

*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"*

Lima, 9 de febrero de 2026

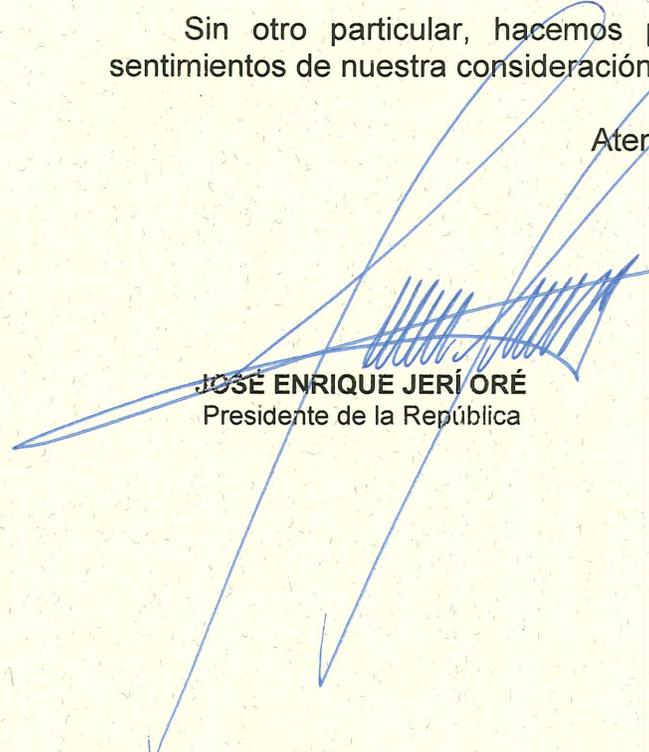
OFICIO N° 062 -2026 -PR

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 104° 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° 1723 , Decreto Legislativo que establece reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones.

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

Atentamente,


JOSÉ ENRIQUE JERI ORÉ
Presidente de la República


ERNESTO JULIO ÁLVAREZ MIRANDA
Presidente del Consejo de Ministros



ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA LAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

Decreto Legislativo ^{Nº 1723}

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

Que, mediante Ley Nº 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materia 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 sub numeral 2.1.17 del numeral 2.1 del artículo 2 de la Ley Nº 32527, establece que el Poder Ejecutivo está facultado para legislar en materias de Seguridad y lucha contra la criminalidad organizada, entre las cuales se considera: "Establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones";

Que, conforme a los numerales 1, 22 y el segundo párrafo del numeral 4 del artículo 2 de la Constitución Política del Perú, toda persona tiene derecho a la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar; así como, a gozar de un ambiente equilibrado y adecuado al desarrollo de su vida, y a que el Estado promueva el uso de las tecnologías de la información y la comunicación en todo el país;

Que, el artículo 44 de la Constitución Política del Perú, establece que son deberes primordiales del Estado, 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;

Que, los artículos 4 y 5 de la Ley Nº 29370, Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones establecen que este Ministerio es competente de manera exclusiva, en materia de infraestructura y servicios de comunicaciones, y tiene, entre otras funciones rectoras, formular, planear, dirigir, coordinar, ejecutar, fiscalizar, supervisar y evaluar la política nacional y sectorial bajo su competencia, aplicable a todos los niveles de gobierno; así como, dictar normas y lineamientos técnicos para la adecuada ejecución, supervisión y evaluación de las políticas, la gestión de los recursos del sector, así como para el otorgamiento y reconocimiento de derechos, la sanción, la fiscalización y ejecución coactiva en materias de su competencia;

Que, la Disposición Preliminar del Texto Único Ordenado de la Ley de Telecomunicaciones aprobado por Decreto Supremo Nº 013-93-TCC, declara de



ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA LA FUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

necesidad pública el desarrollo de las Telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional;

Que, el artículo 2 del Texto Único Ordenado de la Ley de Telecomunicaciones, declara de interés nacional la modernización y desarrollo de las telecomunicaciones, dentro del marco de libre competencia, y establece que su fomento, administración y control corresponde al Estado de acuerdo a dicha Ley. Asimismo, en su artículo 3 establece el derecho que tiene toda persona de usar y prestar servicios de telecomunicaciones en la forma señalada en las disposiciones que regulan la materia;

Que, los numerales 1, 2, 3 y 13 del artículo 75 del Texto Único Ordenado de la Ley de Telecomunicaciones, establecen que son funciones del Ministerio de Transportes y Comunicaciones, fijar la política de telecomunicaciones a seguir y controlar sus resultados; elaborar y proponer la aprobación de los reglamentos y planes de los distintos servicios contemplados en la Ley y expedir resoluciones relativas a los mismos; otorgar y revocar concesiones, autorizaciones, permisos, licencias y controlar su correcta utilización; y, ejercer las facultades inspectoras y sancionadoras previstas en la Ley;

Que, la comisión de actos ilícitos, tales como fraudes, estafas, extorsiones, amenazas o suplantación de identidad, representa un riesgo creciente para la seguridad ciudadana, al afectar directamente la integridad, el patrimonio y la confianza de la población en el uso de los servicios públicos de telecomunicaciones;

