modifica la Ley N°30096, Ley de delitos informáticos, incorporando el delito de adquisición, posesión y tráfico ilícito de datos informáticos.

Sin otro particular, hacemos propicia la oportunidad para renovarle los sentimientos de nuestra consideración.

Atentamente,

JOSÉ ENRIQUE JERÍ ORÉ
Presidente de la República

ERNESTO JULIO ÁLVAREZ MIRANDA
Presidente del Consejo de Ministros

REPÚBLICA DEL PERÚ

ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA VALAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

Decreto Legislativo

N° 1700

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

Que, mediante la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional, el Congreso de la República ha delegado en el Poder Ejecutivo la facultad de legislar, entre otros, en materia de seguridad y lucha contra la criminalidad organizada, por el plazo de sesenta (60) días calendario, computados a partir del día siguiente de su publicación;

Que, el subnumeral 2.1.14 del numeral 2.1 del artículo 2 de la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional, faculta al Poder Ejecutivo de modificar la Ley N° 30096, Ley de Delitos Informáticos, incorporando como delito conductas vinculadas a la adquisición, comercialización y tráfico de datos informáticos, banco de datos, entre otros ilícitamente obtenidos;

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

Que, en ese sentido, resulta necesario modificar la Ley Nº 30096, Ley de Delitos Informáticos, incorporando el delito de adquisición, posesión y tráfico ilícito de datos informáticos, a fin de fortalecer la seguridad y confianza digital a nivel nacional, comprendiendo la ciberseguridad, y materializar la tutela penal reforzada del derecho fundamental a la autodeterminación informativa, elevando el estándar de protección frente a conductas que generan afectaciones masivas y sistemáticas en el entorno digital;

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica

Que, la comercialización y tráfico ilícito de información digital obtenida sin consentimiento del titular o mediante la vulneración de sistemas de seguridad constituye una conducta de elevada lesividad social, en tanto afecta de manera directa la seguridad de los datos, la autodeterminación informativa y la confianza en los sistemas informáticos, generando un riesgo estructural para la seguridad ciudadana y el adecuado funcionamiento de los servicios públicos y privados en el entorno digital;

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

Que, de acuerdo a lo dispuesto en el literal j) del numeral 41.1 del artículo 41 del Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, aprobado mediante Decreto Supremo N° 023-2025-PCM, las entidades públicas están exceptuadas de presentar expediente Análisis de

ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA LAFUERTE FALCON
FEDATARIA DEL CONSEJO DE MINISTROS

Impacto Regulatorio Ex Ante (AIR Ex Ante) a la Comisión Multisectorial de Calidad Regulatoria (CMCR) en el caso de disposiciones normativas en materia penal, o que regulan los procesos en vía judicial (como códigos o leyes procesales), por lo que la presente norma se encuentra excluida del alcance AIR Ex Ante al estar inmersa en el supuesto antes descrito;

De conformidad con lo establecido en el artículo 104 de la Constitución Política del Perú, y en ejercicio de la facultad delegada en el subnumeral 2.1.14 del numeral 2.1 del artículo 2 de la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo a dar cuenta al Congreso de la República:

Ha dado el Decreto Legislativo siguiente:

DECRETO LEGISLATIVO QUE MODIFICA LA LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS, INCORPORANDO EL DELITO DE ADQUISICIÓN, POSESIÓN Y TRÁFICO ILÍCITO DE DATOS INFORMÁTICOS

Artículo 1.- Objeto

El presente Decreto Legislativo tiene por objeto modificar la Ley Nº 30096, Ley de Delitos Informáticos, incorporando un tipo penal autónomo que sancione la posesión, compra, recepción, venta, comercialización, intercambio, facilitamiento o tráfico ilícito de datos informáticos obtenidos sin consentimiento de su titular o mediante la vulneración de sistemas de seguridad o la comisión de un delito informático.

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

Artículo 2.- Finalidad

La finalidad del presente Decreto Legislativo es fortalecer la seguridad y confianza digital a nivel nacional, incluyendo la ciberseguridad, y materializar la tutela penal reforzada del derecho fundamental a la autodeterminación informativa, elevando el estándar de protección frente a conductas que generan afectaciones masivas y sistemáticas en el entorno digital.

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

Artículo 3.- Modificación de la Ley Nº 30096, Ley de Delitos Informáticos, incorporando el artículo 12-A

Se modifica la Ley N° 30096, Ley de Delitos Informáticos, incorporando el artículo 12-A, el cual queda redactado en los siguientes términos:

MINISTERIO DEL INTERIOR - DIRECCIÓN CONTRA EL CRIMEN ORGANIZADO - V°B°

S. DE LA CRUZ Q.

ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA VELAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

"Artículo 12-A.- Adquisición, posesión y tráfico ilícito de datos informáticos

El que posee, compre, recibe, comercialice, vende, facilite, intercambie o trafique datos informáticos, credenciales de acceso o bases de datos personales, teniendo conocimiento o debiendo presumir que se obtuvo sin consentimiento de su titular o mediante la vulneración de sistemas de seguridad o la comisión de un delito informático, es reprimido con pena privativa de libertad no menor de cinco (5) ni mayor de ocho (8) años y con ciento ochenta (180) a trescientos sesenta y cinco (365) días-multa.

La pena privativa de libertad es no menor de ocho (8) ni mayor de diez (10) años, e inhabilitación, cuando:

a) El agente actúa como integrante de una organización criminal;

b) Se cause perjuicio patrimonial grave o afectación a una pluralidad de personas; o

c) La base de datos es procesada o custodiada por una entidad pública.

Queda exceptuada de responsabilidad penal la adquisición, posesión, intercambio o tratamiento de datos informáticos cuando estas conductas se realicen con autorización expresa del titular, conforme a la Ley N° 29733, Ley de Protección de Datos Personales, en cumplimiento de un mandato judicial o administrativo emitido conforme a ley, o en el ejercicio legítimo de derechos fundamentales o de funciones legalmente reconocidas, siempre que no exista finalidad de aprovechamiento ilícito ni de comercialización indebida de la información".

Artículo 4.- Financiamiento

La implementación del presente Decreto Legislativo se financia con cargo al presupuesto de las instituciones públicas involucradas, sin demandar recursos adicionales al Tesoro Público.

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

Artículo 5.- Publicación

El presente Decreto Legislativo es publicado en la Plataforma Digital Única del Estado Peruano para la Orientación al Ciudadano (www.gob.pe) y en la sede digital del Ministerio del Interior (www,gob.pe/mininter) y del Ministerio de Justicia y Derechos Humanos (www,gob.pe/minjus), el mismo día de su publicación en el Diario Oficial "El Peruano".

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica

Artículo 6.- Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros, el Ministro del Interior y el Ministro de Justicia y Derechos Humanos.

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA LLAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

POR TANTO:

Mando se publique y cumpla, dando cuenta al Congreso de la República.

Dado en la Casa de Gobierno, en Lima, a los veintitrés días del mes de enero del año dos mil veintiseis

S. DE LA CRUZ Q.

JOSÉ ENRIQUE JERÍ ORÉ
Presidente de la República

VICENTE TIBURCIO ORBEZO
Ministro del Interior

ERNESTO JULIO ÁLVAREZ MIRANDA
Presidente del Consejo de Ministros

WALTER ELEODORO MARTÍNEZ LAURA
Ministro de Justicia y Derechos Humanos

EXPOSICIÓN DE MOTIVOS

DECRETO LEGISLATIVO QUE MODIFICA LA LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS, INCORPORANDO EL DELITO DE ADQUISICIÓN, POSESIÓN Y TRÁFICO ILÍCITO DE DATOS INFORMÁTICOS

I. OBJETO

El presente Decreto Legislativo tiene por objeto modificar la Ley Nº 30096, Ley de Delitos Informáticos, incorporando un tipo penal autónomo que sancione la posesión, compra, recepción, venta, comercialización, intercambio, facilitamiento o tráfico ilícito de datos informáticos obtenidos sin consentimiento de su titular o mediante la vulneración de sistemas de seguridad o la comisión de un delito informático.

II. FINALIDAD

La finalidad del presente Decreto Legislativo es fortalecer la seguridad y confianza digital a nivel nacional, comprendiendo dentro de dicho marco la ciberseguridad, entendida como la capacidad del Estado para prevenir, detectar, investigar y sancionar conductas que afectan la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos. Asimismo, la norma busca materializar una tutela penal reforzada del derecho fundamental a la autodeterminación informativa, frente a prácticas ilícitas que generan afectaciones masivas y sistemáticas en el entorno digital.

III. MARCO LEGAL

La presente norma se sustenta en un análisis de constitucionalidad y convencionalidad, asegurando su coherencia con el ordenamiento jurídico nacional y los compromisos internacionales asumidos por el Estado peruano.

3.1. Constitución Política del Perú

El presente Decreto Legislativo garantiza la protección de derechos fundamentales consagrados en la Carta Magna, elevando su tutela al ámbito penal frente a las nuevas amenazas del entorno digital:

> ***Artículo 2. Derechos fundamentales de la persona***
>
> *Toda persona tiene derecho:*
>
> *(...)*
>
> *6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.*
>
> *(...)*
>
> *10. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.*
>
> *Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.*

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

Los documentos privados obtenidos con violación de este precepto no tienen efecto legal.

Los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo por orden judicial.

Artículo 44. Deberes del Estado

Son deberes primordiales del Estado: defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

Asimismo, es deber del Estado establecer y ejecutar la política de fronteras y promover la integración, particularmente latinoamericana, así como el desarrollo y la cohesión de las zonas fronterizas, en concordancia con la política exterior.

Artículo 104. Delegación de facultades al Poder Ejecutivo

El Congreso puede delegar en el Poder Ejecutivo la facultad de legislar, mediante decretos legislativos, sobre materia específica y por el plazo determinado establecidos en la ley autoritativa.

No pueden delegarse las materias que son indelegables a la Comisión Permanente.

Los decretos legislativos están sometidos, en cuanto a su promulgación, publicación, vigencia y efectos, a las mismas normas que rigen para la ley.

El presidente de la República da cuenta al Senado o a la Comisión Permanente, de cada decreto legislativo emitido, de acuerdo con el procedimiento establecido por el Reglamento del Senado.

3.2. Convenio sobre la ciberdelincuencia - Convenio de Budapest

La norma cumple con los estándares internacionales vinculantes para el Perú, entre ellos el Convenio sobre la Ciberdelincuencia, que establece:

Artículo 6 - Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;

ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - V°B° - S. DE LA CRUZ Q.

posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

3.3. Ley Nº 30096, Ley de delitos informáticos

El presente Decreto Legislativo se integra orgánicamente a este cuerpo normativo especial. Actualmente, la Ley Nº 30096 sanciona principalmente el "acceso ilícito" en el Artículo 2 del citado cuerpo normativo. La presente modificación incorpora una sanción autónoma a la fase de adquisición, posesión y tráfico ilícito de datos informáticos, cubriendo el vacío legal respecto a los intermediarios que lucran con la información obtenida ilícitamente, perfeccionando así el catálogo de tipos penales informáticos.

3.4. Ley Nº 29733, Ley de protección de datos personales

Mientras la Ley Nº 29733 regula el tratamiento lícito y sanciona administrativamente las infracciones por negligencia o mal manejo de datos, la presente norma penal se reserva para las conductas más graves, cuando se trata de conductas de tráfico doloso y comercial de dicha información.

3.5. Ley Nº 30077, Ley contra el crimen organizado

La incorporación del delito tiene un efecto procesal inmediato, en tanto, al tipificarse dentro de la Ley de Delitos Informáticos y dada la gravedad de la pena, el delito de adquisición, posesión y tráfico ilícito de datos informáticos podrá ser subsumido bajo los alcances de la Ley Nº 30077. Esto habilita al Ministerio Público para emplear técnicas especiales de investigación (agentes encubiertos, videovigilancia, levantamiento del secreto de las comunicaciones) para desarticular las redes complejas que operan detrás de los mercados negros de datos.

3.6. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento; Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital

La presente normativa se articula con el marco vigente de Gobierno Digital, Seguridad Digital y Confianza Digital, regulado por el Decreto Legislativo N° 1412, el Decreto de Urgencia N° 006-2020, el Decreto de Urgencia N° 007-2020, y sus normas reglamentarias, así como con las competencias del Ministerio de Justicia y Derechos Humanos en materia de protección de datos personales y política criminal. En ese contexto, la tutela penal reforzada del derecho a la autodeterminación informativa constituye un componente esencial para consolidar la seguridad y confianza digital a nivel nacional.

3.7. Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional

En lo que respecta al presente decreto legislativo, su emisión se sustenta en la materia delegada en el subnumeral 2.1.14 del numeral 2.1 del artículo 2 de la Ley N° 32527, norma que dispone que el Poder Ejecutivo está facultado para legislar en materia de seguridad y lucha contra la criminalidad, y en ese marco, modificar la Ley 30096, Ley de Delitos Informáticos, incorporando como delito conductas vinculadas a la adquisición, comercialización y tráfico de datos informáticos, banco de datos, entre otros ilícitamente obtenidos.

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica

MINISTERIO DEL INTERIOR - V°B° - Dirección General contra el Crimen Organizado

S. DE LA CRUZ Q.

Artículo 2. Materias de la delegación de facultades legislativas

2.1. Seguridad y lucha contra la criminalidad organizada

(...)

2.1.14. Modificar la Ley 30096, Ley de Delitos Informáticos, para incorporar como delitos las conductas vinculadas a la adquisición, comercialización y tráfico de datos informáticos, banco de datos, entre otros ilícitamente obtenidos.

(...)

IV. FUNDAMENTO TÉCNICO

La presente norma tiene por objeto modificar la Ley Nº 30096, Ley de Delitos Informáticos, incorporando un nuevo tipo penal que sancione de manera expresa la compra, comercialización y tráfico ilícito de datos informáticos, incluyendo aquellos organizados en bases de datos, cuando estos hayan sido obtenidos sin el consentimiento de su titular o mediante la comisión de delitos informáticos, cerrando un vacío normativo actualmente existente en el ordenamiento penal peruano.

A efectos del presente Decreto Legislativo, la expresión "datos informáticos" se emplea en su acepción técnico-jurídica amplia, conforme a la Ley Nº 30096 y a los estándares del Convenio sobre la Ciberdelincuencia (Convenio de Budapest), comprendiendo dentro de dicho concepto a las credenciales de acceso, bases de datos personales y cualquier otra información digital susceptible de tratamiento informático. En consecuencia, la denominación del delito no limita ni restringe el alcance material de las conductas tipificadas.

4.1. IDENTIFICACIÓN DEL PROBLEMA PÚBLICO

El problema público identificado radica en la inexistencia de una tipificación penal autónoma que sancione de forma directa y específica a quienes adquieren, compran, comercializan, poseen o trafican datos informáticos o bases de datos obtenidas ilícitamente, pese a que dichas conductas constituyen un eslabón esencial dentro de la dinámica económica delictiva asociada a la ciberdelincuencia y al crimen organizado.

Si bien el ordenamiento jurídico penal sanciona la fase inicial de la conducta —esto es, la obtención ilícita de datos mediante el acceso no autorizado a sistemas informáticos (artículo 2 de la Ley Nº 30096)—, no contempla una respuesta penal adecuada frente al denominado "mercado negro de datos", que permite la monetización, reutilización y expansión del daño causado por el delito informático primigenio.

Este vacío normativo favorece la impunidad de los agentes que, sin haber ejecutado el acceso ilícito, financian, incentivan y sostienen la actividad criminal mediante la adquisición y comercialización de información sensible, la cual es posteriormente utilizada para la comisión de delitos graves como extorsión, fraude informático, suplantación de identidad, secuestro, trata de personas y otros delitos vinculados al crimen organizado. Lo cual evidencia una falla estructural de tutela punitiva, caracterizada por una ausencia de regulación específica en el ordenamiento penal peruano que sancione el ciclo económico del cibercrimen.

Desde una perspectiva constitucional, el problema no se limita a la sustracción de información, sino que trasciende a la vulneración sistemática del derecho fundamental a la

autodeterminación informativa y a la intimidad personal, reconocidos en el artículo 2, inciso 6, de la Constitución Política del Perú.

> *Artículo 2.*
>
> *Toda persona tiene derecho:*
>
> *(...)*
>
> *6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.*
>
> *(...)*

Al respecto, el Tribunal Constitucional ha desarrollado el contenido de este derecho, denominado Autodeterminación Informativa, estableciendo líneas jurisprudenciales que justifican la necesidad de sancionar el tráfico de datos. Así, por ejemplo, en la STC Nº 04739-2007-PHD/TC (Fundamentos 2-4), el Tribunal ha establecido el alcance del control de los datos de un ciudadano, concluyendo que la autodeterminación informativa no se limita a una protección defensiva, sino que consiste en:

> "La serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos".

Asimismo, en el STC Nº 1797-2002-HD/TC (Caso Wilo Rodríguez, f.j. 3), se ha establecido que:

> "Mientras que el derecho a la intimidad protege la vida privada [rechazando intromisiones], el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen".

En ese sentido se reconoce que el ciudadano debe tener el dominio sobre quién, cómo y para qué se usan sus datos, dominio que es arrebatado por las organizaciones criminales al comercializarlos sin consentimiento.

El máximo intérprete de la Constitución en el Caso Jhonny Colmenares vs. Centrales de Riesgo (STC Nº 04227-2009-PHD/TC), se pronunció sobre la ilicitud de comercializar datos personales, declarando inconstitucional que se comercialicen datos (como la dirección domiciliaria o el teléfono) bajo el contexto de una evaluación crediticia, señalando que dicha comercialización "carece de relevancia y resulta desproporcionada", vulnerando el derecho fundamental.

En consecuencia, la posición jurisprudencia a nivel del Tribunal Constitucional es uniforme y concluye que la comercialización de datos sin consentimiento es una conducta lesiva que merece reproche jurídico, lo cual se pretende elevar a categoría penal.

Desde una perspectiva dogmática-penal, se identifica una disfuncionalidad en la Ley Nº 30096, Ley de Delitos Informáticos. Como se ha venido adelantando, la legislación vigente sanciona eficazmente la "etapa de intrusión" o acceso ilícito (hacking, artículo 2 de la Ley

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B° - S. DE LA CRUZ Q.

30096). Sin embargo, existe un vacío de punibilidad en la etapa de agotamiento y monetización. Actualmente, el sujeto que no *"hackea"*[1], pero que dolosamente compra, almacena y revende bases de datos obtenidos ilícitamente, opera en un umbral de atipicidad o enfrenta imputaciones difusas (como una receptación patrimonial que no se ajusta a la naturaleza de los bienes intangibles).

En ese sentido, al no sancionar de manera autónoma y con la gravedad debida a los "intermediarios" (*brokers*[2] de datos) y "compradores finales", el Estado permite que se mantenga el incentivo económico del delito, provocando un incentivo perverso del mercado ilícito de datos informáticos. Este vacío legal actúa como el motor financiero que sostiene a las organizaciones criminales, las cuales utilizan estas bases de datos (bancarias, policiales, de identidad) como insumo indispensable para planificar delitos de alto impacto como la extorsión, el fraude bancario masivo y el sicariato digital.

4.2. ANÁLISIS DEL ESTADO ACTUAL DE LA SITUACIÓN FÁCTICA

4.2.1. Evidencia empírica y casos documentados

Existen evidencias concretas que confirman la comercialización de datos informáticos a través de las redes sociales, siendo uno de los principales indicadores de que los datos tienen un valor comercial, en tanto, tras las filtraciones masivas se advierten "ofertas" en la *dark web*[3], redes sociales y otros foros clandestinos de las bases de datos, obtenidas. A continuación, se detallan los datos fácticos y los casos documentados en el país:

A) **Caso del "Zorrito Run Run" (2022):** Este fue uno de los casos más mediáticos en el país. Una plataforma denominada "Zorrito Run Run" filtró y puso a la venta los datos personales de millones de peruanos. La información incluía nombres completos, números de DNI, direcciones, números telefónicos e incluso datos de familiares.

Al respecto, el Tercer Despacho de la Fiscalía Corporativa en Ciberdelincuencia informó que la banda es investigada por los delitos de acceso ilícito, en tanto, habrían accedido a datos de entidades del Estado, bancos, AFPs, entre otros. Ellos ofertaban los datos personales obtenidos ilícitamente – nombre, dirección, huella dactilar, firmas, lugar de trabajo, récord crediticio – a través de WhatsApp y Telegram. El grupo tenía más de 350 integrantes y cobraban hasta S/ 120 por datos, incluidos otros servicios como acceso a Netflix o similares usando la data robada[4].

B) **Filtración de Interbank (2024):** El 30 de octubre del 2024, un delincuente cibernético detrás del usuario "kzoldiyck" anunció en "Breach Forums" —un foro de la dark web — que había accedido a datos relacionados a las cuentas bancarias de

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno - MI

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica - MI

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B° - S. DE LA CRUZ Q.

[1] Definiciones de *la Real Academia Española*. Adapt. del ingl. *to hack,* con el suf. *-ear. En español,* jaquear significa Introducirse de forma no autorizada en un sistema informático.

[2] Definiciones de *la Real Academia Española*. Nombre masculino y femenino Economía. Agente intermediario en operaciones financieras o comerciales que percibe una comisión por su intervención.

[3] Parte oculta de Internet accesible solo mediante navegadores especiales

[4] https://ebiz.pe/noticias/zorrito-run-run-detienen-y-encarcelan-a-presuntos-autores-del-delito/ Fecha de acceso el 27/08/2025

más de 3 millones de clientes del Banco Internacional del Perú (Interbank), y que los estaba poniendo a la venta.

La información fue posteriormente ofrecida a través de la red social Telegram. Este caso es un claro ejemplo de cómo las redes sociales se utilizan como un canal para exhibir y negociar la venta de datos robados de otras fuentes.

El 5 de noviembre del 2024, el abogado Aníbal Quiroga León señaló —en representación de Interbank, ante la Comisión de Defensa del Consumidor del Congreso— que la entidad no sabe desde dónde opera el criminal que filtró la información de sus clientes. También dijo que, probablemente, será difícil ubicarlo. OjoPúblico ha podido conocer que el ciberdelincuente creó su cuenta en el portal Breachforums el 18 de agosto del 2024 y que, previamente, había vendido información de países como Egipto, Turquía e Israel. En el caso de Interbank, de acuerdo a la evidencia recabada a la fecha, empezó a comercializar datos de los clientes desde el 30 de octubre del 2024[5].

En su primera publicación, "kzoldiyck", seudónimo que utilizaba por esa fecha en la *dark web*, anunció que supuestamente tenía 3,7 terabytes de datos personales y accesos a cuentas bancarias, que iría vendiendo por partes. En esa misma publicación, agregó un link oculto al que solo se podía acceder con el pago de un aproximado de ocho créditos; para obtener los créditos es necesario realizar pagos con criptomonedas. Lo mínimo que se puede recargar es ocho euros, que equivalen a 30 créditos en esta plataforma.

En los días posteriores, el usuario —que cambió su apodo de "kzoldiyck" a "m0riarty"— publicó nuevos mensajes anunciando que la información se podría adquirir a través de Telegram. El 05 de noviembre del 2024, volvió a publicar indicando que había recibido muchas solicitudes por la data robada y, por ello, ofrecía nueva información de clientes de Interbank y datos de otras empresas.

Ante ello, el cuarto despacho de la fiscalía en ciberdelincuencia de Lima Centro inició diligencias preliminares contra los que resulten responsables del presunto delito informático contra datos y sistemas informáticos.

C) Reportaje de "Latina Noticias" emitido el 6 de abril del 2025 con el título "¿Como un extorsionador obtiene tus datos? Criminales ofrecen y venden información por web ilegal" [6]:

El reportaje muestra un mercado global, donde los "hackers" criminales ofrecen información sensible de diferentes países, entre ellos, "Bridge Forums", como uno de los tantos espacios digitales a través del cual se obtiene información de instituciones peruanas públicas o privadas. Esta información puede ser comercializada en la web oscura o dark web[7], en la red de mercados al menudeo, como en el Centro de Lima o redes sociales como Telegram.

"Breach Forums", el foro en línea que sirve de mercado para criminales, surgió en el 2022 en reemplazó de otra página similar confiscada y bloqueada el 21 de marzo

[5] https://ojo-publico.com/5390/ciberdelincuencia-la-ruta-detras-del-robo-datos-interbank Fecha de acceso: 27/08/2025

[6] https://www.youtube.com/watch?v=fMUFbISDNfs Fecha de consulta: 21 de octubre del 2025.

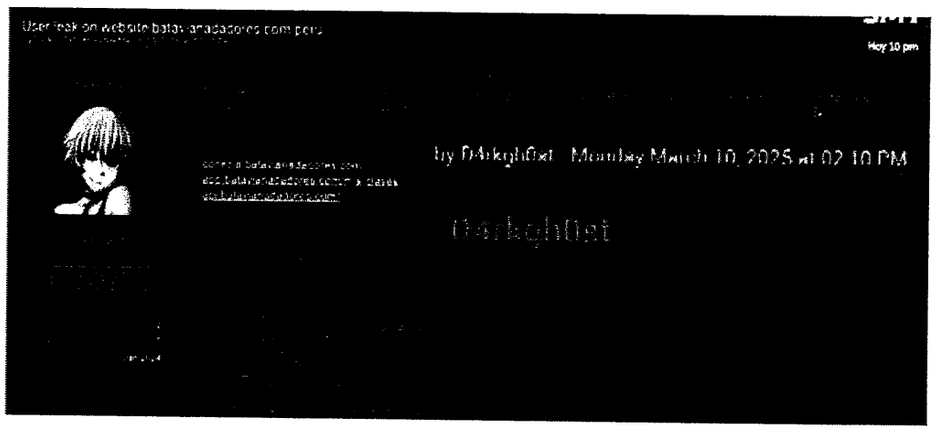
[7] Dark web: Es una parte de Internet compuesta por sitios web no indexados por motores de búsqueda y que, teóricamente, sólo pueden visitarse con completo anonimato

S. DE LA CRUZ Q.

del 2023 y cuyo creador fue Conor Brian Fitzpatrick, quien fue detenido por el FBI de Estados Unidos. Sin embargo, cada vez que las autoridades logran bloquear el sitio, quienes lo gestionan se encargan de restablecerlo, es como un ladrón que cambia de residencia cada vez que está a punto de ser capturado.

Perseguidos por el FBI[8] y otras autoridades de Europa, "Breach Forums" ha aumentado su nivel de seguridad para admitir nuevos miembros. Tras algunas semanas de pruebas el equipo de Latina Noticias, logró ingresar a este mercado digital y con la palabra clave Perú logrando advertir que se ofrecía lo siguiente:

> **C.1.-** El 10 de marzo del 2025, el usuario con el alias de "D4rkgh0st" [9], aseguró haber hackeado la información de los clientes de una conocida academia de natación en Surco (Academia de Natación Batavia Nadadores - Sede Surco). Nombres, teléfonos, correos de contacto, incluso el usuario y contraseña de la web.



El equipo de Latina Noticias, con la finalidad de demostrar que en esta web se trafica con información real, descargaron la data publicada por "D4rkgh0st" y al realizar la prueba con un usuario y contraseña, realizamos la prueba y en efecto, los datos proporcionados funcionaron:

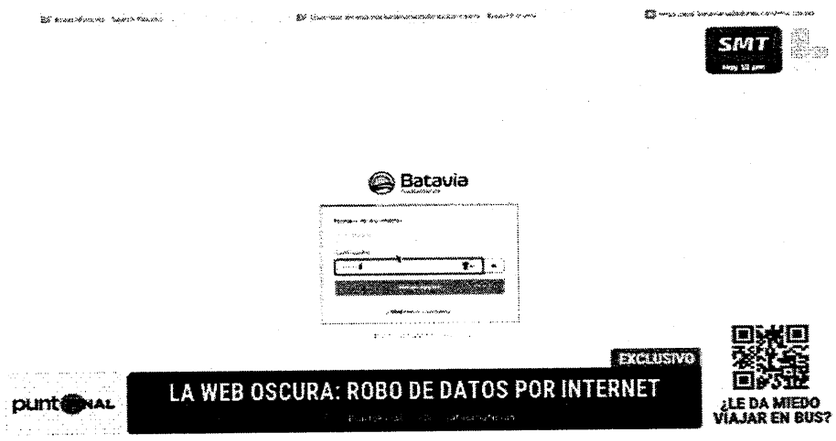
MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B°

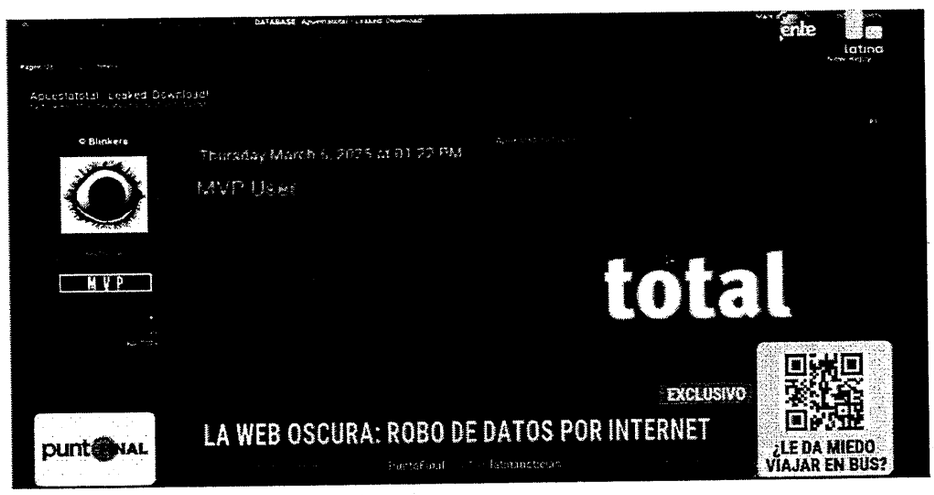
S. DE LA CRUZ Q.

[8] Federal Bureau of Investigation
[9] Fantasma Oscuro



De manera aleatoria, seleccionaron un número de teléfono y al realizar la llamada, contestó el padre de un alumno de la academia de natación, quién luego de conocer el contexto y motivo de la llamada, el padre de familia expresó encontrarse muy preocupado, porque su hijo es un menor de edad y conocer que datos tan delicados, personales, están al acceso de cualquiera, incrementa su ansiedad y angustia.

C.2.- El 6 de marzo de este 2025, otro ciberdelincuente con el alias de "MVP User" publicó en "Bridge Forums" un anuncio ofreciendo bajo la modalidad de pago, datos de la conocida casa de apuestas "Apuesta total", a modo de muestra, se publicó un pequeño extracto con una larga lista de nombres.



Al respecto, la empresa "Apuestatotal" mediante comunicado informó que el 6 de marzo del 2025 se detectó una irregularidad, pero en una base de datos de prueba usada solo con fines técnicos, asegurando que no se expusieron contraseñas o información sensible, ni información de tarjetas de ningún cliente.

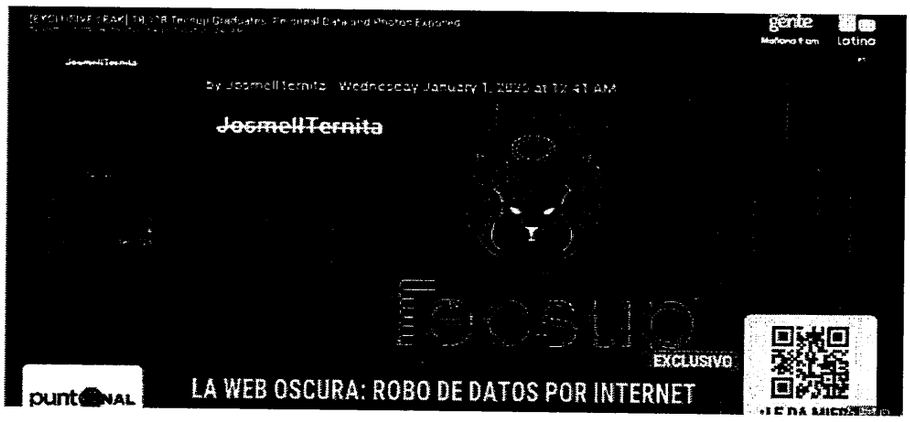
MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

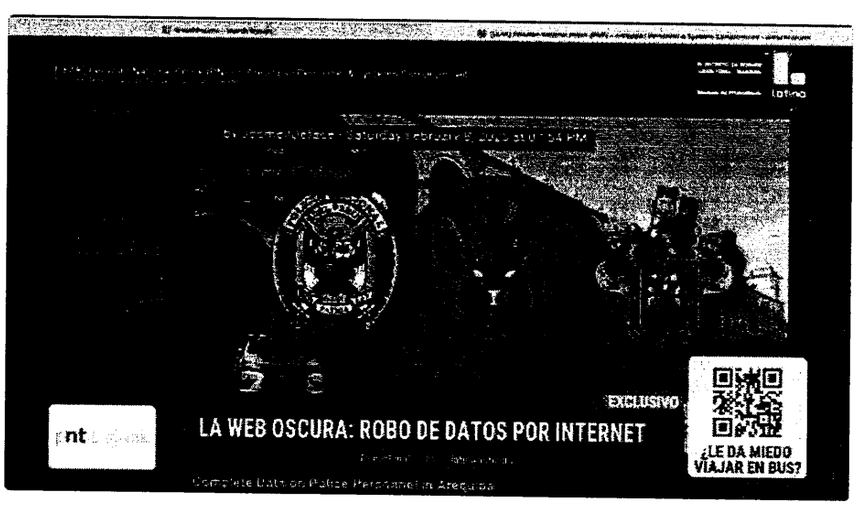
S. DE LA CRUZ Q.

C.3.- El 01 de enero del 2025, otro usuario de "Bridge Forums", identificado como "Josmell Ternita", aseguró tener información de un instituto superior privado (TECSUP), nombres, teléfonos, correos y hasta fotografías de los egresados de TECSUP. Se ubicó un enlace para descargar la información que ya no está activa. Sin embargo, en las imágenes de muestra que compartió el ciberdelincuente se pueden ver los datos de una veintena de personas.



En este contexto, Harold Moreno, periodista de Latina Noticias, llamó a uno de los números para verificar la información y efectivamente quedó corroborado que los datos proporcionados por "Josmell Ternita" eran correctos. Al respecto, Tecsup mediante un comunicado admitió el incidente, señaló que se vulneró una plataforma independiente de los sistemas académicos y administrativos, que no almacena datos sensibles, procediendo a cerrar temporalmente la plataforma y mejorar seguridad.

C.4.- No solamente las instituciones privadas son blancos de ciberataques, el Estado Peruano es la víctima más recurrente, el 8 de febrero del 2025, el usuario "JosmellDeface" en Bridge Forums hizo una publicación.



MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

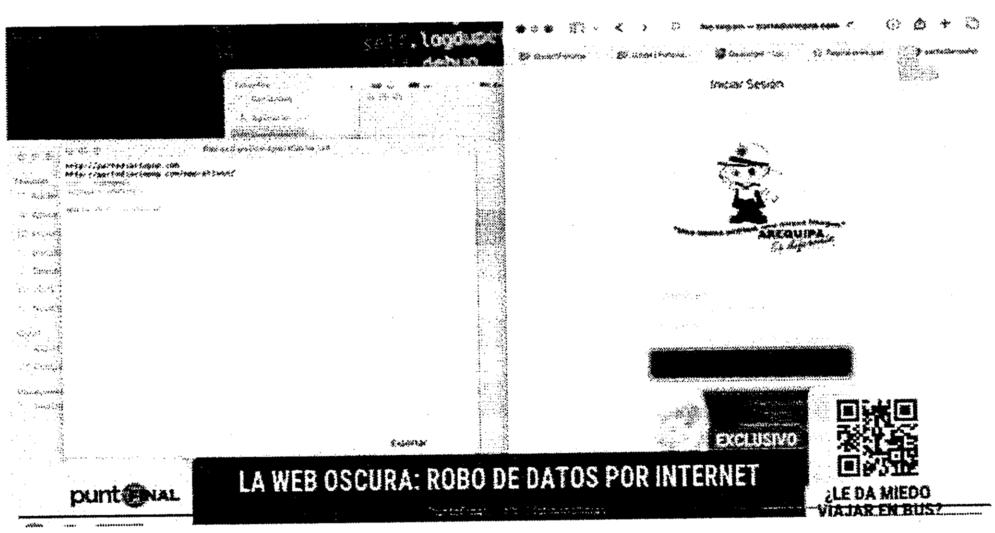
S. DE LA CRUZ Q.

Bajo la siguiente descripción consignada en idioma inglés:

> "Leaked information.
>
> Complete data on Police Personnel in Arequipa.
>
> - Full names, surnames, rank, position, and assigned police station
>
> - Current status: active services, leave, vacation , special commission, or medical treatment.
>
> - Shift schedules and duty assignments.
>
> - Personal and institutional phone numbers[10]" (...)

El equipo de Latina Noticias, tras un proceso largo y complicado para los no expertos en informática, logró descargar la información dividida en varias partes.

Latina Noticias, corroboró que a la fecha de emisión del reportaje se encontraba activa, en tanto, ingresaron con un usuario y contraseña.



Asimismo, verificaron que los datos policiales y números telefónicos eran correctos mediante una llamada telefónica.

Precisa el reportaje de Latina Noticias que, la forma de obtener esta información es variada, desde modalidades de hackeo o a través de *insiders*, esto es, personas que forman parte de una organización, de una empresa, de una municipalidad, del gobierno, de una institución gubernamental que

---

[10] Información filtrada.
Datos completos del personal policial en Arequipa.
Nombres, apellidos, rango, cargo y comisaría asignada.
Estado actual: servicio activo, licencia, vacaciones, comisión especial o tratamiento médico.
Horarios de turnos y asignación de funciones.
Números de teléfono personales e institucionales.

traiciona a su institución y brinda los accesos. Esta información ordenada permite crear una base de datos con un valor comercial, el cibercriminal puede vender la información, a delincuentes comunes o extorsionadores como compradores finales; los objetivos de los cibercriminales son variados, así como sus métodos.

Concluye el reportaje indicando que, la información obtenida ilícitamente por un cibercriminal puede ser ofrecida en la web oscura o también en mercados al menudeo como el Centro de Lima o por Telegram.

Por otro lado, existe evidencia concreta que la comercialización de datos informáticos no se limita al espacio de las redes sociales, sino también se extiende a espacios físicos como los ubicados en la Av. Wilson – Cercado de Lima.

A) Reportaje de "ATV Noticias" publicado en la plataforma Youtube el 15 de septiembre de 2025 con el título "¡Exclusivo! Inescrupulosos venden información de clientes VIP de bancos" [11]:

El reportaje muestra cómo las mafias acceden a bases de datos de clientes de bancos ofrecidos por menos de 100 soles.

La unidad de investigación de "Ocurre Ahora" de ATV Noticias, en las inmediaciones de la Av. Wilson del Cercado de Lima, a través de un "jalador", estableció contacto con una persona de sexo femenino[12] quien por 70 soles vendió una base de datos con 51,000 registros con nombres, apellidos, DNI, teléfono fijo, número de celular e información bancaria de distintos bancos, como el dinero disponible en las tarjetas de crédito de miles y miles de usuarios.

La mujer agrega que, "escúchame, también estoy consiguiendo este tipo de cliente, mira, este tiene 276 mil, lo que tiene en su cuenta", señalando que esta base de datos tiene un costo de S/. 3 000.00 soles por 5 mil registros, agrega que "esos son pedidos, ah, ya van 3 veces que me van pidiendo, hoy día tengo otro pedido. Para que me han pedido ... los que me han pedido dicen que es para una campaña política, no sé, yo no creo, porque tienen cantidad de dinero".

Daniel Subauste, especialista en Ciberseguridad, en el reportaje precisó que, eso permite a los ciberdelincuentes saber si eres una persona de interés para la extorsión, con la información de los montos máximos del préstamo que alguien puede adquirir se evidencia que se trata de una persona con cierto tipo de ingreso para ser extorsionada o no.

Jessica Lara, reportera de Ocurre Ahora de ATV, indica que la investigación periodística inició a raíz de una denuncia de un cliente de un banco y luego de varios días, llegaron al lugar ubicado en la Av. Wilson, añade que esta información les fue entregada en un USB. La reportera resalta que, existen categorías de información, denominados "documentos premium" con datos de personas que manejan mucho más dinero, de usuarios de bancos que manejan hasta más de 200,000 soles.

En el minuto 8:53 del reportaje, se observa las imágenes de la misma persona de sexo femenino, quien mostrando una conversación de Whatsapp desde su celular indica: "Mira, tengo varios clientes de banco. Ahí está, ¿ve? clientes de banco. Ellos

[11] https://www.youtube.com/watch?v=AWtGnxbuPiQ Fecha de consulta: 21 de octubre del 2025.
[12] A quién se conocería como "tía Gloria", según señala la periodista Mávila Milagros Huertas Centurión

poco a poco van avanzando y van pidiendo, van avanzando. Ahí les voy mandando cosas. Ahí esta es la fecha, de cuándo le he mandado también, el 03 del 09 del 2025, ve"

Resulta particularmente grave la comercialización de datos de efectivos policiales activos, detectada en febrero de 2025, que incluía nombres, rangos, teléfonos, turnos de servicio y situación administrativa, generando un riesgo directo para la seguridad ciudadana y el principio de autoridad.

De los casos reales documentados (Filtraciones Interbank, RENIEC, PNP), se concluye jurídicamente que nos enfrentamos a una conducta con autonomía delictiva, distinta al mero acceso ilícito, caracterizada por una lesividad pluriofensiva (afecta patrimonio y seguridad personal) y ejecutada bajo esquemas de criminalidad organizada. Estos elementos fácticos demuestran que la respuesta punitiva actual es insuficiente y exigen la creación de un tipo penal específico que contemple la cadena de comercialización y posesión como el eslabón crítico que financia y facilita la ciberdelincuencia en el Perú.

4.2.2. Evidencia cuantitativa que grafica el problema público

4.2.2.1. Incremento sostenido de incidencia por delitos cibernéticos

El aumento de las denuncias por ciberdelitos y las operaciones policiales son una muestra de la existencia de este mercado ilegal. Según la Defensoría del Pueblo, las denuncias por delitos informáticos se han incrementado considerablemente. En el INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia de la Defensoría del Pueblo del Perú13 se señala que, en el 2021, la Policía Nacional del Perú recibió casi 12,000 denuncias de ciberdelincuencia, con un 70% de ellas relacionadas con fraude informático. Muchas de estas estafas y fraudes se inician con la adquisición ilegal de datos personales, los cuales se obtienen de bases de datos filtradas y comercializadas en línea.

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

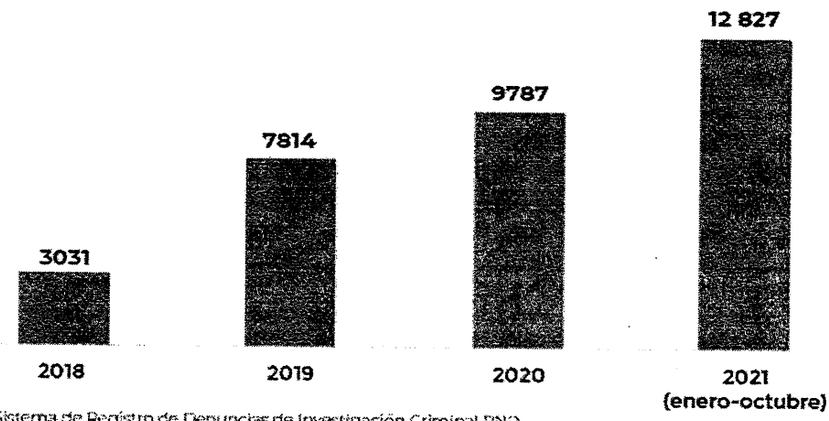
MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B°

S. DE LA CRUZ Q.

[13] Defensoría del Pueblo. La ciberdelincuencia en el Perú: estrategias y retos del Estado. INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia, Defensoría del Pueblo, 2023, https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

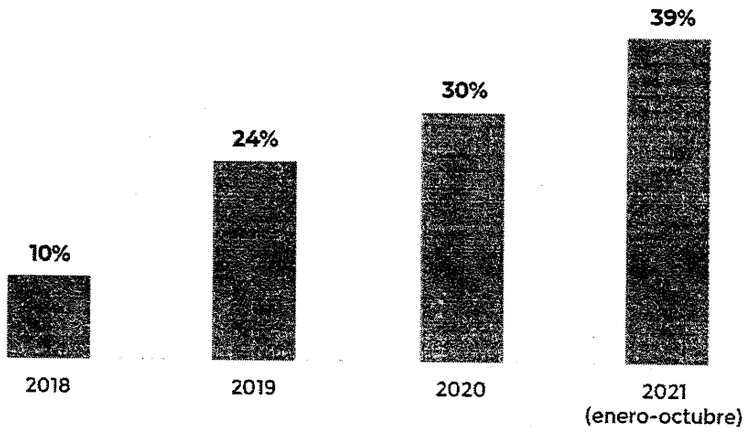
Gráfico N° 4
Denuncias de ciberdelitos ante la PNP
(Perú, 2018-2021)



Fuente: Sistema de Registro de Denuncias de Investigación Criminal PNP
Elaboración: Defensoría del Pueblo

37 Consejo Nacional de Política Criminal (2020). Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. Elaborado por la Dirección General de Asuntos Criminológicos del Minjus, a través del Observatorio Nacional de Política Criminal. Lima, página 67.

Gráfico N° 5
Tasas de denuncias de ciberdelitos ante la PNP por 100 mil habitantes
(Perú, 2018-2021)



Fuente: Sistema de Registro de Denuncias de Investigación Criminal PNP
Elaboración: Defensoría del Pueblo

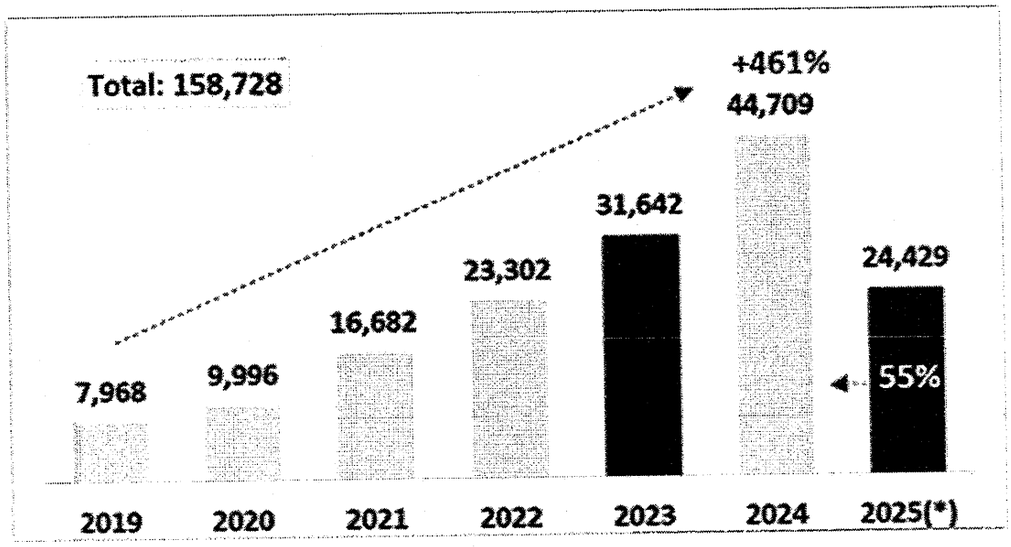
MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO
S. DE LA CRUZ O.

En los años posteriores a la fecha, el incremento de la tasa de denuncias por delitos informáticos se ha sostenido, reafirmando la tendencia al alza. Así muestran los datos obtenidos del Sistema Informático de Registro de Denuncias Policiales de la Policía Nacional del Perú al 2025.

Denuncias por delitos informáticos, 2019-2025 JUL

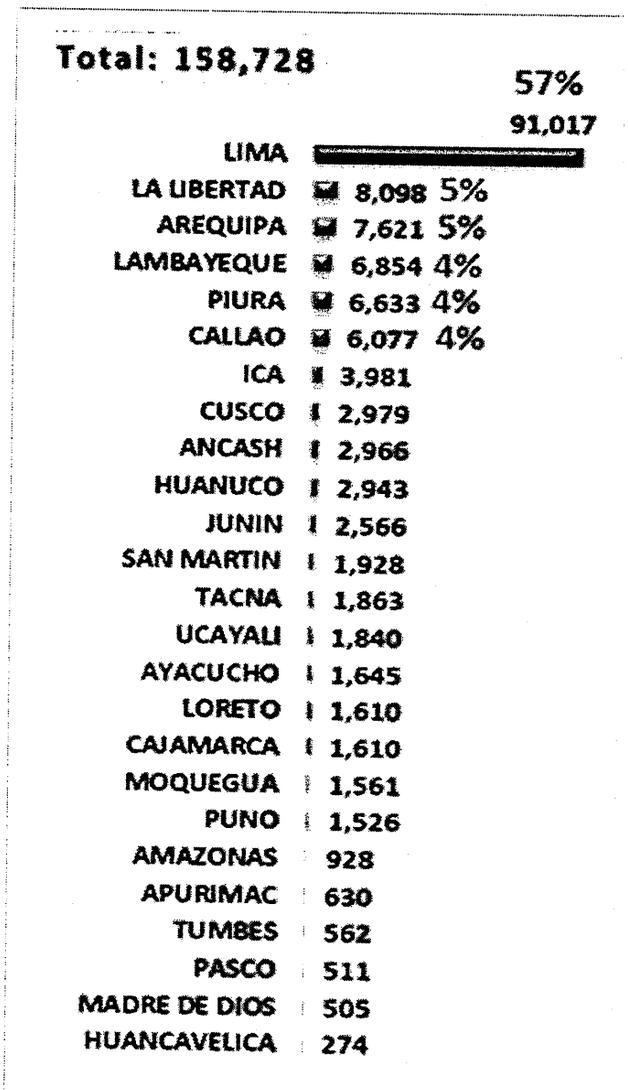


(*) Enero a julio
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

Los datos estadísticos del Sistema muestran el incremento consistente de incidencia de los delitos informáticos, concentrados en el departamento de Lima:

S. DE LA CRUZ Q.

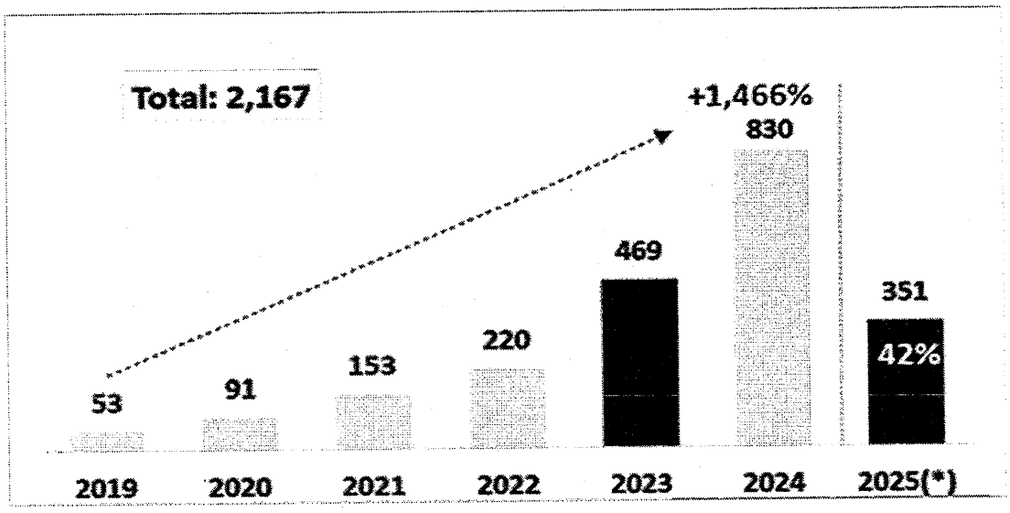
Denuncias por delitos informáticos, según departamento, 2019-2025JUL



Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

Frente a la cifra macro de las denuncias por delitos informáticos, es peculiar e importante mostrar el incremento desmesurado en +1,466% de incidencia por el delito de acceso ilícito (Artículo 2 de la Ley de delitos informáticos) que comprende las modalidades de vulneración de las medidas de seguridad de los sistemas informáticos y acceso no autorizado a los sistemas informáticos.

Denuncias por delitos informáticos, subtipo Contra datos y sistemas informáticos, modalidad: Acceso ilícito, 2019-2025JUL



(*) Enero a julio

Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

En otras palabras, en los años 2023, 2024 y en lo que va del 2025, se evidenció un alto índice de vulnerabilidad y acceso ilegal a los sistemas informáticos. Lo anterior deberá ser analizado en coherencia con los diversos reportajes periodísticos y operativos policiales (Latina Noticias, ATV Noticias, PNP - DGIS) que han documentado casos de venta de bases de datos con información bancaria, laboral, educativa o policial, tanto de entidades públicas como privadas.

4.2.2.2. Identificación de denunciados por delitos informáticos

El comparativo entre el total de denuncias por delitos informáticos y el número de ellas con identificación del(los) denunciado(s), arrojó que, entre el año 2019 al setiembre del 2025 se registró un total de 166,200 denuncias por delitos informáticos y sólo en 19,640 de ellas se identificó a los denunciados, esto representa un 12% del total. En tabla 1 se muestra esta información por cada año, incluyendo el total de denunciados.

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

MINISTERIO DEL INTERIOR - Dirección General de Asesoría Jurídica

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

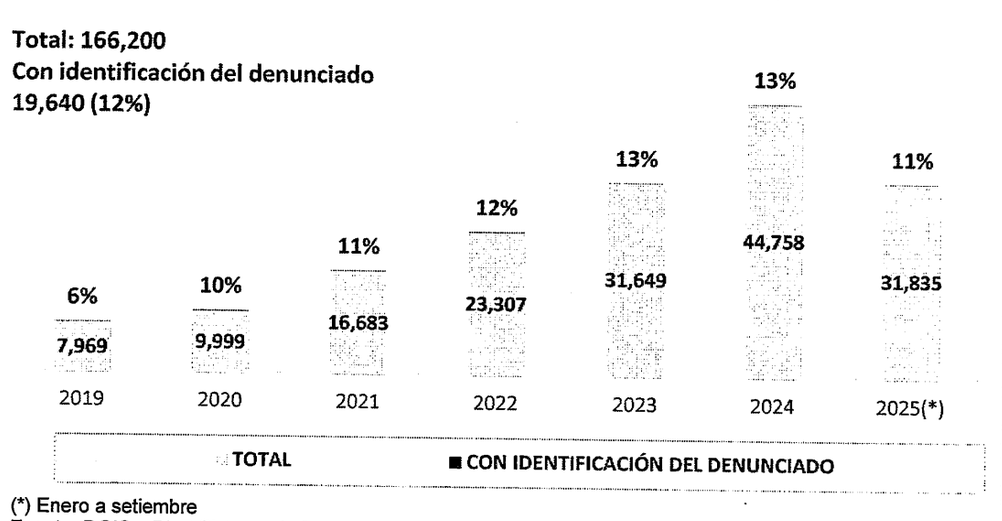
Tabla 1
Comparativo anual: Total denuncias por delitos informáticos versus con identificación del(los) denunciado(s), 2019-2025(*)

Año	Total Denuncias	Denuncias (Con identificación del denunciado)	Porcentaje	N° Denunciados
2019	7,969	513	6%	693
2020	9,999	1,002	10%	1,364
2021	16,683	1,918	11%	2,808
2022	23,307	2,789	12%	3,824
2023	31,649	4,010	13%	5,306
2024	44,758	5,945	13%	7,641
2025(*)	31,835	3,463	11%	4,422
TOTAL	**166,200**	**19,640**	**12%**	**26,058**

(*) Enero a setiembre
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL

Este análisis comparativo es posible advertir en el Gráfico 1, con fines de evidenciar el total de denuncias y la identificación del denunciado.

Gráfico 1
Comparativo anual: Total denuncias por delitos informáticos versus con identificación del(los) denunciado(s), 2019-2025(*)



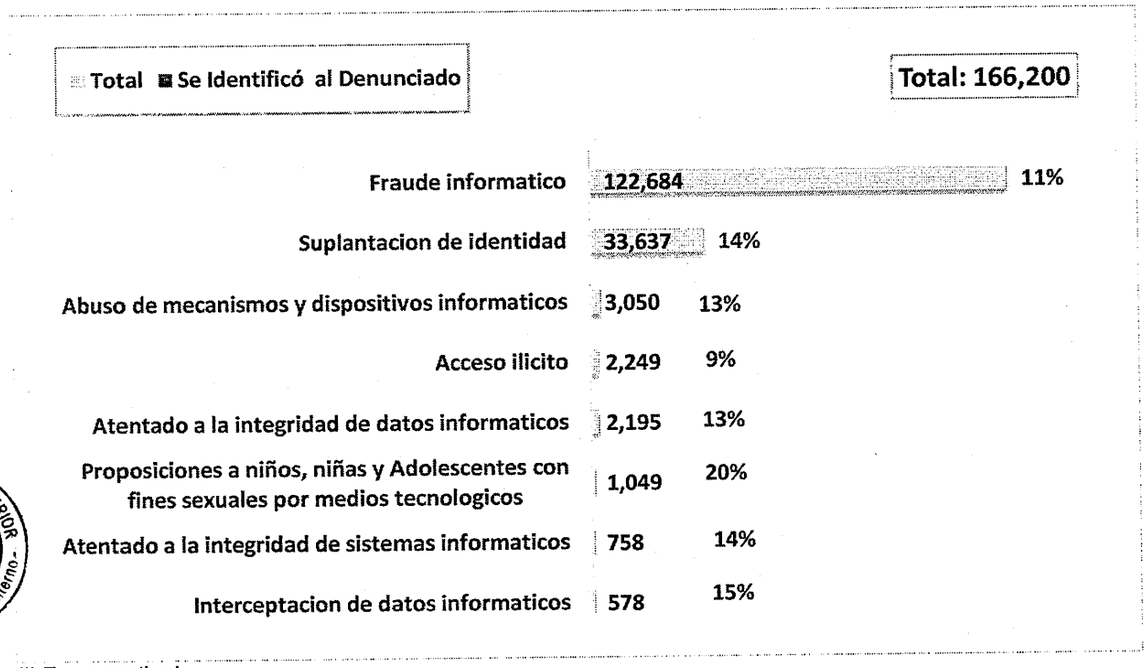
(*) Enero a setiembre
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL

Por otro lado, el comparativo realizado a nivel de modalidad de delito, muestra que, a nivel general hay mayor cantidad de denuncias con identificación del(los) denunciado(s) en la modalidad de "proposiciones a niños, niñas y adolescentes con fines sexuales, por medios tecnológicos" (20%), "interceptación de datos informáticos" (15%), "suplantación de identidad (14%) y "atentado a la integridad de

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -
MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CIBERDELINCUEN
S. DE LA CRUZ Q.
MINISTERIO DEL INTERIOR - Dirección General de Asesoría Jurídica -

sistemas informáticos" (14%), entre otros (Gráfico 2). En tablas 2 y 3 se muestra esta información por cada año.

Gráfico 2
Comparativo entre el total denuncias por delitos informáticos versus con identificación del(los) denunciado(s), por modalidad de delito informático, 2023-2025(*)



(*) Enero a setiembre
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

Tabla 2

Comparativo anual: Total denuncias por delitos informáticos versus con identificación del(los) denunciado(s), por modalidad de delito informático, según año 2019-2022

Modalidad de Delito Informático	2019			2020			2021			2022		
	Total	Se Identificó al Denunciado	%	Total	Se Identificó al Denunciado	%	Total	Se Identificó al Denunciado	%	Total	Se Identificó al Denunciado	%
Abuso de mecanismos y dispositivos informaticos	284	20	7%	586	77	13%	533	73	14%	480	66	14%
Acceso ilicito	53	6	11%	91	7	8%	153	16	10%	220	22	10%
Atentado a la integridad de datos informaticos	260	22	8%	174	23	13%	228	25	11%	292	33	11%
Atentado a la integridad de sistemas informaticos	75	7	9%	75	5	7%	90	17	19%	98	9	9%
Fraude informatico	6511	347	5%	7596	684	9%	12088	1402	12%	17814	2100	12%
Interceptacion de datos informaticos	84	11	13%	78	10	13%	70	14	20%	54	9	17%
Proposiciones a niños, niñas y Adolescentes con fines sexuales por medios tecnologicos	116	14	12%	168	32	19%	171	39	23%	145	29	20%
Suplantacion de identidad	586	86	15%	1231	164	13%	3350	332	10%	4204	521	12%
Total	**7,969**	**513**	**6%**	**9,999**	**1002**	**10%**	**16,683**	**1918**	**11%**	**23,307**	**2789**	**12%**

Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL

Tabla 3

Comparativo anual: Total denuncias por delitos informáticos versus con identificación del(los) denunciado(s), por modalidad de delito informático, según año 2023-2025(*) y total

Modalidad de Delito Informático	2023			2024			2025(*)			TOTAL		
	Total	Se Identificó al Denunciado	%	Total	Se Identificó al Denunciado	%	Total	Se Identificó al Denunciado	%	Total	Se Identificó al Denunciado	%
Abuso de mecanismos y dispositivos informaticos	339	43	13%	447	74	17%	381	53	14%	3,050	406	13%
Acceso ilicito	470	28	6%	831	93	11%	431	41	10%	2,249	213	9%
Atentado a la integridad de datos informaticos	429	50	12%	574	90	16%	238	35	15%	2,195	278	13%
Atentado a la integridad de sistemas informaticos	91	18	20%	234	36	15%	95	15	16%	758	107	14%
Fraude informatico	23848	2902	12%	31411	3970	13%	23416	2340	10%	122,684	13,745	11%
Interceptacion de datos informaticos	87	8	9%	116	17	15%	89	18	20%	578	87	15%
Proposiciones a niños, niñas y Adolescentes con fines sexuales por medios tecnologicos	141	28	20%	175	41	23%	133	27	20%	1,049	210	20%
Suplantacion de identidad	6244	933	15%	10970	1624	15%	7052	934	13%	33,637	4,594	14%
Total	**31,649**	**4010**	**13%**	**44,758**	**5945**	**13%**	**31,835**	**3463**	**11%**	**166,200**	**19,640**	**12%**

(*) Enero a setiembre

Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL

En ese sentido, la estadística oficial de la PNP revela una brecha de impunidad alarmante, a nivel policial, esto es que, el 88% de los delitos informáticos terminan

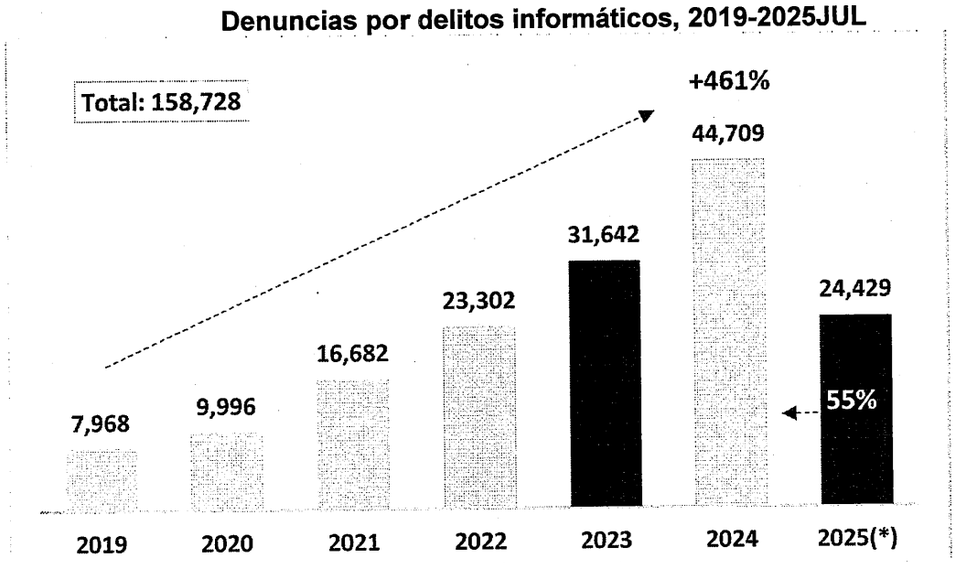
sin un responsable identificado. Esto se debe, entre otros motivos, a que la ley actual se enfoca en la intrusión técnica (difícil de probar), el acceso ilícito a los sistemas informáticos (sancionado en el artículo 2 de la Ley 30096), ignorando el eslabón más visible y rastreable de la cadena del mercado de comercialización. Al criminalizar la posesión y venta, el Estado tendrá mayores oportunidades de identificar a los responsables (el 12%), ya que el vendedor o poseedor de la base de datos es un objetivo estático, a diferencia del hacker que es volátil.

4.2.2.3. Reporte estadístico diferenciado entre el delito de "Acceso Ilícito" sancionado en el artículo 2 de la Ley 30096 y "Tráfico Ilegal de Datos Personales" prescrito en el artículo 154 del Código Penal

Resulta pertinente realizar un análisis comparativo entre las figuras delictivas recogidas en el Código Penal y la ley penal especial de delitos informáticos, a efectos de evidenciar su eficacia.

DELITOS INFORMÁTICOS (LEY N°30096, MODIFICADA POR LEY N°30171), SUBTIPO: DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS, MODALIDAD: ACCESO ILÍCITO

Denuncias por delitos informáticos, 2019-2025JUL



(*) Enero a julio
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

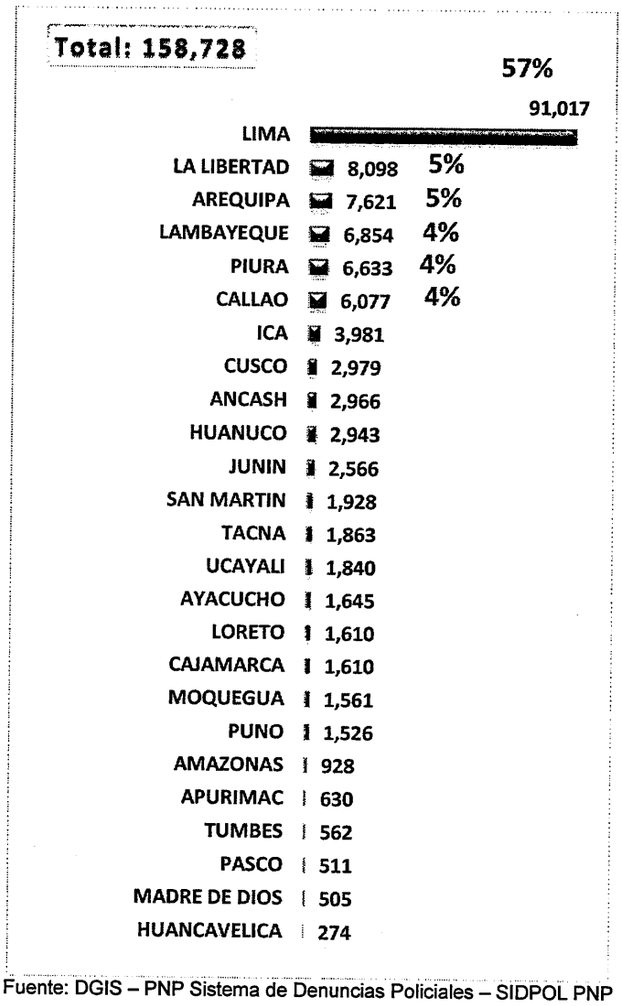
MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B°

S. DE LA CRUZ Q.

Denuncias por delitos informáticos, según departamento, 2019-2025JUL



Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

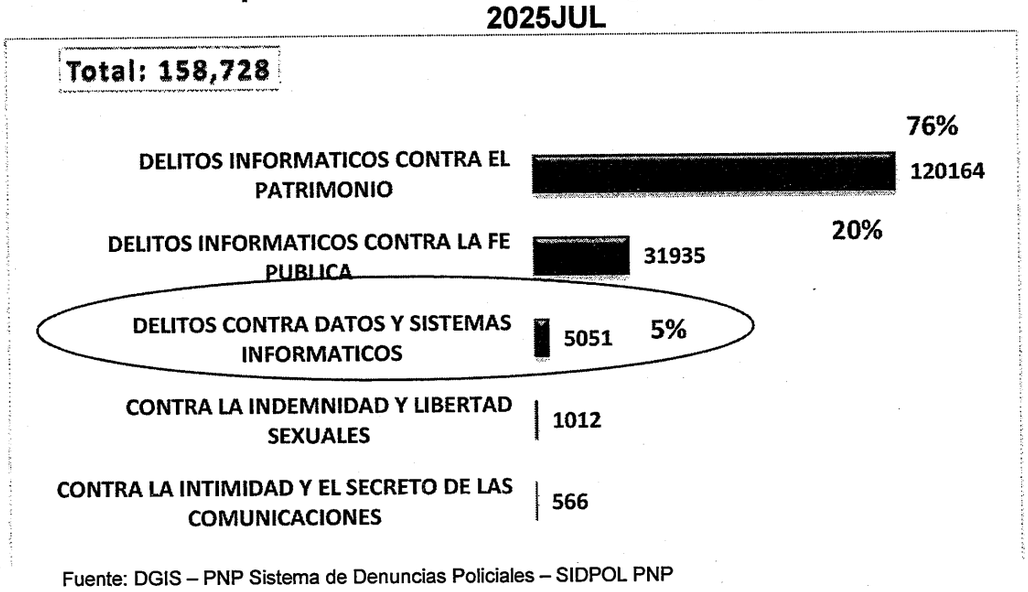
MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Dirección General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

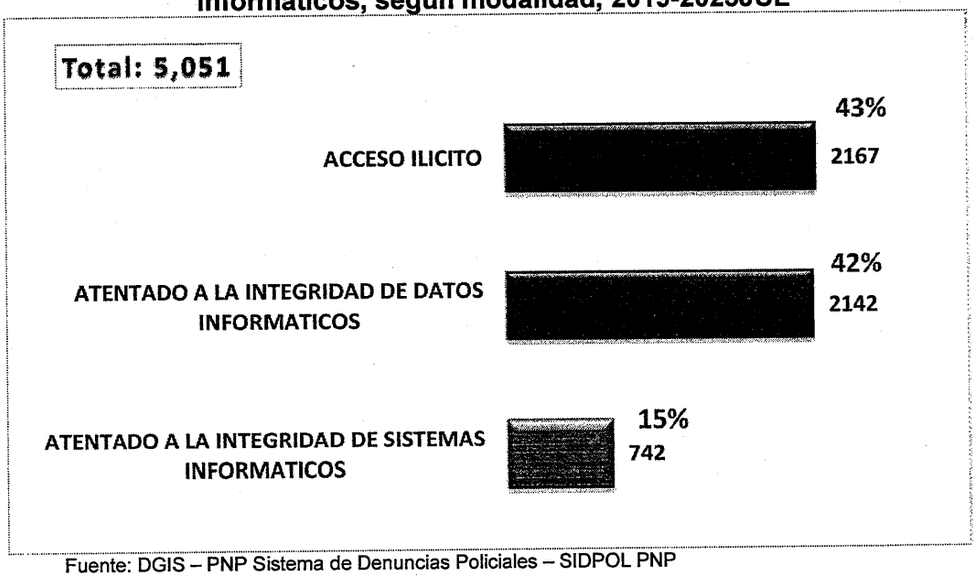
S. DE LA CRUZ Q.

Denuncias por delitos informáticos, según subtipo de delito, 2019-2025JUL



Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

Denuncias por delitos informáticos, subtipo Contra datos y sistemas informáticos, según modalidad, 2019-2025JUL



Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

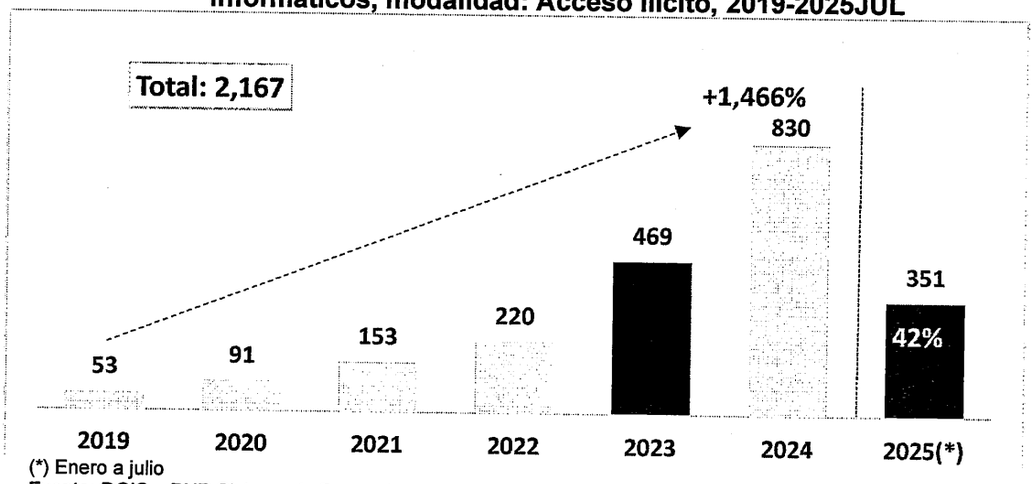
MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B°

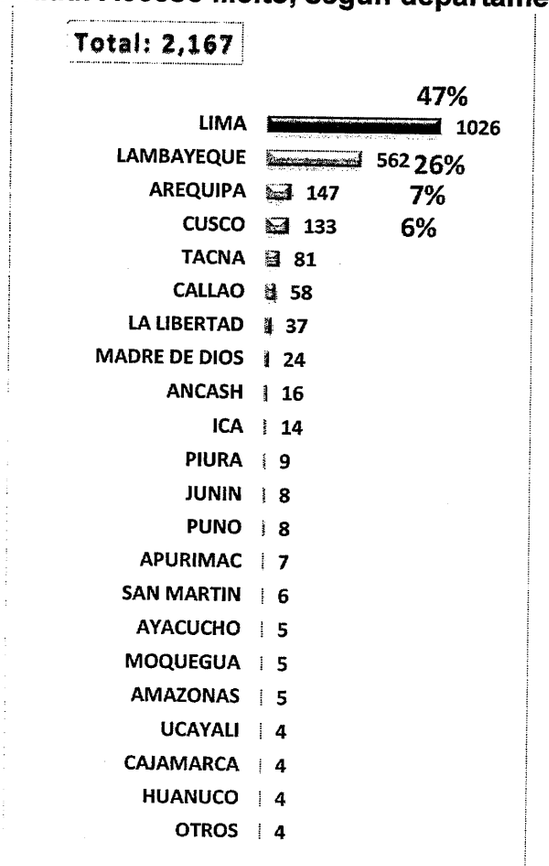
S. DE LA CRUZ Q.

Denuncias por delitos informáticos, subtipo Contra datos y sistemas informáticos, modalidad: Acceso ilícito, 2019-2025JUL



(*) Enero a julio
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

Denuncias por delitos informáticos, subtipo Contra datos y sistemas informáticos, modalidad: Acceso ilícito, según departamento, 2019-2025JUL



Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno

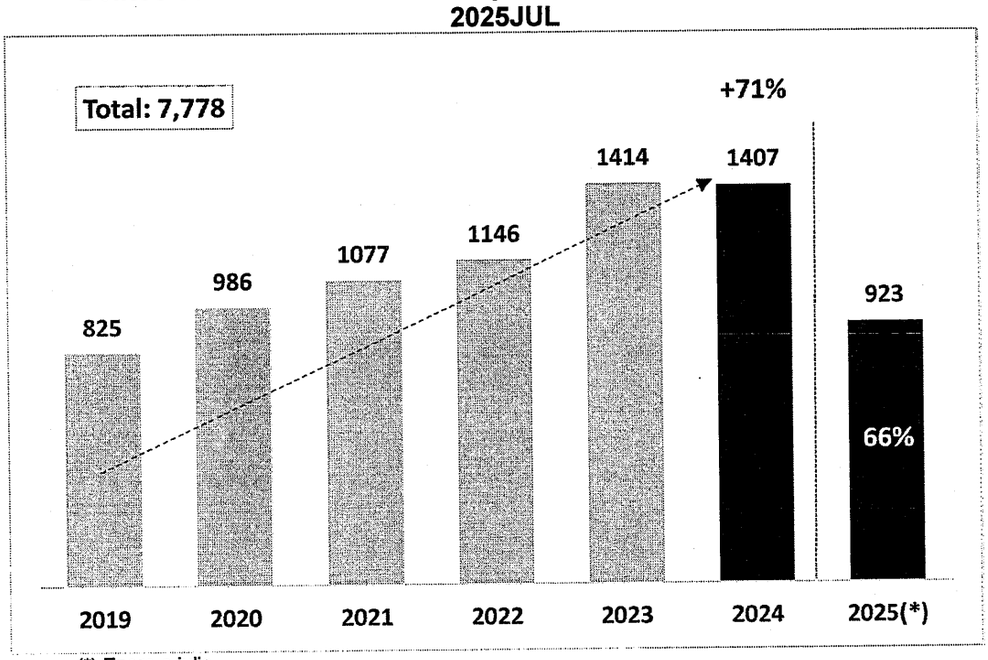
MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

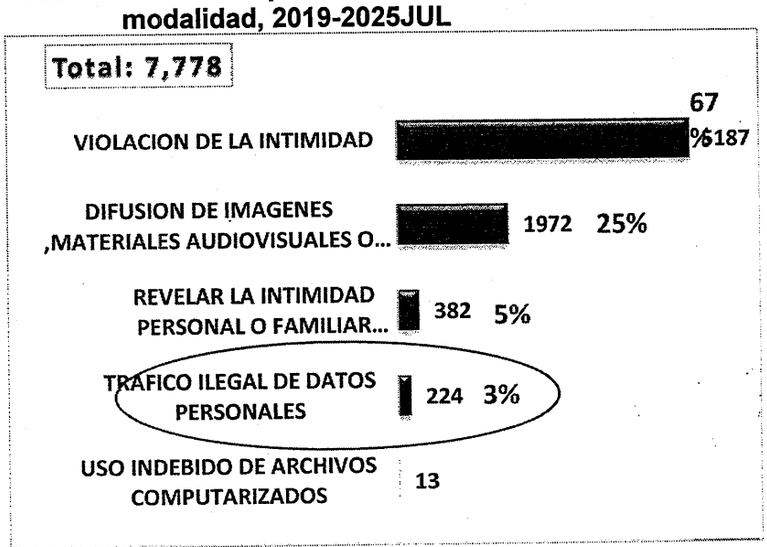
DELITOS CONTRA LA LIBERTAD, SUBTIPO: VIOLACIÓN DE LA INTIMIDAD, MODALIDAD TRÁFICO ILEGAL DE DATOS PERSONALES

Delitos contra la libertad – Subtipo Violación de la intimidad, 2019-2025JUL



(*) Enero a julio
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

Delitos contra la libertad – Subtipo Violación de la intimidad, según modalidad, 2019-2025JUL



Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

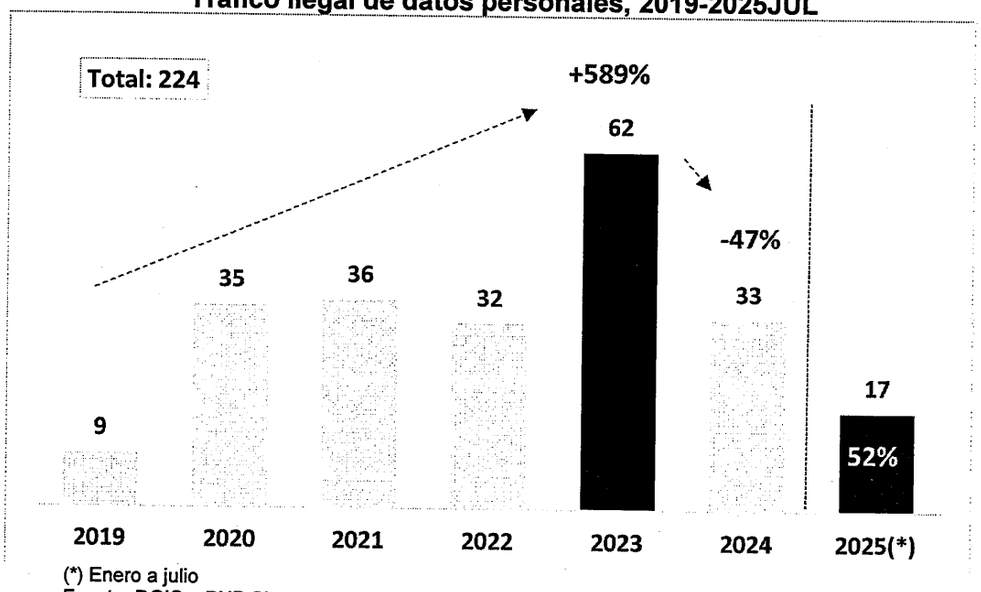
MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B°

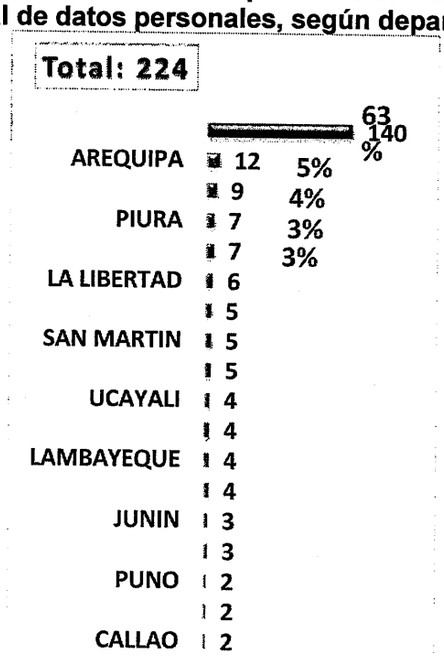
S. DE LA CRUZ Q.

Delitos contra la libertad – Subtipo Violación de la intimidad, Modalidad: Tráfico ilegal de datos personales, 2019-2025JUL



(*) Enero a julio
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

Delitos contra la libertad – Subtipo Violación de la intimidad, Modalidad: Tráfico ilegal de datos personales, según departamento, 2019-2025JUL



(*) Enero a julio
Fuente: DGIS – PNP Sistema de Denuncias Policiales – SIDPOL PNP

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno
MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica
MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO
S. DE LA CRUZ Q

El reporte diferencia entre "Acceso Ilícito" y "Tráfico Ilegal de Datos Personales" (como violación de la intimidad); y muestra que mientras el 'Acceso Ilícito' se dispara, las denuncias por 'Tráfico Ilegal de Datos' bajo el esquema actual (delitos contra la intimidad) no reflejan la realidad del mercado masivo criminal. Esto evidencia que el tipo penal vigente (Artículo 154 Código Penal) no es operativo para la ciberdelincuencia organizada. En ese sentido, la presente norma, pretende trasladar y especificar esta conducta en la Ley de Delitos Informáticos, lo cual dotaría a la Policía Nacional del Perú y Fiscalía de herramientas especializadas para perseguir el verdadero volumen de tráfico que hoy permanece oculto.

En conclusión, los reportes estadísticos del Sistema de Denuncias Policiales (SIDPOL - PNP) corroboran la necesidad urgente de modificar la estrategia punitiva. Entre el año 2019 y septiembre de 2025, se registraron 166,200 denuncias por delitos informáticos; sin embargo, apenas en 19,640 casos se logró identificar al presunto autor a nivel policial, lo que representa una tasa de eficacia de identificación de tan solo el 12%.

Esta cifra revela que el 88% de los ciberdelitos permanecen en el anonimato en la interposición de la denuncia, en gran medida porque la tipificación actual exige probar la autoría del "acceso ilícito" o "interceptación", modalidades que presentan tasas de identificación de autores sumamente bajas (15% en interceptación de datos).

El delito de adquisición, posesión y tráfico ilícito de datos informáticos, incluyendo la conducta de posesión, revertirá esta tendencia al permitir actuar contra los tenedores y comercializadores de la información, quienes constituyen el eslabón tangible de la cadena criminal, cerrando así la brecha de impunidad que actualmente favorece a las organizaciones criminales.

4.3. ANÁLISIS SOBRE LA NECESIDAD, VIABILIDAD Y OPORTUNIDAD

De conformidad con los estándares de técnica legislativa y la exigencia de racionalidad de la ley penal, se procede a sustentar la necesidad, viabilidad y oportunidad del presente decreto legislativo, amparada en evidencia empírica (criminológica), dogmática penal y el bloque de constitucionalidad.

4.3.1. NECESIDAD: El imperativo de cerrar la brecha de impunidad

La necesidad de la reforma no responde a un mero populismo punitivo, sino a una urgencia pragmática ante la ineficacia estructural del tipo penal vigente. Nos encontramos ante lo que la doctrina denomina una "crisis de punibilidad" que vulnera el deber estatal de protección.

Siguiendo al catedrático Jesús-María Silva Sánchez[14], la "crisis de punibilidad" surge cuando el Derecho Penal clásico se muestra inoperante frente a los riesgos de la moderna sociedad de la información. El autor advierte que ante la "delincuencia de masas" o fenómenos macro-criminales (lo que sería el tráfico masivo de datos), el Estado corre el riesgo de caer en una "impotencia funcional", donde la incapacidad de procesar eficazmente miles de conductas

[14] Silva Sánchez, J. M. (2011). La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales (3.ª ed.). B de F.

lesivas genera una sensación de anomia (ausencia de ley) en la ciudadanía. (Silva Sánchez, 2011)

Ciertamente, centrar la persecución exclusivamente en el "Acceso Ilícito" no resulta eficaz, así muestra la evidencia estadística de la Policía Nacional del Perú (SIDPOL) que concluye que: entre 2019 y septiembre de 2025, de 166,200 denuncias por delitos informáticos, solo se logró identificar al autor en 19,640 casos, a nivel policial. Esto revela una tasa de impunidad del 88% en sede preliminar, que demanda la urgencia de cerrar una brecha normativa que actualmente impide al Estado cumplir con su rol garantista.

La inacción legislativa frente a nuevas modalidades delictivas supone una vulneración directa del artículo 44 de la Constitución Política.

> *"Artículo 44. Deberes del Estado*
> *Son deberes primordiales del Estado: defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.*
>
> *Asimismo, es deber del Estado establecer y ejecutar la política de fronteras y promover la integración, particularmente latinoamericana, así como el desarrollo y la cohesión de las zonas fronterizas, en concordancia con la política exterior."*

La Constitución Política del Perú, consagra como deber primordial del Estado proteger a la población de las amenazas contra su seguridad. Esta obligación no es meramente declarativa; posee un contenido prestacional exigible.

Al respecto, el Tribunal Constitucional, en el Expediente Nº 00012-2005-PI/TC (Fundamentos 15-17), ha establecido jurisprudencia vinculante que los derechos fundamentales poseen una "dimensión objetiva". Esta dimensión exige que el Estado no se limite a abstenerse de vulnerar derechos, sino que debe garantizar su plena vigencia mediante un ordenamiento jurídico eficaz y operativo. En consecuencia, cuando el sistema penal tolera bolsones de impunidad sistémica por deficiencias normativas, el Estado incumple su mandato constitucional, dejando a la ciudadanía en un estado de indefensión fáctica frente al crimen organizado.

La brecha de impunidad se explica por una deficiencia estructural en la Ley Nº 30096. La legislación vigente centra la persecución penal casi exclusivamente en el "Acceso Ilícito" (artículo 2), exigiendo probar la autoría de la intrusión técnica (hackeo); una conducta volátil, anónima y frecuentemente transfronteriza.

Existe, por tanto, una "laguna de punibilidad técnica", debido a que el sistema sanciona la sustracción (difícil de probar), pero omite tipificar autónomamente la comercialización posterior.

Asimismo, resulta ineficaz pretender sancionar el tráfico masivo de bases de datos bajo el tipo penal de "Violación de la Intimidad" (Art. 154 del Código Penal). Dicho delito protege la esfera privada individual, pero resulta insuficiente ante la "Seguridad de los Datos" como activo supraindividual en la sociedad de la información.

La evidencia muestra que mientras el "Acceso Ilícito" creció un 1,466%, las denuncias por tráfico de datos bajo el esquema tradicional sancionado por el artículo 154 del Código Penal, son estadísticamente irrelevantes, demostrando su desuso fáctico. Es imperativo concebir esta conducta a la Ley de Delitos Informáticos, no solo por coherencia sistemática, sino por necesidad procesal, debido a que, habilitará a los operadores de justicia el uso de técnicas especiales de investigación (levantamiento del secreto de las comunicaciones, agente encubierto digital), herramientas que la legislación actual restringe para delitos que no están catalogados dentro de la criminalidad informática o la criminalidad organizada.

Finalmente, el presente Decreto Legislativo resulta coherente desde la perspectiva dogmática penal, pues sugiere que, ante nuevas formas de criminalidad organizada, el Derecho Penal debe adelantar la barrera de punición.

Como señala Roxin en su 'Parte General', la complejidad de la vida moderna legitima la creación de tipos penales de peligro abstracto, donde el legislador no espera la lesión efectiva del bien jurídico, sino que sanciona la peligrosidad de la conducta para evitar daños catastróficos futuros[15].

Desde la perspectiva funcionalista de Jakobs[16], el Derecho Penal debe garantizar la estabilidad normativa. En contextos de criminalidad organizada, esto implica adelantar la intervención punitiva a los actos preparatorios y de organización (como la logística de datos), pues esperar a la consumación del fraude final supondría una claudicación del Estado ante la estructura criminal.

Frente a dichas consideraciones, resulta necesario tipificar la comercialización y posesión ilegítima, dado que los intermediarios son "nodos estáticos" y detectables en flagrancia; lo cual adicionalmente, podría materializar el principio de tutela jurisdiccional efectiva (reconocido en el numeral 3 del artículo 139 de la Constitución), pues un sistema que no identifica responsables es un sistema que deniega justicia.

Con la finalidad de cerrar este vacío, se busca tipificar la posesión y comercialización ilegítima de datos, dado que los intermediarios ("data *brokers* ilegales") son objetivos estáticos y detectables en flagrancia. Esta reforma es necesaria para materializar la "Proscripción de la Impunidad", estándar exigido por la Corte Interamericana de Derechos Humanos, permitiendo al Estado golpear los eslabones visibles y rentables de la cadena delictiva.

S. DE LA CRUZ Q.

[15] Roxin, C. (1997). Derecho Penal. Parte General. Tomo I: Fundamentos. La estructura de la teoría del delito. Civitas

[16] Jakobs, G. (1997). Derecho Penal. Parte General. Fundamentos y teoría de la imputación. Marcial Pons.

4.3.2. VIABILIDAD: Desde una perspectiva constitucional y convencional

La presente norma supera el test de constitucionalidad y se alinea con los compromisos internacionales del Estado Peruano.

4.3.2.1. Perspectiva constitucional

Se respeta escrupulosamente el Principio de Legalidad consagrado en el literal d), inciso 24 del artículo 2 de la Constitución Política, en su vertiente material de mandato de determinación (*Lex Certa*).

A diferencia de tipos penales abiertos que vulneran la seguridad jurídica, la presente fórmula legislativa opta por la descripción taxativa de las conductas prohibidas a través de verbos rectores inequívocos: "vender", "comprar" y "poseer ilegítimamente". Esta técnica legislativa cumple con el estándar exigido por el Tribunal Constitucional en la STC Nº 0010-2002-AI/TC (Caso Tineo Silva), fundamento jurídico 34, donde el Supremo Intérprete establece:

> "El principio de legalidad exige que la ley penal sea previa, escrita, estricta y cierta (...) El mandato de certeza o determinación (*lex certa*[17]) obliga al legislador a formular la conducta prohibida de modo tal que el ciudadano pueda conocer con suficiente precisión qué es lo que se le prohíbe, reduciendo al máximo la discrecionalidad del juzgador."

En ese sentido, al tipificar la conducta mediante acciones descriptivas concretas (actos de comercio y tenencia), se cierra el paso a la arbitrariedad judicial y se garantiza que el ciudadano conozca exactamente la frontera entre lo lícito y lo ilícito. Asimismo, la inclusión del elemento normativo "ilegítimamente" actúa como una válvula de garantía, asegurando que no se sancione la posesión autorizada (ej. administradores de bases de datos lícitas), sino únicamente aquella que carece de título jurídico válido, superando así el test de constitucionalidad.

4.3.2.2. Perspectiva Convencional (Convenio de Budapest)

El presente decreto legislativo no constituye un acto discrecional aislado, sino un ejercicio de adecuación normativa en cumplimiento de las obligaciones internacionales asumidas por el Estado Peruano. De conformidad con el artículo 55 y la Cuarta Disposición Final y Transitoria de la Constitución Política, los tratados de derechos humanos y lucha contra la criminalidad forman parte del derecho nacional, integrando el denominado "Bloque de Constitucionalidad".

En este marco, se materializa el cumplimiento del Convenio de Budapest sobre Ciberdelincuencia, instrumento que establece estándares mínimos de

S. DE LA CRUZ Q.

[17] Significa "ley cierta" o "ley precisa" en latín y es un principio fundamental del derecho penal que exige que las leyes que definen delitos y penas sean claras, exactas y no ambiguas, para que los ciudadanos sepan qué conductas están prohibidas y para evitar la arbitrariedad judicial. Impone al legislador la obligación de describir de forma detallada los supuestos de hecho (el "tipo penal") que configuran un delito, asegurando que no haya vaguedades.

punibilidad que el legislador nacional está obligado a observar bajo el principio de *Pacta Sunt Servanda*[18].

A. El mandato del Artículo 6 del Convenio (Criminalización de actos preparatorios)

El literal a) del numeral 1 del artículo 6 del Convenio de Budapest impone a los Estados Parte el deber jurídico de tipificar no solo la intrusión informática, sino los actos que facilitan su comisión. Textualmente, la norma supranacional exige sancionar la producción, venta, obtención para el uso, importación o distribución de: a) Dispositivos o programas informáticos diseñados para cometer ciberdelitos, b) Contraseñas, códigos de acceso o datos informáticos similares que permitan acceder a un sistema.

El presente Decreto Legislativo, al criminalizar la comercialización y posesión ilegítima de datos, responde directamente a este mandato. Como señala el Informe Explicativo del Convenio de Budapest (Council of Europe), la *ratio legis* de este artículo es combatir el "mercado negro" de herramientas delictivas, reconociendo que la peligrosidad no reside solo en el ataque final, sino en la disponibilidad y tráfico de los medios para realizarlo. Omitir esta tipificación supone una infracción por defecto del tratado internacional.

B. El ejercicio del control de convencionalidad ex officio

Desde la perspectiva jurisprudencial, la aprobación de esta norma constituye un acto de control de convencionalidad ex officio en sede legislativa. La Corte Interamericana de Derechos Humanos (Corte IDH), en el caso Almonacid Arellano y otros Vs. Chile (2006), ha establecido que no solo los jueces, sino todos los órganos del Estado tienen la obligación de verificar que las leyes internas no contravengan el objeto y fin de la Convención Americana y los tratados conexos. (fundamento 123)[19]

Por tanto, mantener un vacío legal respecto a la comercialización de bases de datos robadas resulta ineficiente.

4.3.2.3. Estándares del Sistema Interamericano de Derechos Humanos

Asimismo, la presente norma resulta plenamente compatible con las obligaciones internacionales del Estado peruano en materia de derechos humanos. La tipificación del tráfico ilícito de datos materializa la tutela tanto de

S. DE LA CRUZ Q.

[18] Es una locución latina que significa "los pactos deben cumplirse", un principio fundamental del derecho que establece que los acuerdos y contratos, una vez establecidos libremente, son obligatorios para las partes y deben cumplirse fielmente, como si fueran ley entre ellos, aplicándose tanto en el derecho civil (contratos) como en el derecho internacional (tratados).

[19] El cumplimiento por parte de agentes o funcionarios del Estado de una ley violatoria de la Convención produce responsabilidad internacional del Estado, y es un principio básico del derecho de la responsabilidad internacional del Estado, recogido en el Derecho Internacional de los Derechos Humanos, en el sentido de que todo Estado es internacionalmente responsable por actos u omisiones de cualesquiera de sus poderes u órganos en violación de los derechos internacionalmente consagrados, según el artículo 1.1 de la Convención Americana149.

la vida privada (Artículo 11) como de la protección judicial (Artículo 25) consagradas en la Convención Americana sobre Derechos Humanos.

Al respecto, la Corte Interamericana de Derechos Humanos, en el reciente fallo del Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia (2023), ha establecido que el derecho a la autodeterminación informativa prohíbe injerencias arbitrarias o abusivas, exigiendo a los Estados que la ley establezca mecanismos efectivos frente a dichas vulneraciones. En esa línea, la sanción penal de la comercialización ilegal de datos refuerza el deber estatal de garantía (Artículos 1 y 2 de la Convención Americana) frente a afectaciones provenientes de terceros que utilizan dicha información como insumo para delitos de extorsión, fraude o trata de personas.

4.3.2.4. Estándares de la Convención de las Naciones Unidas contra la Ciberdelincuencia

La iniciativa se enmarca y alinea estratégicamente con los objetivos de la Convención de las Naciones Unidas contra la Ciberdelincuencia, instrumento internacional suscrito por el Estado peruano en el año 2025. Esta Convención constituye el nuevo estándar global que establece obligaciones generales para que los Estados Parte adopten marcos normativos robustos, dinámicos y eficaces frente a las amenazas emergentes en el ciberespacio.

La Convención promueve no solo la sanción del acceso ilícito (hacking), sino que insta a los Estados a abordar de manera integral las conductas que facilitan, sostienen o financian los mercados ilícitos asociados a dichos delitos. Al criminalizar la comercialización y el tráfico de datos, el Perú da cumplimiento a este mandato, atacando el componente económico que incentiva la ciberdelincuencia transnacional.

Si bien los instrumentos internacionales establecen estándares mínimos de criminalización, estos no restringen la facultad soberana de los Estados para adoptar medidas más específicas a sus realidades y necesidades nacionales. Por tanto, la presente norma constituye el ejercicio legítimo de dicha potestad soberana para proteger la integridad de los sistemas y la autodeterminación informativa de los ciudadanos peruanos frente a su explotación económica ilegal en mercados negros locales y globales.

S. DE LA CRUZ Q.

4.3.3. OPORTUNIDAD: El contexto de emergencia digital y la seguridad ciudadana

La oportunidad de la presente reforma legislativa no responde a una coyuntura mediática, sino a la imperiosa necesidad de actualizar la política criminal del Estado conforme a la doctrina del "Derecho penal en la sociedad del riesgo"[20].

[20] Como advierte la doctrina de la Sociedad del Riesgo (Ulrich Beck), ante amenazas que tienen el potencial de desestabilizar la confianza en sistemas completos (como el sistema bancario o la identidad nacional), el Derecho Penal no puede esperar a la consumación del daño individual, sino que debe gestionar y sancionar la creación del riesgo mismo (tráfico de datos).

En la era digital, el riesgo ya no es local ni estático, sino resulta global, instantáneo y masivo, por lo que, postergar su regulación implica una claudicación del Estado ante amenazas que evolucionan a una velocidad superior a la capacidad de respuesta de la ley actual.

En ese sentido, la intervención penal propuesta se inserta dentro del ecosistema normativo de seguridad y confianza digital del Estado, complementando las políticas de prevención, gobernanza y protección de datos con una respuesta penal dirigida específicamente contra las conductas que sostienen el mercado ilícito de datos informáticos.

4.3.3.1. Explosión delictiva y el principio de intervención inmediata

La estadística criminal oficial revela un escenario de hiper-crecimiento delictivo que exige una intervención legislativa de *ultima ratio* pero de aplicación inmediata. Según la data consolidada, las denuncias por ciberdelitos han escalado de 7,968 casos en 2019 a una proyección que supera los 44,000 casos para el cierre de 2024. Este incremento del 461% no es lineal, es exponencial.

Por lo que, legislar en este contexto se ha traducido en un imperativo de orden público, debido a que la curva de crecimiento demuestra que los mecanismos de control social informal (seguridad privada de las empresas) han sido rebasados.

4.3.3.2. La convergencia criminal debido a que concurren los delitos informáticos como fuente de violencia físico

Resulta oportuno y crítico legislar bajo una visión sistémica actual del delito. La criminología moderna advierte sobre el fenómeno de la "Convergencia Criminal", donde el ciberdelito deja de ser una infracción meramente patrimonial o "de guante blanco" para convertirse en el motor de delitos de sangre.

Conforme al estudio oficial "Cobro y Silencio: La dinámica de la extorsión en el Perú" (Ministerio del Interior, 2025), la extorsión no opera como un fenómeno aislado, sino que se sostiene sobre una estructura de mercados ilícitos interconectados. El informe identifica taxativamente al "Mercado de Información" como el primer eslabón de esta cadena delictiva, en este mercado, el tráfico ilegal de bases de datos cumple una función logística crítica para seleccionar y perfilar a la víctima. La información sustraída (direcciones, teléfonos, composición familiar, movimientos bancarios) constituye la "materia prima" que permite a las bandas criminales planificar sus ataques con precisión, reduciendo sus costos de búsqueda y aumentando la eficacia de la intimidación[21].

Al cortar el flujo de datos ilícitos mediante la penalización de su comercialización, el Estado no solo protege el bien jurídico "patrimonio" o "intimidad", sino que despliega una medida de prevención directa contra la violencia callejera para cortar el suministro de información criminal.

[21] Ministerio del Interior del Perú. (2025). Cobro y Silencio: La dinámica de la extorsión en el Perú (1.ª ed.). Dirección General Contra el Crimen Organizado. pp. 38, 43, 46-47.

4.3.4. ANÁLISIS DE CONSTITUCIONALIDAD: TEST DE PROPORCIONALIDAD

Dado que la presente norma implica una intervención en la libertad individual (mediante la creación de un tipo penal y pena privativa de libertad), corresponde acreditar su legitimidad constitucional a través del Test de Proporcionalidad, demostrando que la medida supera los subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto.

4.3.4.1. Examen de idoneidad (adecuación teleológica)

El subprincipio de idoneidad exige que la medida legislativa sea apta para alcanzar un fin constitucionalmente válido. La norma busca proteger el derecho fundamental a la Autodeterminación Informativa (inciso 6 del artículo 2 de la Constitución Política) y la Seguridad Ciudadana (artículo. 44 de la Constitución Política), gravemente amenazados por la libre circulación de datos personales en mercados negros.

En ese sentido, la criminalización de la venta y posesión ilegítima de bases de datos es una medida idónea porque ataca directamente el incentivo económico del delito y rompe la cadena de pagos. Al elevar el costo del delito (riesgo de cárcel) y permitir la incautación de los activos digitales, se logra desincentivar la comercialización, lo cual es el medio causal adecuado para reducir la exposición de la información privada de los ciudadanos.

4.3.4.2. Examen de necesidad frente al control administrativo

Este subprincipio, también llamado de "intervención mínima", exige verificar si existen medios alternativos menos gravosos (como el Derecho Administrativo) que logren el mismo grado de eficacia. El análisis demuestra que el control administrativo es estructuralmente insuficiente para este fenómeno específico.

La potestad sancionadora de la Autoridad Nacional de Protección de Datos Personales (ANPD) está diseñada para fiscalizar a los "Titulares de Bancos de Datos" formales (empresas, bancos, entidades públicas). La ANPD puede multar a una empresa por negligencia en una filtración, pero carece de competencia y capacidad coercitiva para perseguir, investigar y sancionar al ciberdelincuente anónimo o al intermediario ("data broker" ilegal) que vende esa información en Telegram o la Dark Web.

Asimismo, se evidencia insuficiencia de herramientas de investigación en el ámbito del procedimiento administrativo, mientras que el Derecho Penal habilita el uso de técnicas especiales de investigación (agente encubierto digital, levantamiento del secreto de las comunicaciones, allanamientos y decomiso de servidores) necesarias para desarticular redes de tráfico de datos. En ese sentido, combatir redes criminales complejas con procedimientos administrativos devienen en ineficaces.

Por otro lado, las multas al mercado negro no son mecanismos disuasivos eficientes, en tanto que para un delincuente que lucra millones con la venta de datos, una multa administrativa (que además es difícil de ejecutar contra sujetos anónimos o insolventes) no genera disuasión. Por lo que, la pena privativa de

libertad posee la fuerza intimidatoria suficiente (prevención general negativa) para contener la demanda y oferta en mercados ilegales.

En ese sentido, no existe una medida menos gravosa que el Derecho Penal que consiga el mismo objetivo de protección con igual eficacia, concluyendo la necesidad de la medida.

4.3.4.3. Examen de proporcionalidad en sentido estricto (ponderación)

Corresponde ponderar si la restricción de la libertad personal del infractor guarda equilibrio con la satisfacción de los derechos protegidos.

Si bien se restringe la libertad de tránsito (pena privativa de libertad) de quienes comercian ilegalmente con datos, la medida genera un grado de satisfacción muy alto para la sociedad, pues protege no solo la privacidad de millones de peruanos, sino su patrimonio (frente a fraudes) y su integridad física (frente a extorsiones facilitadas por data filtrada).

Por lo que, la seguridad jurídica, la paz social y la protección de datos de los ciudadanos tienen un peso constitucional superior al interés de un individuo de lucrar ilícitamente con información ajena, en otras palabras, el sacrificio de la libertad del delincuente es proporcional a los inmensos daños sociales que su conducta genera (extorsiones masivas, vaciamiento de cuentas, suplantación de identidad). En consecuencia, se supera el test de proporcionalidad, legitimando el uso del *Ius Puniendi*[22] estatal.

4.4. PRECISIÓN DEL NUEVO ESTADO QUE GENERA EL PRESENTE DECRETO LEGISLATIVO

La presente norma responde a la imperiosa necesidad de actualizar la política criminal del Estado frente a la evolución de la ciberdelincuencia. La incorporación de un tipo penal autónomo que sancione expresamente la compra, venta, comercialización y tráfico ilícito de datos informáticos no constituye una mera adición punitiva, sino un cambio estructural en la estrategia de persecución penal.

Se pretende que el ordenamiento jurídico penal peruano transite hacia un nuevo estado de protección, caracterizado por los siguientes efectos directos:

4.4.1. Desarticulación de la cadena económica del delito informático. La evidencia criminológica demuestra que la sustracción de datos (hacking) no es un fin en sí mismo, sino un medio para obtener un activo. Hasta la fecha, la legislación se ha centrado en el intruso informático, dejando en una zona de impunidad a los mercados negros (físicos y digitales) que monetizan dicha información. La creación de este tipo penal ataca directamente la rentabilidad del delito, debido a que se tipifica la comercialización como delito autónomo, se elevan los costos transaccionales y los riesgos para los intermediarios y vendedores, rompiendo el ciclo de oferta y demanda. El nuevo estado generado por la norma elimina el incentivo económico que motiva la intrusión inicial, bajo la premisa de que, sin

[22] Potestad del Estado para castigar mediante los dos sistemas represivos existentes en nuestro derecho: el derecho penal, que es aplicado por los jueces y tribunales, y el derecho administrativo sancionador, que es aplicado por la Administración.

mercado de receptación de datos, disminuye drásticamente el incentivo para su sustracción.

4.4.2. Persecución penal efectiva de los beneficiarios finales y el "mercado gris". El vacío legal existente permitía que actores inescrupulosos —desde organizaciones criminales dedicadas a la estafa hasta empresas que realizan competencia desleal— adquirieran bases de datos ilícitas alegando desconocimiento de su origen técnico (falta de dolo en el acceso ilícito). El presente Decreto Legislativo permite perseguir penalmente no solo a quien accede ilícitamente a la data, sino fundamentalmente a quien financia la actividad delictiva mediante la compra o se beneficia de su uso indebido.

Se instaura así un deber de legalidad en la adquisición de activos digitales para quien adquiera, posea o trafique con datos personales o corporativos sin acreditar su legítima procedencia.

4.4.3. Fortalecimiento de la tutela penal de los datos personales y la seguridad digital. Se eleva el estándar de protección del bien jurídico "autodeterminación informativa" y "reservada de las comunicaciones", respuesta estatal que resulta coherente a la naturaleza de las bases de datos, que constituyen un activo crítico, cuya vulneración afecta la seguridad ciudadana y la estabilidad económica. El nuevo tipo penal autónomo envía un mensaje claro de prevención general positiva, frente a la seguridad digital como un bien jurídico colectivo, debido a que se sanciona el tráfico de datos, se tutela la confianza de la ciudadanía en el ecosistema digital y se obliga a los actores del mercado a reforzar sus protocolos de *compliance*[23] y diligencia debida[24], evitando nutrir sus operaciones con información obtenida al margen de la ley.

En consecuencia, la medida genera un ordenamiento jurídico hermético frente al cibercrimen, superando el modelo reactivo (centrado únicamente en el acceso indebido) para adoptar un modelo integral que sanciona todas las etapas del *iter criminis*[25] económico, desde la obtención ilegal, pasando por la intermediación, hasta la comercialización final. Esto dota al Ministerio Público y a la Policía Nacional del Perú de herramientas legales precisas para incautar, detener y sancionar las operaciones de tráfico de datos que hoy operan en impunidad.

---

[23] (cumplimiento normativo) es el sistema de políticas y procesos de una empresa para asegurar el apego a leyes y ética.

[24] (Due Diligence) es una investigación profunda que se realiza *dentro* de ese marco de compliance para evaluar riesgos (legales, financieros, éticos) de terceros (clientes, socios, proveedores) *antes* de establecer una relación, como fusiones, contrataciones o inversiones, para prevenir delitos y daños a la reputación. En resumen, el compliance es el sistema general y la diligencia debida es una herramienta clave para verificar su efectividad y la integridad de las partes interesadas.

[25] Conjunto de etapas que atraviesa la ejecución de un delito y que comprende tanto los actos que tienen lugar en la fase interna como los que se llevan a cabo en la fase externa. *acto preparatorio del* iter criminis, *fase externa del delito*, *fase interna del delito*, *formas de aparición del delito*. Consulta realizada en Diccionario panhispánico del español jurídico en su versión digital revisada el 09.01.2026 en: https://dpej.rae.es/lema/iter-criminis

4.5. OBJETIVOS DEL PRESENTE DECRETO LEGISLATIVO

La presente norma se fundamenta en los principios de necesidad, idoneidad y proporcionalidad, buscando cerrar una brecha de punibilidad identificada en la fenomenología del cibercrimen en el Perú. Los objetivos se desarrollan a continuación:

4.5.1. OBJETIVO GENERAL: Criminalizar de manera expresa y autónoma la compra, comercialización y tráfico ilícito de datos informáticos.

El objetivo central es satisfacer el Principio de Taxatividad (*Lex Certa*) y superar la insuficiencia normativa actual. La realidad criminológica evidencia que la venta de bases de datos —ya sea en soportes físicos (galerías informáticas) o mediante canales digitales (grupos de Telegram, foros de la Deep Web)— configura materialmente una conducta lesiva que hoy carece de una respuesta penal directa.

Actualmente, estos actos se asemejan a una receptación "agravada impropia", pero al no encajar perfectamente en los supuestos del delito patrimonial clásico que exige probar un delito fuente (hackeo) a menudo imposible de rastrear, sumada a la discusión doctrinaria sobre la intangibilidad de los datos, convierte al Artículo 194 del Código Penal en una herramienta obsoleta para este fin, generando espacios de impunidad.

Por tanto, el objetivo es dotar al sistema de justicia de un tipo penal que sancione el tráfico de datos por su propia naturaleza delictiva, sin depender de la prueba del hacking inicial.

4.5.2. OBJETIVOS ESPECÍFICOS

a) Desincentivar el mercado ilegal de datos personales y corporativos

Se busca aplicar la lógica del Análisis Económico del Derecho Penal: anular la rentabilidad del delito elevando el costo de la sanción para el comprador y el intermediario.

Desde una perspectiva doctrinaria, el presente Decreto Legislativo se alinea con lo sostenido por Ulrich Sieber[26], quien argumenta que en la moderna "sociedad de la información", la integridad y confidencialidad de los datos trascienden el interés individual; se constituyen como requisitos previos indispensables para la funcionalidad de la economía global. Al proteger penalmente el dato frente a su tráfico, el Estado peruano protege la operatividad misma del mercado digital, impidiendo que se convierta en un entorno hostil para la inversión y el comercio.

b) Reducir la incidencia de delitos derivados (Interrupción del *Iter Criminis*)

S. DE LA CRUZ Q.

[26] Sieber, U. (2010). Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law. En: A. Santos & J. L. de la Cuesta (Eds.), Criminal Law in the 21st Century (pp. 127-138). Maklu.

El tráfico de datos actúa como un "delito instrumental" o facilitador. Al restringir el acceso a bases de datos ilegales, se impacta directamente en la logística de las organizaciones criminales dedicadas a la extorsión, el fraude bancario y la suplantación de identidad, privándolas de la "materia prima" necesaria para seleccionar y atacar a sus víctimas.

c) Fortalecer la seguridad y confianza digital nacional, incluida la ciberseguridad, y materializar la tutela constitucional de la Autodeterminación Informativa

La norma tiene por objeto elevar el estándar de protección de los derechos fundamentales en el entorno digital, pasando de una tutela administrativa a una tutela penal reforzada.

Este objetivo materializa lo establecido por el Tribunal Constitucional en la sentencia recaída en el Expediente N° 04467-2006-PHD/TC. En dicho fallo, el supremo intérprete de la Constitución estableció que el derecho a la autodeterminación informativa no se limita a la facultad de acceder a la propia información, sino que implica fundamentalmente la capacidad de "controlar su flujo" y evitar que los datos sean objeto de "manipulación o transferencia indebida".

Al criminalizar el tráfico de datos, se dota de herramienta para materializar la garantía constitucional del derecho a la autodeterminación informativa, sancionando severamente a quien vulnere ese control de flujo mediante la compraventa no autorizada de información personal.

4.6. ANÁLISIS DE LAS OPINIONES

La necesidad de la presente reforma legislativa no solo respondió a estadísticas delictivas, sino al reconocimiento expreso de las debilidades estructurales del sistema de control administrativo, evidenciadas en las recientes Mesas de Trabajo Multisectoriales lideradas por el Ministerio del Interior, entre ellas, las desarrolladas en los meses de setiembre y octubre del 2025, las cuales permitieron identificar nudos críticos que facilitan la impunidad del tráfico de datos y la extorsión.

La urgencia de la reforma, que se presenta en la fecha, ha sido admitida por los propios organismos técnicos del Ejecutivo. En el Acta del 4 de septiembre de 2025, el Registro Nacional de Identificación y Estado Civil (RENIEC) confirmó que ya integra una mesa técnica con la Dirección General Contra el Crimen Organizado (DGCO) del Ministerio del Interior. Asimismo, se estableció como compromiso institucional la incorporación del Ministerio de Transportes y Comunicaciones (MTC) a dicho espacio para diseñar un "marco normativo idóneo para regular el uso de las redes sociales para la *dark web* y el comercio de datos". Esto demuestra un consenso interinstitucional sobre la necesidad imperiosa de un nuevo marco legal.

Posteriormente, en la Mesa de Trabajo del 29 de octubre de 2025, se expresó que el tráfico de datos personales *(doxeo)* se ha convertido en el insumo principal para vulnerar los sistemas de seguridad, en tanto, las organizaciones criminales aprovechan la información de la ficha RENIEC (específicamente la huella del dedo índice) para activar líneas de manera fraudulenta. La autoridad policial señaló la urgencia de migrar hacia una verificación

biométrica facial o el uso aleatorio de huellas dactilares, dado que la estática actual permite la suplantación de identidad masiva.

Finalmente, en la Mesa de Trabajo del 13 de enero de 2026, organizada por la Dirección General contra el Crimen Organizado (DGCO) del Ministerio del Interior, con participación del Registro Nacional de Identificación y Estado Civil (RENIEC) y representantes de la Policía Nacional del Perú, se dejó constancia del consenso interinstitucional en torno a la necesidad de incorporar un tipo penal autónomo que sancione la posesión, adquisición y comercialización ilícita de datos informáticos; y de manera complementaria, se advirtió la conveniencia de evaluar, en una etapa posterior, la modificación de la Ley de Responsabilidad Administrativa de las Personas Jurídicas, a fin de fortalecer los mecanismos de prevención y control corporativo, sin que ello forme parte del objeto inmediato del presente decreto legislativo.

Lo expuesto en las actas oficiales confirma que las entidades del Estado advierten la necesidad de reforma penal, y manifiestan un consenso de la fórmula legal, en tanto, las dinámicas criminales son distintas que han superado los controles administrativos.

4.7. DESCRIPCIÓN Y TIPICIDAD

La presente Decreto Legislativo tiene por objeto la modificar la Ley Nº 30096, Ley de Delitos Informáticos, incorporando un tipo penal autónomo, en estricto ejercicio de la habilitación legislativa conferida al Poder Ejecutivo conforme al artículo 104 de la Constitución Política del Perú.

Desde una perspectiva político-criminal, en la presente norma yace la finalidad teleológica de subsanar un "vacío de punibilidad" detectado en la estructura normativa vigente, debido a que, actualmente, el mercado ilícito del cibercrimen goza de impunidad en sus eslabones intermedios (comercialización). La norma busca sancionar la "monetización" del ilícito informático, abarcando no solo la intrusión (*hacking*), sino la adquisición, posesión, comercialización y tráfico de los activos digitales obtenidos.

Esta medida responde al principio de Fragmentariedad del Derecho Penal o *ultima ratio*, en tanto los mecanismos administrativos contemplados en la Ley de Protección de Datos Personales, resultan insuficientes para disuadir la existencia de mercados negros organizados, conforme se ha tenido oportunidad de desarrollar en el acápite correspondiente al "Examen de necesidad".

En el contexto del tráfico ilícito de datos, el análisis de necesidad revela lo siguiente:

1. Inocuidad de la exigencia de agotamiento de la vía administrativa frente a la criminalidad organizada. El marco normativo actual, presidido por la Ley Nº 29733 (Ley de Protección de Datos Personales), opera bajo una lógica de regulación de mercados formales, es decir, sus mecanismos coercitivos (multas) son efectivos para corregir conductas negligentes de empresas formales, pero resultan inocuos frente a actores criminales que operan en la clandestinidad (mercados negros y *Deep Web*). Pretender combatir redes de tráfico de información con sanciones administrativas constituye un error de política criminal, pues estas organizaciones asumen las multas —en el improbable caso de ser detectadas sin herramientas penales— como un simple costo operativo.

S. DE LA CRUZ Q.

Al respecto, la doctrina penal autorizada es contundente al señalar que la subsidiariedad no equivale a pasividad estatal. Como establece Claus Roxin[27], la naturaleza de ultima ratio del Derecho Penal "no implica inacción, sino intervención selectiva allí donde los otros medios de control social resultan inútiles para garantizar la paz social". Siguiendo al autor alemán, en el caso del tráfico masivo de datos, la afectación a la seguridad ciudadana y la confianza digital desborda la capacidad regulatoria administrativa, haciendo indispensable el recurso a la pena para restablecer la vigencia de la norma.

2. Mandato constitucional de materializar la tutela penal efectiva. La intervención penal se justifica, además, cuando la conducta traspasa el umbral de la mera infracción regulatoria y ataca las bases de la convivencia pacífica, poniendo en riesgo derechos fundamentales.

En concordancia con lo anterior, el Tribunal Constitucional del Perú ha establecido que el legislador no solo tiene la facultad, sino el deber de penalizar conductas gravemente lesivas. En la sentencia recaída en el Expediente Nº 00012-2006-AI/TC (Caso de la Legislación Antiterrorista), el Tribunal reconoció que "el Estado tiene el deber de utilizar el Derecho Penal cuando los bienes jurídicos constitucionales [...] sufren agresiones graves que no pueden ser repelidas por otros medios".

Aplicando este criterio jurisprudencial al presente, la vulneración sistemática de la privacidad y la seguridad personal (mediante el perfilamiento de víctimas para extorsión o fraude) constituye una "agresión grave" a bienes constitucionales (Artículo 2 de la Constitución) que no puede ser repelida eficazmente por la Autoridad Nacional de Protección de Datos Personales, requiriendo la fuerza preventiva y sancionadora del Derecho Penal.

Finalmente, conforme se ha evidenciado en el diagnóstico situacional (Acápite Identificación del problema), la persistencia y crecimiento de mercados ilícitos de datos —a pesar de la vigencia de la Ley Nº 29733 desde hace más de una década— constituye la prueba empírica de la derrota de la vía administrativa para este fenómeno específico, principalmente por la agresividad y sofisticación del mercado negro actual.

En consecuencia, la criminalización expresa de la compra y venta de datos no vulnera el principio de subsidiariedad, y no busca administrativizar el Derecho Penal, sino ofrecer una respuesta contundente ante el fracaso estructural de los controles extrapenales para contener la comercialización de datos ilícitos; sancionando el "plus de antijuridicidad" que representa el dolo de traficar con la identidad ajena y diferenciándolo cualitativamente de la mera infracción administrativa por negligencia en la custodia de la información.

Superado este análisis es preciso ingresar a la descripción del tipo penal que se pretende incorporar en la Ley N° 30096, Ley de delitos informáticos.

4.7.1. BIEN JURÍDICO PROTEGIDO

La determinación del bien jurídico protegido constituye un elemento esencial para evaluar la legitimidad constitucional del tipo penal, así como su correcta ubicación dentro del sistema normativo. El Tribunal Constitucional ha señalado que la intervención penal solo es válida cuando se orienta a la protección de bienes jurídicos de relevancia constitucional y social (STC Exp. Nº 0008-2012-PI/TC).

---

[27] Roxin, C. (1997). Derecho Penal. Parte General. Tomo I. Civitas.

En el caso del delito de adquisición, posesión y tráfico ilícito de datos informáticos, el bien jurídico protegido no se agota en la intimidad personal, ni se reduce a la protección de datos personales en sentido administrativo, sino que presenta un carácter complejo y pluriofensivo.

4.7.1.1. Bien jurídico principal: la seguridad de la información y de los sistemas informáticos

El bien jurídico principal protegido es la seguridad de la información y de los sistemas informáticos, entendida como la confianza social y jurídica en que:

- Los datos almacenados o transmitidos en sistemas informáticos no serán objeto de apropiación, circulación o aprovechamiento ilícito.
- Los mecanismos de seguridad y control de acceso cumplen efectivamente su función de protección.
- El uso de tecnologías de la información se desarrolla en un entorno de confiabilidad.

La Ley Nº 30096, Ley de Delitos Informáticos ha sido diseñada precisamente para proteger este bien jurídico, sancionando conductas que afectan la confidencialidad, integridad y disponibilidad de la información. El tipo penal se inserta en esta lógica, al sancionar no el acceso inicial, sino la explotación posterior del resultado ilícito, que perpetúa y amplifica el daño.

4.7.1.2. Bienes jurídicos concurrentes

Sin perjuicio de lo anterior, el tipo penal protege de manera concurrente los siguientes bienes jurídicos:

a) **Autodeterminación informativa,** reconocida por el inciso 6 del artículo 2 de la Constitución, se ve afectada cuando los datos personales o información digital son utilizados o comercializados sin consentimiento del titular.
b) **Patrimonio y seguridad económica,** el tráfico de datos constituye el principal insumo para delitos patrimoniales como fraude informático, extorsión, suplantación de identidad y vaciamiento de cuentas.
c) **Seguridad ciudadana y orden público,** la comercialización masiva de datos alimenta mercados criminales organizados, afectando la capacidad del Estado para prevenir y reprimir el delito.

Este carácter pluriofensivo refuerza la legitimidad de la intervención penal, conforme al principio de proporcionalidad.

4.7.2. ANÁLISIS DE TIPICIDAD DE DELITO

La proscripción de la responsabilidad objetiva en el Derecho penal trae como consecuencia lógica que la tipicidad deba incluir también una faceta subjetiva. En

S. DE LA CRUZ Q.

consecuencia, esta categoría del delito debe estar necesariamente compuesta por una tipicidad objetiva y una tipicidad subjetiva[28].

La tipicidad objetiva se encarga de determinar fundamentalmente la incidencia social de la conducta en términos de infracción de un rol jurídicamente atribuido, mientras que la tipicidad subjetiva está referida a la vinculación subjetiva del autor con la infracción del rol bajo la forma de dolo o culpa. Esta diferenciación conceptual no debe llevar, sin embargo, a la conclusión de que se trata de elementos autónomos con criterios propios de determinación[29]. El tipo objetivo y el tipo subjetivo se encuentran mutuamente condicionados, pues el primero es el objeto del segundo y el segundo define la relevancia típica del primero. Ambos aspectos de la imputación sólo adquieren un sentido completo cuando son contemplados de manera conjunta.

La construcción del tipo penal sigue los lineamientos de la teoría del delito aplicada a la ciberdelincuencia:

4.7.2.1. Tipo Objetivo: Dado que el derecho penal sanciona la conducta de una persona que perjudica a la otra, el tipo penal debe precisar primeramente quienes son los sujetos del delito.

A) Sujetos:

a.1) Sujeto Activo: Delito común (*delictum communis*[30]), puede ser cometido por cualquier persona, de allí que la fórmula legal considere la redacción de "El que..."

El sujeto activo es indeterminado, por lo que, nos encontramos frente a un delito común, lo que significa que puede ser cometido por cualquier persona. Como sostiene Villavicencio Terreros[31], la utilización de la fórmula legislativa "El que..." indica que el deber de abstención incumbe a todos los ciudadanos sin requerir una cualidad funcional especial (Villavicencio, 2006, p. 305). Esta configuración es indispensable para abarcar la heterogeneidad de actores que participan en el mercado negro de datos, desde el hacker hasta el revendedor final.

a.2) Sujeto Pasivo: La sociedad (bien colectivo) y el titular de los datos (persona natural o jurídica).

Se adopta una concepción pluriofensiva del injusto penal. A diferencia de los delitos patrimoniales clásicos —donde la afectación suele ser unívoca-, en el tráfico de datos informáticos concurren dos niveles de afectación que definen la titularidad del sujeto pasivo:

---

[28] García Cavero, Percy. Derecho Penal Parte General, 3ra edición corregida y actualizada. 2019. Ideas solución editorial. p. 406

[29] Rojas Aguirre Revista de Derecho, Vol. XXIII, N°1 (julio de 2010), p. 249 y s.

[30] Significa "delito común", refiriéndose a un acto ilícito que puede cometer, sin necesidad de tener una cualidad o condición especial (como ser funcionario o un menor de edad), a diferencia de los delitos especiales donde se requiere una característica particular del autor.

[31] Villavicencio Terreros, F. (2006). Derecho Penal: Parte General. Editora Jurídica Grijley

a.2.1) **El sujeto pasivo inmediato (titular del dato):** Comprende tanto a la persona natural, en su calidad de titular del derecho fundamental a la autodeterminación informativa y la intimidad (inciso 6 del artículo 2 de la Constitución), como a la persona jurídica, cuyos activos de información, secretos comerciales o bases de datos corporativas son objeto de comercialización ilícita.

a.2.2) **El sujeto pasivo mediato (La Sociedad):** El delito trasciende la esfera privada para convertirse en una amenaza al orden socioeconómico y la seguridad pública. La libre circulación de datos robados erosiona la "Confianza Digital" necesaria para el funcionamiento del mercado y la administración pública.

Esta naturaleza dual no es una construcción arbitraria, sino que encuentra sólido respaldo en la doctrina nacional. Al respecto, el profesor Alonso Peña Cabrera Freyre, al analizar la fenomenología de los ciberdelitos, establece que:

> *"En los delitos informáticos, la identificación del sujeto pasivo reviste una complejidad particular. No solo se afecta al titular de la información (sujeto pasivo de la acción), sino que, dada la masividad y el potencial destructivo de estas conductas, se lesiona la seguridad del tráfico jurídico y la fe pública. Por tanto, estamos ante figuras pluriofensivas donde concurren intereses individuales y colectivos, siendo la sociedad el sujeto pasivo mediato que reclama la protección de la integridad del entorno digital."*[32]

En virtud de esta caracterización doctrinaria, se legitima la intervención de oficio del Ministerio Público en defensa de la Sociedad (interés difuso), sin perjuicio del derecho de los titulares afectados (ciudadanos o empresas) de constituirse en actores civiles para reclamar la reparación por el daño directo sufrido.

B) La conducta típica

La conducta típica es la que establece concretamente la forma de actuación (verbo rector) que lesiona la norma penal.

En un primer momento se entendió que esta conducta solamente podía estar constituida por realizaciones activas, por lo que las omisiones solamente se podían castigar si concurría un fundamento especial establecido en la ley o en un contrato. De hecho, el que en muchas legislaciones penales se incorporara una regla general que establecía los presupuestos para castigar la omisión como una comisión, respondía a la lógica de que los tipos penales de la Parte Especial solamente castigan conductas activas.

A esta cláusula general se le asignaba, por tanto, una naturaleza constitutiva, por lo que producía una ampliación de lo punible. Tal comprensión se encuentra actualmente abandonada, siendo la posición dominante aquella

[32] Peña Cabrera Freyre, A. R. (2016). Los Delitos Informáticos en el Código Penal Peruano. Lima: Instituto Pacífico, pp. 85-88

que sostiene que la conducta definida en el tipo penal, salvo supuestos de clara limitación a una actuación comisiva, abarca tanto las acciones como las omisiones. En consonancia con la naturaleza normativa que se le asigna actualmente a la categoría de la tipicidad, la conducta típica no constituye la descripción de una conducta[33].

Ahora bien, desde la perspectiva de la técnica legislativa, nos encontramos ante un tipo penal mixto alternativo, esto significa que la realización de cualquiera de las conductas descritas por los verbos rectores es suficiente para la consumación del delito, sin que sea necesaria la concurrencia de todas ellas.

A fin de garantizar el Principio de Taxatividad, se procede a delimitar el alcance jurídico de cada verbo rector incorporado en la fórmula legal:

b.1). POSEER (Tenencia ilícita)

Esta es la innovación central del presente Decreto Legislativo, diseñada para sancionar la fase estática del delito.

Implica el dominio o señorío de hecho sobre los datos informáticos, independientemente de la titularidad. En el entorno digital, "poseer" se materializa en el almacenamiento de la información en dispositivos físicos (USB, discos duros, servidores) o lógicos (nubes, cuentas de correo), bajo la esfera de control del agente.

La Corte Suprema, en el Acuerdo Plenario Nº 6-2023, al referirse a delitos de posesión, establece que lo determinante es la "disponibilidad potencial" del bien delictivo.

En ese sentido, se sanciona a quien tiene la base de datos "disponible" para ser usada, vendida o distribuida. No se requiere que la esté vendiendo en ese instante; la mera tenencia de un activo ilícito (como una base de datos de huellas dactilares robada) ya configura un peligro abstracto para la seguridad ciudadana.

Se diferencia de la posesión inocua mediante el elemento subjetivo (dolo), en tanto, solo es penalmente relevante la posesión de la base de datos con conocimiento del origen ilícito o presunción del mismo.

b.2). COMPRAR/RECIBIR (La demanda)

Sanciona al "cliente" o receptor final que alimenta el mercado. Se tratan de conductas mediante las cuales el sujeto activo incorpora los datos informáticos a su esfera de dominio, ya sea a título oneroso (compra), por una transferencia gratuita o mediata (recibir).

[33] García Cavero, Percy. Derecho Penal Parte General, 3ra edición corregida y actualizada. 2019. Ideas solución editorial. p. 410

Siguiendo a Prado Saldarriaga[34] en su análisis sobre la Receptación, implica un acto traslativo de dominio fáctico. En el ciberespacio, esto se consuma en el momento de la descarga (*download*) o la recepción de las credenciales que permiten el acceso a la data.

b.3). COMERCIALIZAR y VENDER (La oferta onerosa)

Sanciona la monetización expresa del dato.

Vender: Transacción específica de dar los datos a cambio de una contraprestación económica (dinero, criptomonedas).

Comercializar: Concepto más amplio que abarca toda la actividad mercantil, incluyendo la oferta pública, la publicidad de bases de datos en foros, redes sociales o marketplaces, y la negociación, aunque la venta final no se concrete.

La jurisprudencia en delitos económicos entiende que la comercialización se configura con la puesta en el mercado. Por tanto, quien publica en un grupo de Telegram "Vendo base de datos RENIEC 2024" ya está ejecutando el verbo rector "comercializar", sin necesidad de esperar a que aparezca un comprador.

El Tribunal Constitucional ha sostenido que, "La gravedad de una conducta penal puede determinarse legítimamente cuando el agente transforma un bien ilícito en fuente de lucro o lo introduce en circuitos económicos ilegales". (STC Exp. Nº 0003-2006-PI/TC).

b.4). FACILITAR (El intermediario). Sanciona al "enlace" o *broker* de datos. Se trata de la conducta de quien, sin ser necesariamente el vendedor ni el comprador, presta una ayuda esencial o accesoria que posibilita el flujo de los datos. Incluye a quien provee la plataforma tecnológica para la venta (administradores de foros de *leaking*[35]), a quien desencripta la data para hacerla legible, o a quien pone en contacto a la oferta con la demanda.

Doctrinariamente, se eleva lo que sería una "complicidad" a la categoría de autoría, debido a la importancia estratégica de los intermediarios en la dinámica económica del cibercrimen.

b.5). INTERCAMBIAR (El trueque digital). Sanciona las transacciones no monetarias, muy comunes en la cultura hacker. Entrega recíproca de datos informáticos. En la comunidad del cibercrimen, es común la práctica del "You give me, I give you" (yo te doy una base de datos de Perú, tú me das una de Colombia), sin que medie dinero. Si solo se tipificara la "venta", estos intercambios quedarían impunes por ausencia de lucro dinerario directo. El verbo "intercambiar" cierra esa brecha.

[34] Prado Saldarriaga, V. R. (2017). Derecho Penal: Parte Especial. Instituto Pacífico.

[35] La fuga de *información* ocurre cuando un sistema, diseñado para ser inaccesible a cualquier intruso, revela *información* a terceros no autorizados.

b.6). TRAFICAR (El ciclo integral). Es el verbo "omnibus" o de cierre. Según el penalista Luis Alberto Bramont-Arias[36], "traficar" implica realizar operaciones comerciales o de negociación de manera ilegal y generalizada.

Se utiliza para abarcar conductas complejas de movimiento de datos a gran escala, importación/exportación de bases de datos transfronterizas, o cualquier otra modalidad de circulación ilícita que no encaje perfectamente en los verbos anteriores pero que implique poner los datos en el flujo del comercio ilegal.

A partir de la naturaleza de la acción, y estando la descripción típica de los verbos rectores, debemos precisar que se trata de un delito de mera actividad, en tanto, no requiere que se produzca un fraude bancario efectivo (resultado lesivo posterior) para su consumación; basta con la puesta en circulación de la data, pues dicho acto ya genera un riesgo inaceptable para el bien jurídico.

C) Datos informáticos, credenciales de acceso o bases de datos personales

La correcta delimitación de los conceptos empleados en un tipo penal constituye una exigencia derivada de los principios de legalidad, taxatividad y seguridad jurídica, reconocidos por la Constitución Política del Perú y desarrollados por la jurisprudencia del Tribunal Constitucional. En el ámbito del derecho penal informático, dicha exigencia adquiere especial relevancia, dado el carácter dinámico de la tecnología y la multiplicidad de usos legítimos de la información digital.

En ese marco, el tipo penal incorpora conceptos que ya se encuentran definidos y reconocidos por el ordenamiento jurídico nacional e internacional, lo que garantiza su adecuada interpretación y aplicación.

C.1) Datos informáticos

C.1.1) Definición y naturaleza jurídica

El objeto material del tipo penal se estructura en torno al concepto de datos informáticos, el cual se encuentra expresamente definido en el artículo 2 de la Ley Nº 30096, Ley de Delitos Informáticos. En concordancia con el literal b) del artículo 1del Convenio de Budapest sobre Ciberdelincuencia, se concibe como:

> "Toda representación de hechos, información o conceptos expresados en forma susceptible de ser procesada en un sistema informático, incluidos los programas y las bases de datos."

Esta definición posee un alcance amplio, comprensivo y tecnológicamente neutro, alineado con los compromisos internacionales del Estado. Permite abarcar toda información susceptible de tratamiento digital, con independencia de su formato, soporte o medio de almacenamiento, siempre

[36] Bramont-Arias Torres, L. A. (2002). Manual de Derecho Penal: Parte Especial. Editorial San Marcos.

que sea jurídicamente relevante y funcionalmente idónea para afectar los bienes jurídicos tutelados por la norma penal.

C.1.2) Alcance del concepto

Bajo el paraguas de esta definición legal, el término "datos informáticos" comprende un universo amplio de información digitalizada que incluye, de manera enunciativa mas no limitativa:

- Información alfanumérica almacenada o transmitida mediante sistemas informáticos.
- Archivos digitales tales como textos, imágenes, audios, videos y registros multimedia.
- Registros electrónicos y *logs*[37] de actividad.
- Información contenida en servidores físicos o virtuales, servicios de computación en la nube, discos duros, dispositivos USB u otros soportes tecnológicos.

Este alcance permite abarcar tanto datos estructurados como no estructurados, así como información en tránsito o en reposo, asegurando que el tipo penal no dependa de la forma técnica específica que adopte la información, sino de su naturaleza como dato procesable.

C.1.3) Justificación de la taxatividad del objeto material (Lex Certa)

La delimitación del objeto material en torno al concepto de "datos informáticos" responde a la necesidad de garantizar el principio de legalidad penal en su dimensión de certeza, reconocido en el literal d), inciso 24 del artículo 2de la Constitución Política del Perú y desarrollado por el Tribunal Constitucional (STC Exp. N.os 0014-2002-AI/TC y 010-2002-AI/TC).

En atención a ello, se ha optado por prescindir de fórmulas genéricas adicionales como "cualquier información digital", dado que el concepto técnico-legal de "datos informáticos" ya cumple adecuadamente la función de cláusula de cierre del tipo penal. Incorporar términos indeterminados podría generar un grado de imprecisión incompatible con el Derecho Penal moderno, el cual exige que el objeto material guarde una relación funcional directa con el bien jurídico protegido.

En consecuencia, el presente Decreto Legislativo se centra en el concepto de datos informáticos como eje rector, precisando expresamente la inclusión de credenciales de acceso y bases de datos personales únicamente por su especial relevancia criminológica y su habitual instrumentalización para la comisión de delitos patrimoniales y fraudes, reforzando así la claridad normativa sin sacrificar la neutralidad tecnológica.

C.2) Credenciales de acceso

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

[37] Un *log* es un registro oficial, cronológico y secuencial de eventos que ocurren dentro de un sistema, red, servidor o aplicación. Se generan automáticamente cada vez que un usuario (humano o máquina) realiza una acción.

Las credenciales de acceso se encuentran expresamente contempladas en la Ley Nº 30096, particularmente en su artículo 8, que sanciona el tráfico ilegal de contraseñas, códigos de acceso o datos similares que permitan acceder a un sistema informático.

Esta regulación reconoce que las credenciales constituyen instrumentos habilitantes del acceso a sistemas informáticos, aun cuando no contengan información personal en sentido estricto.

C.2.1) Concepto jurídico-funcional

Desde una perspectiva legal y técnico-funcional, las credenciales de acceso comprenden, entre otros:

- Usuarios y contraseñas.
- Códigos PIN y claves de seguridad.
- Tokens de autenticación.
- Claves de acceso a correos electrónicos, aplicativos, plataformas financieras o sistemas institucionales.
- Códigos de verificación.

Estas credenciales permiten el control funcional del sistema, posibilitando la ejecución de acciones que el titular legítimo no ha autorizado.

C.2.2) Relevancia penal

Las credenciales de acceso no constituyen simples datos neutros, sino medios idóneos para la afectación directa de la seguridad informática, ya que son: a) El principal objeto de comercio en mercados digitales ilícitos; b) Permiten la comisión de delitos posteriores como fraude informático, extorsión, suplantación de identidad y vaciamiento de cuentas; y c) Facilitan el acceso reiterado y masivo a sistemas protegidos.

Por ello, su inclusión expresa en el tipo penal resulta indispensable para cerrar la cadena delictiva, sancionando no solo al intruso que vulnera el sistema, sino también a quienes compran, comercializan o trafican los accesos ilícitos.

C.3) Bases de datos personales

Las bases de datos personales se encuentran reguladas principalmente por la Ley Nº 29733, Ley de Protección de Datos Personales, y su Reglamento aprobado por el Decreto Supremo Nº016-2024-JUS, entendiéndose como: "Todo conjunto organizado de datos personales, automatizado o no, independientemente del soporte, que permita el acceso a los datos."

C.3.1) Elementos esenciales del concepto

De la definición legal se desprenden los siguientes elementos esenciales:

- Un conjunto organizado de información.
- Referida a personas naturales identificadas o identificables.
- Susceptible de tratamiento automatizado o manual.

Estas bases pueden contener información de carácter:

- Identificatorio.
- Económico o financiero.
- Laboral, educativo o académico.
- Biométrico o sensible.

C.3.2) Necesidad de una protección penal reforzada

Si bien la Ley Nº 29733 prevé un régimen de sanciones administrativas, este resulta insuficiente frente a la gravedad del fenómeno criminal actual, caracterizado por: La comercialización masiva de bases de datos, su uso como insumo para delitos graves, e impacto directo en la seguridad ciudadana, patrimonial y digital.

En ese contexto, la tipificación penal de la compra y tráfico de bases de datos personales responde a la necesidad de una protección penal reforzada, en armonía con el derecho fundamental a la autodeterminación informativa, reconocido en el inciso 6 del artículo 2 de la Constitución Política.

D) Definición de los elementos normativos de ilicitud

Los términos empleados sobre la procedencia de la data se interpretan conforme al ordenamiento vigente, así por ejemplo:

D.1) "Obtenida sin consentimiento": Se remite al estándar de la Ley Nº 29733, Ley de protección de datos personales; en este instrumento normativo el consentimiento se define como la manifestación de voluntad libre, previa, expresa e informada. Por lo que, la frase "sin consentimiento" atrapa aquellas conductas donde el acceso original pudo ser lícito (ej. un administrador de sistemas), pero el desvío de la información (para venderla) no fue consentido.

Al respecto, el Tribunal Constitucional (Exp. 04467-2006-PHD/TC) establece que el consentimiento es la piedra angular de la autodeterminación informativa, sin él, cualquier tratamiento o transferencia comercial deviene en ilícita.

D.2) "Vulneración de sistemas de seguridad": Se remite a los tipos penales de la Ley Nº 30096 (artículo 2 y siguientes) y al estándar del Convenio de Budapest. El artículo 2 de la Ley N° 30096, Ley de delitos informáticos, sanciona a quien accede a un sistema "vulnerando medidas de seguridad"; regulación que se alinea con el artículo 2 del Convenio de Budapest, mediante el cual se exige que el acceso sea sancionado cuando se infringe una medida de seguridad (física o lógica).

D.3) "Comisión de un delito informático": Considerada como una cláusula de cierre. Este es el término "paraguas" u omnicomprensivo, que hace referencia a cualquier conducta tipificada en la Ley Nº 30096, Ley de Delitos Informáticos, para cubrir modalidades que no necesariamente implican "vulnerar seguridad" en el sentido clásico.

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - V°B° - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

S. DE LA CRUZ Q.

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

Este elemento normativo tiene como finalidad evitar lagunas legales; por lo que, si la data provino de un phishing (fraude) y no de un hacking de fuerza bruta, este término asegura que su venta sea delito.

El análisis de estos elementos normativos deben ser interpretados bajo la comprensión de información no pública. El tipo penal abarca "información digital no pública", por lo que, es vital definir esto para no criminalizar la recolección de fuentes abiertas (OSINT[38]). La legislación peruana tiene definiciones claras al respecto:

La Ley de transparencia y acceso a la información pública (Ley Nº 27806): Esta ley establece por exclusión qué es información pública. Define tres categorías protegidas (no públicas):

- Información Secreta: Ámbito militar y defensa nacional (artículo 15).
- Información Reservada: Seguridad ciudadana, inteligencia policial (artículo 16).
- Información Confidencial: Datos personales, secreto bancario, secretos comerciales e industriales (artículo 17).

Por su parte, **la Constitución Política del Perú**, protege el secreto bancario y reserva tributaria, así como, secreto e inviolabilidad de comunicaciones, en los numerales 5 y 10 del artículo2 de la Constitución, respectivamente.

4.7.2.2. ANÁLISIS DEL TIPO SUBJETIVO: EL DOLO Y LA PRESUNCIÓN DE ILICITUD

La configuración del injusto penal es eminentemente dolosa. La norma rechaza cualquier forma de responsabilidad objetiva (sanción por el mero resultado) y, en su lugar, exige un vínculo subjetivo claro entre el autor y el origen ilícito del dato.

Para ello, la fórmula legislativa "teniendo conocimiento o debiendo presumir" abarca dos modalidades de imputación subjetiva que son necesarias.

A. EL DOLO DIRECTO: "Teniendo Conocimiento"

Esta modalidad se configura cuando el agente tiene plena conciencia (aspecto cognitivo) y voluntad (aspecto volitivo) de que los datos informáticos que posee, vende o trafica tienen un origen delictivo. Se acredita cuando la ilicitud es explícita.

Ejemplo: El sujeto que compra una base de datos en un foro de la *Dark Web* donde el vendedor anuncia explícitamente: "Vendo base de datos del Banco X". Aquí, el conocimiento de la procedencia ilegal ("vulneración de sistemas") es innegable. El autor quiere realizar la conducta sabiendo que trafica una base no pública.

[38] *Open Source Intelligence* (Inteligencia de Fuentes Abiertas) y se refiere a la práctica de recopilar, analizar y difundir información disponible públicamente en internet y otras fuentes abiertas (redes sociales, noticias, registros públicos, foros) para generar conocimiento útil, aplicado comúnmente en ciberseguridad, periodismo, investigación y seguridad nacional para evaluar riesgos, identificar amenazas o apoyar la toma de decisiones.

B. EL DOLO EVENTUAL Y LOS INDICIOS DE CRIMINALIDAD ("DEBIENDO PRESUMIR")

La frase "debiendo presumir" habilita al juzgador a construir la imputación subjetiva (dolo eventual) a partir de indicios objetivos concomitantes. No se exige que el sujeto activo haya confesado saber que la data era robada (prueba directa), sino que las circunstancias externas hacían evidente su ilicitud.

La Corte Suprema ha validado reiteradamente el uso de indicios para acreditar el conocimiento del origen ilícito en delitos de mercado negro (Receptación). Resulta aplicable mutatis mutandis el criterio establecido en el Recurso de Nulidad N° 3390-2011/LIMA: "El conocimiento de la procedencia ilícita no requiere una certeza absoluta, sino que basta con que el agente, por las circunstancias del hecho (precio, lugar, modo), haya tenido la posibilidad de representarse el origen delictuoso y, pese a ello, haya actuado indiferente al bien jurídico protegido."

Asimismo, en el Recurso de Nulidad N° 2582-2013/LIMA, la Corte Suprema establece los "Indicios de ilicitud" que el juez debe valorar y que fundamentan la cláusula "debiendo presumir", así por ejemplo, podemos señalar:

La clandestinidad del canal de adquisición: La adquisición de datos en entornos no regulados o anónimos (grupos de Telegram, foros de la Deep Web, galerías informáticas informales) constituye un indicio unívoco de ilicitud. Como señala la jurisprudencia, el "ciudadano medio" sabe que las bases de datos legítimas no se venden en mercados negros.

El precio vil o irrisorio: Comprar una base de datos con millones de registros (activos de alto valor) a un precio muy por debajo del costo de mercado o de una licencia oficial, activa el deber de presunción de ilicitud. La desproporción económica es, según la Ejecutoria Suprema R.N. N° 3203-2003, un indicador objetivo del origen delictivo.

La ausencia de documentación: La falta de contratos, facturas o cláusulas de consentimiento informado que respalden la transferencia de la data impide alegar buena fe. En el derecho penal económico moderno, el incumplimiento de deberes de veracidad documental impide invocar el Principio de Confianza.

En ese sentido, no se trata de una presunción legal absoluta *(iuris et de iure)*, sino de una inferencia basada en indicios objetivos concomitantes.

4.7.2.3. FUNDAMENTACIÓN DE LAS CIRCUNSTANCIAS AGRAVANTES

La estructura penológica establece un marco punitivo base de cinco (5) a ocho (8) años, y un tipo cualificado agravado de ocho (8) a diez (10) años de pena privativa de libertad. Este incremento de la punibilidad no responde a criterios de arbitrariedad, sino a una exigencia del Principio de Proporcionalidad, reservando la sanción más severa para aquellos supuestos donde la conducta del agente denota una mayor peligrosidad o genera un daño sistémico.

En ese sentido, se han seleccionado taxativamente tres circunstancias agravantes que transforman la naturaleza del ilícito, elevando su lesividad de un plano individual a uno de seguridad pública y orden socioeconómico:

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -
MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B° - S. DE LA CRUZ Q.
MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

A. INTEGRACIÓN EN ORGANIZACIÓN CRIMINAL (mayor desvalor de la acción)

Esta agravante sanciona el peligro inherente a la estructura delictiva. Desde una perspectiva criminológica, el tráfico de datos ha evolucionado de la acción individual (*hacker* solitario) a una "industria criminal" jerarquizada. En consecuencia, la intervención de una organización criminal (conforme a los alcances de la Ley Nº 30077, Ley contra el Crimen Organizado) implica una división funcional de roles (obtención, procesamiento, venta y lavado de activos) y una vocación de permanencia en el tiempo.

La actuación corporativa disminuye las posibilidades de defensa de la víctima y del Estado, garantizando la continuidad del mercado ilícito incluso si se detiene a un individuo. Por tanto, el plus de antijuridicidad reside en el aparato logístico que el agente pone al servicio del delito, justificando la máxima severidad penal para desarticular la dinámica económica del cibercrimen.

B. AFECTACIÓN DE UNA PLURALIDAD DE PERSONAS O PERJUICIO PATRIMONIAL GRAVE

Esta circunstancia recoge un criterio mixto (cuantitativo y cualitativo) para medir la magnitud del daño, reconociendo la potencialidad expansiva única de los delitos informáticos.

La afectación a una pluralidad de personas: A diferencia de los delitos patrimoniales clásicos, la comercialización de una sola base de datos (v.gr. filtraciones de RENIEC, operadoras de telefonía o entidades bancarias) vulnera simultáneamente la autodeterminación informativa de miles o millones de ciudadanos. En este supuesto, el bien jurídico trasciende la esfera individual para convertirse en una afectación a la Seguridad Ciudadana y la Confianza Digital colectiva. La pluralidad del daño exige una respuesta punitiva equiparable a los delitos de estragos o peligro común.

Por otro lado, el criterio económico sanciona el impacto directo en la economía nacional. El tráfico de datos corporativos, secretos industriales o credenciales financieras suele derivar en fraudes millonarios o competencia desleal destructiva. Cuando el lucro cesante o daño emergente supera el umbral de gravedad —cuya cuantificación corresponderá al juzgador—, la pena debe incrementarse para restablecer la vigencia de la norma y anular la rentabilidad económica del ilícito.

En consecuencia, estas dos agravantes específicas delimitan los contornos de la máxima intervención punitiva del Estado, aplicable únicamente a quienes hacen del delito su *modus vivendi* profesional (Crimen Organizado) o a quienes generan un daño irreparable a la sociedad o la economía (Pluralidad/Gravedad patrimonial).

C. LA BASE DE DATOS ES PROCESADA O CUSTODIADA POR UNA ENTIDAD PÚBLICA

La circunstancia agravante prevista en el literal c) del artículo 12-A responde a la necesidad de otorgar una protección penal reforzada a los datos informáticos que se encuentran bajo titularidad, administración o custodia de entidades públicas. Dichos sistemas de información suelen contener datos sensibles de alcance masivo, cuya afectación ilícita trasciende la esfera individual de sus titulares y compromete la confianza ciudadana en las instituciones del Estado, así como la continuidad y seguridad de los servicios públicos.

Desde una perspectiva dogmático-penal, la obtención, posesión o tráfico ilícito de datos informáticos custodiados por entidades públicas presenta un mayor desvalor de acción y de resultado, en comparación con conductas que recaen sobre información de naturaleza privada. Ello se debe a que tales conductas no solo alimentan el mercado ilícito de datos, sino que afectan directamente el orden público digital, la seguridad de los sistemas estatales y, en determinados casos, la seguridad nacional.

La agravante se justifica, por tanto, por el objeto material de la acción, en la medida en que la información pública cumple una función estructural en la organización del Estado y en la relación de confianza entre la administración y la ciudadanía.

Por otro lado, es necesario otorgar una protección reforzada de los datos personales y de la información en poder del Estado, en tanto, tiene incidencia con el derecho fundamental a la autodeterminación informativa, reconocido por el Tribunal Constitucional. Al respecto, la jurisprudencia constitucional ha destacado que el Estado no solo debe abstenerse de afectar indebidamente los datos personales, sino que tiene el deber positivo de garantizar su adecuada protección; acciones de tutela y protecciones que deben ser especiales cuando estos forman parte de registros públicos o sistemas administrativos.

Finalmente, la agravante prevista en el literal c) es compatible con los estándares internacionales en materia de ciberdelincuencia, los cuales reconocen la importancia de brindar una respuesta penal diferenciada cuando las conductas ilícitas afectan infraestructuras críticas, sistemas estatales o información de relevancia pública. Asimismo, se alinea con una política criminal orientada a desarticular los mercados ilícitos de datos, fortalecer la seguridad ciudadana en el entorno digital, así como el ecosistema normativo de seguridad y confianza digital del Estado.

4.7.3. DELIMITACIÓN DEL TIPO PENAL, CLÁUSULA EXPRESA DE ATIPICIDAD Y SU COHERENCIA CONVENCIONAL

El tipo penal ha sido diseñado conforme a los principios constitucionales de lesividad, proporcionalidad, intervención mínima y culpabilidad, de modo que la sanción penal se circunscribe exclusivamente a aquellas conductas que presentan un desvalor penal efectivo, excluyéndose expresamente aquellas actuaciones que, aun involucrando la posesión, recepción o tratamiento de datos informáticos de origen ilícito, se desarrollan

en el marco de actividades legítimas, constitucionalmente protegidas o legalmente habilitadas.

Si bien el Código Penal contempla en el inciso 8 del artículo 20, una causa general de exclusión de responsabilidad penal por ejercicio legítimo de un derecho, oficio o cargo, dicha disposición opera en el plano de la justificación, una vez afirmada la tipicidad penal. No obstante, tratándose de un tipo penal que sanciona conductas de peligro abstracto y que incorpora verbos amplios como "poseer" o "recibir" datos informáticos, resulta necesario definir *ex ante* el perímetro de lo penalmente relevante, a fin de evitar interpretaciones expansivas incompatibles con el principio de intervención mínima del Derecho Penal.

En tal sentido, el proyecto incorpora una cláusula expresa de atipicidad, destinada a excluir del ámbito de aplicación del tipo penal aquellas conductas que, aun pudiendo involucrar datos informáticos de origen ilícito, se realizan bajo un título legítimo y con una finalidad constitucionalmente protegida, siempre que no exista aprovechamiento ilícito ni comercialización indebida de la información.

Esta exclusión normativa comprende, entre otros supuestos, los casos en que la adquisición, posesión, intercambio o tratamiento de datos informáticos se efectúa con autorización expresa del titular, conforme al marco normativo que establece la Ley Nº 29733, en cumplimiento de un mandato judicial o administrativo emitido conforme a ley[39], o en el ejercicio legítimo de derechos fundamentales o de funciones legalmente reconocidas, tales como el periodismo de investigación[40], la investigación académica, la ciberseguridad defensiva, la respuesta a ataques de ciberseguridad, la investigación forense digital, el ejercicio del derecho de defensa[41] y las obligaciones de *compliance.*

Con ello, el proyecto asegura que la intervención penal se dirija exclusivamente contra las conductas que integran el mercado ilícito de datos informáticos y que presentan un claro desvalor penal, reforzando la tutela de la autodeterminación informativa sin

[39] Desde la dogmática penal, estas conductas se encuentran amparadas por una causa de atipicidad objetiva, en tanto el comportamiento se inserta dentro de un rol normativamente autorizado, excluyendo el desvalor de acción. Como señala Claus Roxin, el Derecho Penal no puede sancionar conductas que el propio ordenamiento jurídico exige, permite o impone, pues ello vulneraría el principio de coherencia del sistema normativo. En el ordenamiento peruano, esta exclusión se vincula con: El deber de colaboración con la justicia, las facultades de investigación del Ministerio Público y la PNP, las actuaciones administrativas de supervisión, fiscalización y control.

[40] Finalmente, se excluyen del tipo penal las conductas realizadas en el ejercicio del periodismo de investigación respecto de hechos de interés público, conforme a la libertad de información reconocida en el artículo 2 inciso 4 de la Constitución y a la jurisprudencia del Tribunal Constitucional. El Tribunal Constitucional ha sostenido que el derecho a informar y a ser informado cumple una función institucional esencial en una sociedad democrática, por lo que cualquier restricción penal debe ser estrictamente necesaria y proporcional. La recepción y análisis de información filtrada, cuando se realiza con fines informativos legítimos y sin finalidad de lucro ilícito, carece de desvalor penal, siendo inadmisible su criminalización.

[41] Tampoco resulta penalmente relevante la posesión o recepción de datos informáticos cuando se realice en el ejercicio del derecho de defensa o con fines de custodia probatoria, siempre que no exista finalidad de aprovechamiento ilícito. El derecho de defensa, reconocido en el artículo 139 inciso 14 de la Constitución, comprende no solo la actuación procesal, sino también la obtención, conservación y análisis de medios probatorios, incluidos aquellos de naturaleza digital.

afectar indebidamente el ejercicio de derechos fundamentales ni generar efectos inhibidores contrarios a un Estado constitucional de derecho.

La exclusión incorporada resulta plenamente compatible con los estándares del Convenio sobre la Ciberdelincuencia (Convenio de Budapest), el cual no impone una criminalización absoluta de la posesión o tratamiento de datos informáticos, sino únicamente de aquellas conductas realizadas de manera deliberada e ilegítima y con finalidad delictiva.

En particular, el artículo 6 del Convenio condiciona la punibilidad de la posesión de datos o credenciales a la intención de que estos sean utilizados para cometer delitos informáticos, mientras que el artículo 15 exige que la aplicación de las disposiciones penales se realice con pleno respeto de los derechos humanos y las libertades fundamentales, tales como la libertad de información, la investigación científica y el derecho de defensa.

En ese marco, la exclusión de responsabilidad penal para actividades como el periodismo de investigación, la ciberseguridad defensiva, la investigación forense digital, la respuesta a ataques de ciberseguridad, la investigación académica y las obligaciones de *compliance* constituye una concreción normativa de dichos estándares internacionales.

4.7.4. ANÁLISIS DE LA PENALIDAD

La penalidad para el delito de adquisición, posesión y tráfico ilícito de datos informáticos responde a la elevada lesividad de las conductas descritas, las cuales no constituyen meros actos preparatorios, sino comportamientos autónomos que consolidan y amplifican el daño generado por los delitos informáticos precedentes.

La posesión, adquisición y comercialización de información digital obtenida ilícitamente sostiene mercados criminales estructurados, facilita la reiteración delictiva y permite la afectación masiva de derechos fundamentales, especialmente la autodeterminación informativa, la seguridad patrimonial y la confianza en los sistemas digitales.

Análisis de la pena base (cinco a ocho años de pena privativa de libertad)

La pena base prevista —no menor de cinco (5) ni mayor de ocho (8) años— resulta razonable y proporcional, considerando: A) La gravedad objetiva de las conductas, que permiten la comisión de múltiples delitos posteriores (fraude, extorsión, suplantación de identidad); B) El carácter reiterativo y escalable del daño, propio del tráfico de información digital; y C) La comparación con otros delitos informáticos regulados en la Ley Nº 30096, cuyos marcos penales alcanzan rangos similares cuando se compromete gravemente la seguridad de la información.

Desde una perspectiva sistemática, el tráfico de datos ilícitos presenta un desvalor equivalente o superior al acceso ilícito aislado, pues no solo vulnera un sistema, sino que multiplica exponencialmente el número de víctimas potenciales.

La multa como sanción complementaria

La imposición de ciento ochenta (180) a trescientos sesenta y cinco (365) días-multa se justifica por la naturaleza lucrativa del delito, orientado al aprovechamiento económico

S. DE LA CRUZ Q.

de información ilícita. Esta sanción cumple una función de prevención general y especial, al neutralizar el incentivo financiero que caracteriza al mercado ilegal de datos y evitar que la actividad delictiva resulte económicamente rentable.

Las sanciones en el marco de las agravantes específicas

La agravante referida a la actuación como integrante de una organización criminal responde al mayor desvalor de acción, en tanto el tráfico de datos suele desarrollarse mediante estructuras organizadas, con división de funciones y capacidad de afectar de manera sistemática a un número indeterminado de víctimas. Por otro lado, la agravante vinculada al resultado permite graduar la respuesta penal conforme al impacto real de la conducta.

En el contexto, la elevación de la pena a un rango de ocho (8) a diez (10) años, resulta acorde con los criterios de política criminal aplicables a la criminalidad organizada, así como al principio de lesividad material, reforzando la proporcionalidad de la pena.

Adicionalmente, la pena de inhabilitación resulta adecuada cuando el agente se vale de su posición funcional, técnica o laboral para acceder, tratar o comercializar información digital ilícita, reforzando la prevención especial y evitando la reiteración delictiva.

Finalmente, es posible concluir que la estructura sancionadora resulta constitucionalmente legítima y coherente con el sistema penal vigente, en tanto: a) Guarda correspondencia con la gravedad del bien jurídico protegido; b) Permite una graduación adecuada de la pena según la entidad del daño; y c) Respeta los principios de proporcionalidad, razonabilidad y culpabilidad.

4.8. EXPLICACIÓN DE LOS ASPECTOS MÁS RELEVANTES Y LEGISLACIÓN COMPARADA

4.8.1. AUTONOMÍA DEL TIPO PENAL

El presente Decreto Legislativo configura el delito de "Adquisición, posesión y tráfico ilícito de datos informáticos", como un tipo penal autónomo. Esta característica dogmática resulta fundamental para superar las barreras probatorias que actualmente garantizan la impunidad en el ciberespacio. Como señala Víctor Prado Saldarriaga, la moderna política criminal exige que los delitos que sancionan el tráfico de bienes ilícitos se "emancipen"[42] de la dependencia procesal de los delitos previos, especialmente cuando estos últimos son de difícil probanza técnica

En el contexto del cibercrimen, condicionar la sanción del vendedor de una base de datos a la previa identificación y condena del *hacker* (autor del acceso ilícito) constituye una "prueba diabólica", dado el uso generalizado de herramientas de anonimato y la extraterritorialidad de los ataques. Por tanto, el presente tipo penal se consuma con la sola realización de los verbos rectores (poseer, comercializar, traficar u otros) sobre datos de procedencia delictiva, siendo irrelevante para la configuración típica si se ha identificado o no al autor de la sustracción inicial.

Esta autonomía se sustenta jurisprudencialmente en el estándar probatorio establecido por la Corte Suprema en el Acuerdo Plenario Nº 3-2010/CJ-116.

[42] Prado Saldarriaga, V. 2017. Derecho Penal: Parte Especial

Conforme a este criterio vinculante, para acreditar el origen ilícito del activo (los datos) no se requiere una sentencia judicial previa sobre el delito fuente, bastando con que se acredite dicho origen criminal a través de indicios suficientes y concurrentes que excluyan cualquier posibilidad de origen lícito.

4.8.2. TRATAMIENTO DEL CONSENTIMIENTO EN EL CASO DE DATOS INFORMÁTICOS DE NIÑAS, NIÑOS Y ADOLESCENTES

El Decreto Legislativo hace referencia a la obtención de datos informáticos "sin consentimiento de su titular", en concordancia con el derecho fundamental a la autodeterminación informativa y con el régimen general de protección de datos personales previsto en la Ley N° 29733. No obstante, resulta necesario precisar que, tratándose de datos personales de niñas, niños y adolescentes, el consentimiento válido se rige por un régimen especial de protección reforzada, atendiendo a su condición de personas en situación de especial vulnerabilidad.

En efecto, el Capítulo IV del Título I del Reglamento de la Ley N° 29733, aprobado por Decreto Supremo N° 016-2024-JUS, establece reglas específicas para el tratamiento de los datos personales de personas menores de dieciocho años. En particular, el artículo 22 dispone que el tratamiento de dichos datos se considera lícito cuando se obtiene el consentimiento de quien o quienes ejercen la patria potestad o tutela, según corresponda. Asimismo, reconoce que los adolescentes mayores de catorce y menores de dieciocho años pueden otorgar consentimiento para el tratamiento de sus datos personales, de acuerdo con su capacidad, siempre que la información sea proporcionada en un lenguaje claro y comprensible, y prohíbe expresamente que dicho consentimiento sea utilizado para permitir el acceso a bienes o servicios restringidos por razón de edad.

En ese marco, la referencia al "consentimiento del titular" contenida en el tipo penal propuesto no debe interpretarse de manera aislada o uniforme, sino de forma sistemática y conforme al régimen especial aplicable a los datos personales de niñas, niños y adolescentes. Ello implica que, para efectos de la configuración del delito, se considerará inexistente o inválido el consentimiento cuando el tratamiento, posesión, adquisición o tráfico de datos informáticos de personas menores de edad se realice al margen de las reglas específicas establecidas en el citado Reglamento, aun cuando formalmente se alegue la existencia de una autorización.

En consecuencia, la interpretación del tipo penal propuesto debe realizarse en concordancia con la Ley N° 29733 y su Reglamento.

4.8.3. JUSTIFICACIÓN DE LA INCORPORACIÓN DEL TIPO PENAL EN LA LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS

La Ley Nº 30096 constituye el marco normativo especializado para la protección penal frente a conductas que afectan la seguridad informática. El tipo penal tiene como objeto material los datos informáticos, credenciales de acceso e información digital.

En ese sentido, por el objeto materia del delito se vincula directamente con delitos fuente previstos en la propia Ley Nº 30096 (acceso ilícito, interceptación, fraude informático). Asimismo, se busca sancionar una fase posterior del *iter criminis*: la explotación y circulación del producto del delito informático.

4.8.3.1. Sobre su ubicación sistemática en la Ley N° 30096

La Ley Nº 30096, Ley de Delitos Informáticos ha sido objeto de sucesivas modificaciones destinadas a adecuar la respuesta penal frente a la evolución de la criminalidad informática. En dicho proceso, el legislador ha optado de manera consistente por una técnica legislativa de adición progresiva, mediante la creación de artículos suplementarios identificados con letras ("A"), en lugar de reestructurar el texto original o reactivar disposiciones previamente derogadas.

Este criterio se evidencia, entre otros, en la inclusión de los artículos 5-A, 8-A y 9-A, lo que revela una práctica normativa consolidada orientada a preservar la coherencia sistemática y la seguridad jurídica. Se reconoce que esta técnica resulta idónea cuando se integran nuevas modalidades delictivas en leyes penales especiales, pues permite ampliar su alcance material sin desnaturalizar su estructura original.

El Tribunal Constitucional ha señalado que la técnica legislativa debe respetar el principio de seguridad jurídica, garantizando normas claras, previsibles y estables (STC Exp. N.º 0008-2012-PI/TC). En tal sentido, la creación de un nuevo artículo 12-A resulta preferible a la reactivación de artículos derogados, pues evita la confusión interpretativa sobre la vigencia de disposiciones previas y preserva la confianza normativa de los operadores jurídicos.

Asimismo, desde la perspectiva del principio de conservación del derecho, la inserción de un nuevo artículo permite introducir un tipo penal autónomo, depurado y conforme a los estándares constitucionales actuales, sin reproducir deficiencias normativas previamente superadas. Reactivar un artículo previamente derogado —como ocurrió con el antiguo artículo 6 de la Ley Nº 30096— podría generar incertidumbre respecto del alcance de la voluntad legislativa, además de riesgos de contradicción con reformas posteriores.

Las leyes penales especiales deben organizarse conforme a criterios funcionales y de especialidad, agrupando conductas que protegen un mismo bien jurídico o que forman parte de una misma cadena delictiva (Roxin, Derecho Penal. Parte General, Tomo I). En el caso de la Ley Nº 30096, la adopción del artículo 12-A resulta coherente, en tanto el nuevo tipo penal se vincula directamente con delitos fuente ya previstos en la ley, sanciona una fase posterior del fenómeno criminal informático y permite reforzar la protección del bien jurídico central: la seguridad de la información y de los sistemas informáticos.

En consecuencia, la implementación del delito de adquisición, posesión y tráfico ilícito de datos informáticos como nuevo artículo 12-A de la Ley Nº 30096 constituye una opción técnicamente idónea, constitucionalmente legítima y sistemáticamente coherente, al reforzar la protección penal de la seguridad de la información sin alterar la arquitectura normativa vigente.

MINISTERIO DEL INTERIOR - Viceministerio de Orden Interno -

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO - V°B° S. DE LA CRUZ Q.

MINISTERIO DEL INTERIOR - Oficina General de Asesoría Jurídica -

4.8.4. SOBRE LA INEXISTENCIA DE SUPERPOSICIÓN CON EL ARTÍCULO 154-A DEL CÓDIGO PENAL

Si bien el ordenamiento cuenta con el Artículo 154-A (Tráfico ilegal de datos personales) del Código Penal, la evidencia empírica demuestra su ineficacia para desarticular un circuito delictivo asociado a la ciberdelincuencia, debido a:

La atipicidad de la posesión: El tipo vigente exige probar la "comercialización o venta". Esto impide la intervención penal en casos de hallazgo de bases de datos en poder del delincuente si no se acredita la transacción mercantil, generando impunidad en la fase de acopio.

El Bien jurídico restringido: El Artículo 154-A solo protege datos de "personas naturales". Se amplía el espectro a 'datos informáticos' y 'credenciales', protegiendo también la seguridad corporativa y financiera, activos críticos en la economía digital. Por lo que, no existe doble incriminación, considerando que se tratan de figuras autónomas que tutelan bienes jurídicos distintos y sancionan conductas claramente diferenciadas.

4.8.5. DERECHO COMPARADO

La presente norma para sancionar el tráfico y comercialización de datos informáticos no constituye una creación aislada del Perú, sino que responde a una tendencia de armonización global impulsada por la necesidad de combatir la ciberdelincuencia. El análisis comparado evidencia que los ordenamientos jurídicos de vanguardia han transitado de sancionar únicamente el "acceso ilícito" (*hacking*) a tipificar autónomamente los actos preparatorios y de comercialización (*trafficking*), reconociendo que el mercado negro de datos es el motor financiero del cibercrimen.

El referente supranacional vinculante es el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), del cual el Perú es parte. El artículo 6 de dicho Convenio regula el "Abuso de dispositivos", este artículo obliga a los Estados parte a tipificar la producción, venta, obtención para el uso, importación, distribución o puesta a disposición de dispositivos (incluidos programas informáticos y contraseñas de ordenador o códigos de acceso) diseñados para cometer ciberdelitos.

La *Ratio Legis*[43] de este artículo es criminalizar la existencia del "mercado de herramientas" y credenciales, por lo que, con ello el Perú está dando cumplimiento efectivo a este mandato internacional, cerrando la brecha de punibilidad respecto a los intermediarios de acceso.

A. ESPAÑA: EL ADELANTAMIENTO DE LA BARRERA PUNITIVA

El Código Penal español, referente histórico de nuestra legislación, incorporó tipos penales específicos para sancionar la "fase intermedia" del delito informático, superando la visión tradicional de la revelación de secretos.

[43] Ratio legis es una expresión latina que significa la "razón de la ley" o el "motivo legal", y se refiere a la finalidad, propósito o fundamento intrínseco de una norma jurídica, buscando entender el porqué de su existencia más allá de su letra literal para aplicarla correctamente.

El legislador español, en los artículos 197.bis y 197.ter del Código Penal Español, sanciona autónomamente a quien, sin haber accedido al sistema, "facilite" a terceros el acceso o posea programas/contraseñas para tal fin. Se castiga la mera posesión con fines delictivos.

Como señala el catedrático Francisco Muñoz Conde[44], estas reformas responden a la necesidad de castigar actos que, aunque preparatorios en la teoría clásica, poseen en el ciberespacio una lesividad autónoma suficiente para justificar la intervención penal.

B. ESTADOS UNIDOS: LA SANCIÓN AL "TRAFFICKING"

La legislación federal estadounidense cuenta con una de las normas más robustas contra el comercio de datos, enfocándose en el aspecto patrimonial del delito. Estados Unidos en el "18 U.S. Code § 1029 - Fraud and related activity in connection with access devices"[45] sanciona específicamente a quien "a sabiendas y con intención de defraudar, trafique (produzca, use o venda) con uno o más dispositivos de acceso falsificados o no autorizados".

---

[44] Muñoz Conde, F. (2019). Derecho Penal. Parte Especial. 22ª Ed. Valencia: Tirant lo Blanch. (Sobre los delitos informáticos en el CP español).

[45] Fraud and related activity in connection with access devices

(a) Offenses.— Whoever—

[...]

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

[...]

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(e) Definitions. As used in this section

(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

[...]

(5) the term "traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of.

La legislación norteamericana define "dispositivo de acceso" de forma amplia, incluyendo credenciales, números de cuenta y contraseñas; lo cual también se adopta en el presente Decreto Legislativo bajo esta lógica al incluir expresamente "credenciales de acceso y contraseñas" en el tipo penal, alineándose con la potencia investigativa del FBI en casos de Carding (tráfico de tarjetas).

C. CHILE: LA NUEVA LEY DE DELITOS INFORMÁTICOS (2022)

En el ámbito regional, Chile ha modernizado recientemente su legislación mediante la Ley Nº 21.459, que constituye el modelo más cercano y actualizado de implementación del Convenio de Budapest en Sudamérica. Chile en el artículo 6 (Receptación de datos informáticos), prescribe:

> "El que conociendo su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene [...] datos informáticos provenientes de la realización de las conductas descritas (acceso ilícito), sufrirá la pena de..."

La ley chilena utiliza los verbos "comercialice, transfiera o almacene", validando la estructura de la presente norma. En su oportunidad, la reforma chilena se sustentó en la necesidad de evitar la impunidad de quienes compran bases de datos robadas (el mercado secundario).

En ese sentido, la presente norma penal no introduce una innovación aislada, sino que se armoniza con los estándares internacionales y con la evolución del derecho penal comparado, reforzando la protección penal frente al tráfico de información digital ilícita y garantizando una respuesta coherente con el fenómeno contemporáneo del cibercrimen.

V. ANÁLISIS DE IMPACTOS CUANTITATIVOS Y/O CUALITATIVOS DE LA NORMA

5.1. Impactos cualitativos de la norma

El delito de adquisición, posesión y tráfico ilícito de datos informáticos genera impactos cualitativos relevantes y positivos en el sistema jurídico y en la política criminal del Estado, en tanto introduce una respuesta penal específica frente a un fenómeno que actualmente opera como un mercado ilícito estructurado y de alta rentabilidad.

En primer lugar, la norma tiene un efecto disuasivo directo sobre el mercado ilegal de datos informáticos, al sancionar no solo el acceso indebido, sino también la posesión, adquisición y comercialización de información digital de origen ilícito. La doctrina penal[46] ha señalado que la criminalización de los mercados secundarios constituye una estrategia eficaz para debilitar la criminalidad compleja, al afectar el incentivo económico que sostiene estas conductas.

En segundo término, la norma contribuye a la reducción de delitos derivados, tales como la extorsión, el fraude electrónico y la suplantación de identidad, en la medida en que dichos ilícitos requieren, como insumo esencial, el acceso a bases de datos, credenciales o información digital previamente obtenida o comercializada de forma ilegal. Este enfoque preventivo resulta compatible con la jurisprudencia constitucional que reconoce la

[46] Roxin, C. (2000). Política criminal y sistema del derecho penal (2.ª ed.). Civitas.

legitimidad de la intervención penal frente a riesgos estructurales y sistemáticos (STC Exp. Nº 0017-2011-PI/TC).

Asimismo, la tipificación fortalece la confianza digital en las transacciones electrónicas y en la gestión de información por parte de entidades públicas y privadas, al establecer un estándar penal claro frente al uso indebido de datos, lo cual incide positivamente en la seguridad jurídica y en el desarrollo de la economía digital.

Finalmente, el impacto cualitativo más relevante se proyecta en la protección reforzada de derechos fundamentales, particularmente la intimidad, la identidad personal, el honor y la autodeterminación informativa, reconocidos por el inciso 6 del artículo 2 de la Constitución y desarrollados por el Tribunal Constitucional como derechos que requieren una tutela penal efectiva frente a afectaciones masivas o reiteradas (STC Exp. Nº 04739-2007-PHC/TC).

5.2. Impactos cuantitativos de la norma

Desde el punto de vista cuantitativo, la necesidad de la intervención normativa se sustenta en indicadores institucionales que evidencian un incremento sostenido de los delitos informáticos y de las conductas asociadas al uso ilícito de información digital.

De acuerdo con reportes estadísticos de la Policía Nacional del Perú (SIDPOL), las denuncias vinculadas al acceso ilícito a sistemas informáticos han registrado un crecimiento exponencial en los últimos años, con incrementos acumulados significativamente superiores a los registrados en otros tipos delictivos, lo que revela una expansión acelerada de este fenómeno criminal.

A esta realidad operativa se suma la evidencia financiera reportada por la Unidad de Inteligencia Financiera (UIF-Perú). Según su Boletín Estadístico (Periodo 2015-2025)[47], los delitos informáticos han escalado hasta convertirse en una fuente relevante de activos ilícitos, registrándose 14 Informes de Inteligencia Financiera (IIF) vinculados específicamente a esta tipología por un monto acumulado de USD 45.6 millones.

La peligrosidad patrimonial de estas conductas se confirma en las medidas de coerción real: se han ejecutado y convalidado judicialmente 31 medidas de congelamiento de fondos por delitos informáticos, inmovilizando un total de USD 12,982,791. Cifra que, en términos de casos convalidados, supera incluso a delitos convencionales como el tráfico ilícito de drogas (12 casos) o la minería ilegal (5 casos).

Asimismo, según el informe oficial "Cobro y Silencio: La dinámica de la extorsión en el Perú"[48] (Ministerio del Interior, 2025), las denuncias por extorsión registraron un crecimiento exponencial del 679% en el último quinquenio, pasando de 2,605 casos en 2020 a 21,277 casos en 2024. Este incremento no es aleatorio, sino que responde a la masificación de modalidades virtuales: el 87% de estos delitos se cometen a través de medios no físicos (llamadas, mensajería instantánea y redes sociales), lo que ha obligado a las unidades

S. DE LA CRUZ Q.

[47] Superintendencia de Banca, Seguros y AFP. (2025). Información estadística de la Unidad de Inteligencia Financiera del Perú: Enero de 2015 a noviembre de 2025. Unidad de Inteligencia Financiera del Perú. Pág. 12 y 17

[48] Ministerio del Interior. (2025). Cobro y silencio: La dinámica de la extorsión en el Perú. Dirección General de Inteligencia del Ministerio del Interior (DIGIMIN).

especializadas a aperturar 5,759 expedientes de geolocalización tecnológica solo en 2024, un aumento drástico frente a los 1,176 de 2021.

En definitiva, la evidencia estadística revela que el Perú no enfrenta una simple ola delictiva, sino una mutación estructural de la criminalidad, donde la extorsión ha dejado de ser un delito de coacción física para convertirse en una industria digital de alto rendimiento financiero, con un incremento explosivo del 679% en la incidencia delictiva y una operatividad basada en un 87% en medios virtuales. Esta realidad deja obsoleto el marco legal actual, convirtiendo esta reforma en un imperativo indispensable para sancionar el tráfico de los activos digitales que hoy financian y sostienen al crimen organizado en el país.

Por otro lado, es preciso señalar que la aprobación y vigencia de la presente norma no irroga gastos adicionales al Tesoro Público. La modificación a la Ley N° 30096, Ley de Delito Informáticos, Ley N° 30096 y la persecución del nuevo tipo penal se financia con cargo al presupuesto institucional de los pliegos involucrados (Ministerio del Interior, Ministerio Público, Poder Judicial y Ministerio de Justicia y Derechos Humanos), sin demandar recursos adicionales.

VI. ANÁLISIS DE IMPACTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La presente norma tiene un impacto directo en el fortalecimiento del marco jurídico penal peruano, optimizando la respuesta del Estado frente a la ciberdelincuencia, sancionando el tráfico y comercialización de datos.

El impacto normativo se analiza desde las siguientes dimensiones de coherencia y vigencia:

6.1. Conformidad constitucional y protección de derechos fundamentales

Se alinea irrestrictamente con la Constitución Política del Perú, desarrollando legislativamente la protección de derechos fundamentales que hoy se ven vulnerados en el entorno digital, entre ellos:

- **Autodeterminación Informativa (inciso 6 del Artículo 2,):** La norma protege el derecho de los ciudadanos a que los servicios informáticos no suministren informaciones que afecten la intimidad personal y familiar. Al criminalizar el tráfico de bases de datos, el Estado eleva el estándar de protección de este derecho, pasando de una tutela meramente administrativa a una tutela penal (Ultima Ratio).
- **Secreto e Inviolabilidad de las Comunicaciones (inciso 10 del Artículo 2):** Al sancionar la comercialización de "credenciales de acceso y contraseñas", la norma protege la llave digital que resguarda el secreto de las comunicaciones privadas y documentos digitales.

6.2. Integración y cierre de brechas en la ley de delitos informáticos, Ley Nº 30096

El presente Decreto Legislativo impacta directamente en la Ley Nº 30096, llenando un vacío de punibilidad estructural, en tanto, actualmente, la Ley N° 30096 sanciona principalmente al "intruso" (quien realiza el hacking o acceso ilícito - Artículo 2 de la Ley 30096). Sin embargo, el ecosistema criminal moderno ha separado roles, como quien roba la data no siempre es quien la vende.

El nuevo artículo dota de autonomía sustantiva a la fase de fase de adquisición, posesión y tráfico ilícito de datos informáticos. Esta configuración normativa resulta fundamental para

S. DE LA CRUZ Q.

cerrar la brecha de impunidad que actualmente beneficia a los intermediarios de datos (*Data Brokers*), quienes operan tanto en mercados informales físicos como en entornos digitales (Deep Web, mensajería encriptada y redes sociales). De este modo, se neutraliza la estrategia de defensa basada en la ajenidad respecto al delito fuente, permitiendo la sanción penal del comercializador por la tenencia y tráfico del activo ilícito, independientemente de su participación en la intrusión informática inicial *(hacking).*

La norma se erige como Ley especial frente a la receptación patrimonial (Artículo 194 CP), superando la controversia dogmática sobre la idoneidad de los activos intangibles como objeto material del delito. De este modo, se dota de autonomía típica al tráfico de datos, emancipándolo de los elementos normativos propios de los delitos contra el patrimonio.

6.3. Armonización con el derecho administrativo sancionador, Ley Nº 29733

Se respeta el principio de *Non Bis In Idem* y articula con la Ley de Protección de Datos Personales. Mientras la Autoridad Nacional de Protección de Datos Personales (ANPD) sanciona administrativamente (multas) a las empresas formales por negligencia en el tratamiento de datos o fugas de información; el presente tipo penal se reserva para conductas dolosas de tráfico ilícito.

El impacto legislativo reside en criminalizar conductas que exceden la esfera administrativa. No se castiga al mal gestor de datos, sino al delincuente que lucra con ellos. Esto fortalece la capacidad disuasoria del Estado donde las multas administrativas han resultado insuficientes.

6.4. Impacto en el ordenamiento procesal penal

Al establecer una pena conminada de cinco a ocho años (tipo base) y ocho a diez años (agravada), se tiene un impacto estratégico en la investigación criminal regulada por el Código Procesal Penal, promulgado con el Decreto Legislativo Nº 957.

En ese contexto, al superar el umbral de los 4 años de pena privativa de libertad, este delito permite el uso de herramientas procesales avanzadas como el levantamiento del secreto bancario y de las comunicaciones y la videovigilancia.

Por otro lado, la severidad de la pena (superior a 5 años) permite a los operadores de justicia solicitar y dictar medidas de prisión preventiva para los traficantes de datos, algo que con la legislación actual (penas menores o multas) resulta procesalmente inviable, generando una percepción de impunidad.

La tipificación genera una conexión normativa automática con el régimen de excepción procesal de la Ley Nº 30077, Ley contra el Crimen Organizado, en tanto, al incorporarse el nuevo tipo penal dentro del catálogo de delitos de la Ley Nº 30096, Ley de Delitos Informáticos, se activa por remisión expresa lo dispuesto en el Artículo 3, inciso 9 de la Ley Nº 30077. Esta concordancia normativa tiene un impacto procesal estratégico, pues habilita al Ministerio Público y Policía Nacional del Perú para el uso de técnicas especiales de investigación reservadas para delitos de alta complejidad, tales como: Agentes encubiertos y especiales, interceptación postal y de comunicaciones, videovigilancia y seguimiento electrónico.

Finalmente, en el ámbito de la extradición y cooperación Internacional, tiene impacto dado que, al establecer penas graves, el delito cumple con el principio de doble incriminación

exigido en los tratados de extradición, facilitando la persecución de ciberdelincuentes que operan desde el extranjero.

VII. ANÁLISIS DE IMPACTO REGULATORIO EX ANTE – AIR EX ANTE

El Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, aprobado mediante Decreto Supremo N° 023-2025-PCM, señala lo siguiente:

> ***Artículo 33.- Ámbito de aplicación del AIR Ex Ante***
>
> *33.1 Es obligatorio presentar un expediente AIR Ex Ante, para evaluación de la CMCR, a fi n de obtener dictamen favorable que permita continuar con el trámite de aprobación del proyecto normativo.*
>
> *33.2 Las entidades públicas tienen la obligación de aplicar un AIR Ex Ante como herramienta de análisis previo, cuando el proyecto normativo de carácter general establezca y/o modifique una obligación, condición, requisito, responsabilidad, prohibición, limitación y/o cualquier otra regla que imponga exigencia(s):*
>
> *a) Que genere(n) o modifique(n) costos en su cumplimiento por parte de las personas; y/o,*
> *b) Que limite(n) el ejercicio, otorgamiento y/o reconocimiento de derechos de las personas, restringiendo el desarrollo de actividades económicas y sociales que contribuyan al desarrollo integral, sostenible, y al bienestar social.*
>
> *(...)*
>
> *33.4 El órgano de línea proponente coordina con el oficial de mejora de calidad regulatoria para identificar si un proyecto normativo requiere la presentación de un expediente AIR Ex Ante a la CMCR. En caso de que se determine que el proyecto normativo está fuera del alcance del AIR Ex Ante por encontrarse en alguno de los supuestos establecidos en el numeral 41.1 del artículo 41 del presente Reglamento, se justifica de manera expresa en la exposición de motivos.*
>
> *(...)*
>
> ***Artículo 41.- Supuestos que están fuera del alcance de la obligación de presentar expediente AIR Ex Ante a la CMCR***
>
> *41.1 Las entidades públicas están exceptuadas de presentar expediente AIR Ex Ante a la CMCR, por lo que se encuentran fuera de lo dispuesto en el numeral 33.2 del artículo 33 del presente Reglamento, en los siguientes supuestos:*
>
> *(...)*
>
> *j) Disposiciones normativas en materia penal, o que regulan los procesos en vía judicial (como códigos o leyes procesales).*
>
> *(...)*

De acuerdo a lo dispuesto en el literal j) del numeral 41.1 del artículo 41 del Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, aprobado mediante Decreto Supremo N° 023-2025-PCM, las entidades públicas están exceptuadas de presentar expediente Análisis de Impacto Regulatorio Ex Ante (AIR Ex Ante) a la Comisión Multisectorial de Calidad Regulatoria (CMCR) en el caso de disposiciones normativas en materia penal, o que regulan los procesos en vía judicial (como códigos o leyes procesales). En esa línea, la presente norma

se encuentra excluida del alcance AIR Ex Ante al estar inmersa en el supuesto antes descrito.

VIII. EXCEPCIÓN DE LA PUBLICACIÓN DE PROYECTOS NORMATIVOS

El Reglamento que establece disposiciones sobre publicación y difusión de normas jurídicas de carácter general, resoluciones y proyectos normativos, aprobado mediante Decreto Supremo N° 009-2024-JUS, establece en el numeral 19.1 del artículo 19 que los proyectos de normas jurídicas de carácter general deben ser publicados en las sedes digitales de las entidades de la Administración Pública a cargo de su elaboración o en otro medio, asegurando su debida difusión y fácil acceso.

Por otro lado, el numeral 19.2 del artículo 19 del mencionado reglamento regula las excepciones para la publicación de proyectos normativos:

> *19.2. Se exceptúa de la publicación del proyecto normativo a las siguientes disposiciones:*
>
> *a) Los decretos de urgencia ordinarios y los decretos legislativos.*
>
> *b) Las disposiciones que regulan actos, instrumentos y procedimientos de gestión interna de la entidad de la Administración Pública, o que regulan las relaciones interinstitucionales, así como disposiciones referidas a la organización del Estado.*
>
> *(...)*

En atención a lo expuesto, la presente propuesta se encuentra exceptuada de ser publicada en las sedes digitales, al encontrarse prevista como supuesto de excepción en el literal a) del numeral 19.2 del artículo 19 del Reglamento que establece disposiciones sobre publicación y difusión de normas jurídicas de carácter general, resoluciones y proyectos normativos, aprobado mediante Decreto Supremo N° 009-2024-JUS.

S. DE LA CRUZ Q.

El Peruano Firmado por: Editora Perú
Fecha: 24/01/2026 04:05

CUARTA.- Disposiciones normativas complementarias
El Ministerio de Cultura aprueba, por Resolución Ministerial, las disposiciones normativas que resulten necesarias para la aplicación del presente Decreto Legislativo, en un plazo no mayor de ciento veinte (120) días calendario contados a partir de su entrada en vigencia. Estas disposiciones deberán ser concordantes con lo previsto en la Ley N.° 32441, Ley que regula la promoción de la inversión privada mediante Asociaciones Público Privadas y Proyectos en Activos y su respectivo reglamento.

DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA

ÚNICA.- Modificación del artículo 53 de la Ley N° 28296, Ley General del Patrimonio Cultural de la Nación
Se modifica el artículo 53 de la Ley N° 28296, Ley General del Patrimonio Cultural de la Nación, el cual queda redactado en los siguientes términos:

*"**Artículo 53.- Convenios de administración***
*53.1 El Ministerio de Cultura está facultado para suscribir convenios de administración con **entidades públicas**, a fin de concederles autorización para la administración compartida de bienes inmuebles prehispánicos integrantes del Patrimonio Cultural de la Nación, siempre que garanticen su protección, investigación, conservación, restauración o puesta en valor, respetando las formalidades y procedimientos administrativos establecidos en los reglamentos vigentes.*
53.2 Mediante estos convenios puede acordarse mecanismos de distribución de los recursos –ingresos, fondos o contraprestaciones– generados por la puesta en valor del bien cultural inmueble, en los porcentajes y condiciones que las partes pacten en el propio Convenio.
53.3** Estos convenios deben garantizar el significado cultural del bien inmueble, favoreciendo su acceso y uso social. Se suscriben de manera voluntaria, a solicitud de la entidad **pública** que lo requiera **y bajo el trámite establecido por Resolución Ministerial.
***53.4 La vigencia de los convenios de administración** no puede exceder el plazo de diez (10) años renovables por un periodo similar, siempre y cuando no varíe o altere el propósito de este.*
53.5 No se incluye en los convenios de administración los sitios inscritos en la Lista del Patrimonio Mundial de la UNESCO.
*53.6 La suscripción de los convenios de administración no excluyen del cumplimiento de los **procedimientos estipulados en el Reglamento de Intervenciones Arqueológicas y de otras normas aprobadas** por el Ministerio de Cultura".*

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA.- Derogación
Se deroga la Ley N° 29164, Ley de promoción del desarrollo sostenible de servicios turísticos en los bienes inmuebles integrantes del Patrimonio Cultural de la Nación.

POR TANTO:

Mando se publique y cumpla, dando cuenta al Congreso de la República.

Dado en la casa de Gobierno, en Lima, a los veintitrés días del mes de enero del año dos mil veintiséis.

JOSÉ ENRIQUE JERÍ ORÉ
Presidente de la República

ERNESTO JULIO ÁLVAREZ MIRANDA
Presidente del Consejo de Ministros

ALFREDO MARTÍN LUNA BRICEÑO
Ministro de Cultura

2480387-1

DECRETO LEGISLATIVO Nº 1700

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

Que, mediante la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional, el Congreso de la República ha delegado en el Poder Ejecutivo la facultad de legislar, entre otros, en materia de seguridad y lucha contra la criminalidad organizada, por el plazo de sesenta (60) días calendario, computados a partir del día siguiente de su publicación;

Que, el subnumeral 2.1.14 del numeral 2.1 del artículo 2 de la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional, faculta al Poder Ejecutivo de modificar la Ley N° 30096, Ley de Delitos Informáticos, incorporando como delito conductas vinculadas a la adquisición, comercialización y tráfico de datos informáticos, banco de datos, entre otros ilícitamente obtenidos;

Que, en ese sentido, resulta necesario modificar la Ley N° 30096, Ley de Delitos Informáticos, incorporando el delito de adquisición, posesión y tráfico ilícito de datos informáticos, a fin de fortalecer la seguridad y confianza digital a nivel nacional, comprendiendo la ciberseguridad, y materializar la tutela penal reforzada del derecho fundamental a la autodeterminación informativa, elevando el estándar de protección frente a conductas que generan afectaciones masivas y sistemáticas en el entorno digital;

Que, la comercialización y tráfico ilícito de información digital obtenida sin consentimiento del titular o mediante la vulneración de sistemas de seguridad constituye una conducta de elevada lesividad social, en tanto afecta de manera directa la seguridad de los datos, la autodeterminación informativa y la confianza en los sistemas informáticos, generando un riesgo estructural para la seguridad ciudadana y el adecuado funcionamiento de los servicios públicos y privados en el entorno digital;

Que, de acuerdo a lo dispuesto en el literal j) del numeral 41.1 del artículo 41 del Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, aprobado mediante Decreto Supremo N° 023-2025-PCM, las entidades públicas están exceptuadas de presentar expediente Análisis de Impacto Regulatorio Ex Ante (AIR Ex Ante) a la Comisión Multisectorial de Calidad Regulatoria (CMCR) en el caso de disposiciones normativas en materia penal, o que regulan los procesos en vía judicial (como códigos o leyes procesales), por lo que la presente norma se encuentra excluida del alcance AIR Ex Ante al estar inmersa en el supuesto antes descrito;

De conformidad con lo establecido en el artículo 104 de la Constitución Política del Perú, y en ejercicio de la facultad delegada en el subnumeral 2.1.14 del numeral 2.1 del artículo 2 de la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo a dar cuenta al Congreso de la República:

Ha dado el Decreto Legislativo siguiente:

DECRETO LEGISLATIVO QUE MODIFICA LA LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS, INCORPORANDO EL DELITO DE ADQUISICIÓN, POSESIÓN Y TRÁFICO ILÍCITO DE DATOS INFORMÁTICOS

Artículo 1.- Objeto
El presente Decreto Legislativo tiene por objeto modificar la Ley N° 30096, Ley de Delitos Informáticos,

incorporando un tipo penal autónomo que sancione la posesión, compra, recepción, venta, comercialización, intercambio, facilitamiento o tráfico ilícito de datos informáticos obtenidos sin consentimiento de su titular o mediante la vulneración de sistemas de seguridad o la comisión de un delito informático.

Artículo 2.- Finalidad

La finalidad del presente Decreto Legislativo es fortalecer la seguridad y confianza digital a nivel nacional, incluyendo la ciberseguridad, y materializar la tutela penal reforzada del derecho fundamental a la autodeterminación informativa, elevando el estándar de protección frente a conductas que generan afectaciones masivas y sistemáticas en el entorno digital.

Artículo 3.- Modificación de la Ley Nº 30096, Ley de Delitos Informáticos, incorporando el artículo 12-A

Se modifica la Ley Nº 30096, Ley de Delitos Informáticos, incorporando el artículo 12-A, el cual queda redactado en los siguientes términos:

"Artículo 12-A.- Adquisición, posesión y tráfico ilícito de datos informáticos

El que posee, compre, recibe, comercialice, vende, facilite, intercambie o trafique datos informáticos, credenciales de acceso o bases de datos personales, teniendo conocimiento o debiendo presumir que se obtuvo sin consentimiento de su titular o mediante la vulneración de sistemas de seguridad o la comisión de un delito informático, es reprimido con pena privativa de libertad no menor de cinco (5) ni mayor de ocho (8) años y con ciento ochenta (180) a trescientos sesenta y cinco (365) días-multa.

La pena privativa de libertad es no menor de ocho (8) ni mayor de diez (10) años, e inhabilitación, cuando:

a) El agente actúa como integrante de una organización criminal;

b) Se cause perjuicio patrimonial grave o afectación a una pluralidad de personas; o

c) La base de datos es procesada o custodiada por una entidad pública.

Queda exceptuada de responsabilidad penal la adquisición, posesión, intercambio o tratamiento de datos informáticos cuando estas conductas se realicen con autorización expresa del titular, conforme a la Ley Nº 29733, Ley de Protección de Datos Personales, en cumplimiento de un mandato judicial o administrativo emitido conforme a ley, o en el ejercicio legítimo de derechos fundamentales o de funciones legalmente reconocidas, siempre que no exista finalidad de aprovechamiento ilícito ni de comercialización indebida de la información".

Artículo 4.- Financiamiento

La implementación del presente Decreto Legislativo se financia con cargo al presupuesto de las instituciones públicas involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 5.- Publicación

El presente Decreto Legislativo es publicado en la Plataforma Digital Única del Estado Peruano para la Orientación al Ciudadano (www.gob.pe) y en la sede digital del Ministerio del Interior (www,gob.pe/mininter) y del Ministerio de Justicia y Derechos Humanos (www,gob.pe/minjus), el mismo día de su publicación en el Diario Oficial "El Peruano".

Artículo 6.- Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros, el Ministro del Interior y el Ministro de Justicia y Derechos Humanos.

POR TANTO:

Mando se publique y cumpla, dando cuenta al Congreso de la República.

Dado en la Casa de Gobierno, en Lima, a los veintitrés días del mes de enero del año dos mil veintiséis.

JOSÉ ENRIQUE JERÍ ORÉ
Presidente de la República

ERNESTO JULIO ÁLVAREZ MIRANDA
Presidente del Consejo de Ministros

VICENTE TIBURCIO ORBEZO
Ministro del Interior

WALTER ELEODORO MARTÍNEZ LAURA
Ministro de Justicia y Derechos Humanos

2480387-2

DECRETO LEGISLATIVO Nº 1701

DECRETO LEGISLATIVO QUE MODIFICA EL DECRETO LEGISLATIVO Nº 1059, DECRETO LEGISLATIVO QUE APRUEBA LA LEY GENERAL DE SANIDAD AGRARIA

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

Que, mediante Ley Nº 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional, se delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana y lucha contra la criminalidad organizada, crecimiento económico responsable y fortalecimiento institucional, por el plazo de sesenta días calendario, contados a partir de la entrada en vigor de la citada Ley; y, dentro de los alcances de lo dispuesto en los artículos 101 y 104 de la Constitución Política del Perú y en los artículos 5, 72, 76 y 90 del Reglamento del Congreso de la República;

Que, el subnumeral 2.3.1 del numeral 2.3 del artículo 2 de la citada Ley, establece que el Poder Ejecutivo está facultado para legislar en materia de fortalecimiento institucional, a fin de modificar el Decreto Legislativo 1059, Decreto Legislativo que aprueba la Ley General de Sanidad Agraria, para incorporar disposiciones sanitarias de protección y bienestar de animales domésticos (perros y gatos);

Que, el artículo 4 del Decreto Legislativo Nº 1059, Decreto Legislativo que aprueba la Ley General de Sanidad Agraria, señala que la Autoridad Nacional en Sanidad Agraria es el Servicio Nacional de Sanidad Agraria (SENASA), organismo público adscrito al Ministerio de Desarrollo Agrario y Riego (MIDAGRI), que tiene personería jurídica de Derecho Público y constituye pliego presupuestal;

Que, en el marco de la facultad conferida, resulta necesario incorporar disposiciones sanitarias de protección y bienestar de animales domésticos (perros y gatos) al Decreto Legislativo Nº 1059, Decreto Legislativo que aprueba la Ley General de Sanidad Agraria, a fin de otorgar la función al SENASA para normar e inspeccionar su cumplimiento obligatorio en materia de salud en perros y gatos en situación de abandono, siguiendo las normas, directrices o recomendaciones nacionales y/o internacionales;

Que, el artículo 1 de la Ley Nº 30407, Ley de Protección y Bienestar Animal, señala como principio de protección y bienestar animal que el Estado establece las condiciones necesarias para brindar protección a las especies de animales vertebrados domésticos o silvestres y para reconocerlos como animales sensibles, los cuales merecen gozar de buen trato por parte del ser humano y vivir en armonía con su medio ambiente;