Que, asimismo, la Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley N° 29571, Código de Protección y Defensa del Consumidor a fin de ampliar la prohibición de las comunicaciones SPAM, dispone que el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas (spam) que reciben, así como los mecanismos de validación de la información transmitida, mandato que se encuentra únicamente referido a las llamadas spam, cuando la identificación también debe aplicarse a los mensajes de texto, a fin de estar en concordancia con el numeral 58.3 del artículo 58 de la citada Ley N° 29571; por lo que, resulta necesario precisar en ese sentido la Única Disposición Complementaria Final de la Ley N° 32323;

Que, en ese contexto resulta necesario establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto permitiendo identificar su trazabilidad, así como, determinar responsabilidades con el objetivo de combatir su anonimato y evitar las comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana;





ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA VILLAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

Decreto Legislativo



Que, en virtud del numeral 33.2 del artículo 33 del Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, aprobado mediante el Decreto Supremo N° 023-2025-PCM, la presente norma cuenta con dictamen favorable de la Comisión Multisectorial de Calidad Regulatoria que valida el expediente AIR Ex Ante correspondiente;



De conformidad con lo establecido en el artículo 104 de la Constitución Política del Perú; el numeral 1 del artículo 11 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; en ejercicio de la facultad delegada en el sub numeral 2.1.17 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, crecimiento económico responsable y fortalecimiento institucional; la Ley N° 29370, Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones; el Texto Único Ordenado de la Ley de Telecomunicaciones, aprobado mediante Decreto Supremo N° 013-93-TCC; y, el Texto Único Ordenado de su reglamento, aprobado con Decreto Supremo N° 020-2007-MTC;

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:



ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA LAFUENTE FALCÓN
SECRETARIA DEL CONSEJO DE MINISTROS

DECRETO LEGISLATIVO QUE ESTABLECE REGLAS, MEDIDAS Y/O MECANISMOS PARA EL ADECUADO USO DE LA NUMERACIÓN EN LLAMADAS Y MENSAJES DE TEXTO Y SU TRAZABILIDAD, A FIN DE EVITAR EL ANONIMATO Y COMUNICACIONES ILÍCITAS EN PERJUICIO DE LOS USUARIOS DE LOS SERVICIOS PÚBLICOS DE TELECOMUNICACIONES

**CAPÍTULO I
DISPOSICIONES GENERALES**

Artículo 1. Objeto

La presente norma tiene por objeto establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y/o mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana.

Artículo 2. Finalidad

El presente Decreto Legislativo permite la identificación y/o veracidad del número de origen de la comunicación, y evita o mitiga las prácticas de enmascaramiento o manipulación del recurso numérico que conllevan al progreso de llamadas y/o mensajes de texto ilícitos y los efectos negativos que generan en la sociedad.

Artículo 3. Ámbito de aplicación

3.1 La presente norma es aplicable a las empresas operadoras de los servicios públicos de telecomunicaciones y los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto.

3.2 Para efectos del presente Decreto Legislativo, se considera como agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto a toda persona natural o persona jurídica que interviene en el enrutamiento o encaminamiento de las comunicaciones y/o cuenta con información de la trazabilidad de las mismas.

**CAPÍTULO II
OBLIGACIONES DE LAS EMPRESAS OPERADORAS DE SERVICIOS PÚBLICOS DE TELECOMUNICACIONES PARA IDENTIFICAR LA TRAZABILIDAD DE LAS COMUNICACIONES Y EVITAR SU PROGRESO CON FINES ILÍCITOS**





ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA VILLAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

Decreto Legislativo

Artículo 4. Obligaciones de las empresas operadoras de servicios públicos de telecomunicaciones

4.1 Las empresas operadoras adoptan medidas y/o mecanismos técnicos y/u operativos para evitar el progreso de llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos; así como, para permitir a los abonados y usuarios advertir sobre dichas comunicaciones.

4.2 Las empresas operadoras implementan medidas tecnológicas para impedir que se concreten comunicaciones con fines ilícitos

Las empresas operadoras pueden implementar medidas adicionales a lo dispuesto en el párrafo anterior, sin contravenir lo dispuesto en el presente marco normativo.

4.3 Las empresas operadoras adoptan medidas que coadyuvan a determinar el origen de las llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos.

4.4 Las medidas, mecanismos y/o disposiciones mencionadas en los numerales 4.1, 4.2 y 4.3 de la presente norma, son desarrolladas y determinadas en el Reglamento de la misma.

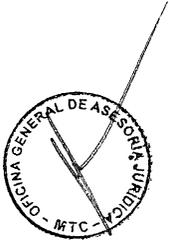
Artículo 5. Gestión y administración de las redes de las empresas operadoras

Las empresas operadoras proporcionan y otorgan las facilidades al Ministerio de Transportes y Comunicaciones, para el acceso y monitoreo constante de sus redes, para verificar el cumplimiento de las obligaciones establecidas en el artículo 4, según corresponda, para la correcta prestación de los servicios públicos de telecomunicaciones, con la finalidad de salvaguardar la seguridad ciudadana en los mismos, en beneficio y protección de los usuarios, resguardando la inviolabilidad y el secreto de las telecomunicaciones.

CAPÍTULO III OBLIGACIONES DE LOS AGENTES VINCULADOS EN LA TRAZABILIDAD DE LAS LLAMADAS Y/O MENSAJES DE TEXTO

Artículo 6. Obligaciones de los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto

6.1 Los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto coadyuvan y/o participan en la identificación y trazabilidad de las referidas



ES COPIA FIE DEL ORIGINAL
MAGALY VIRGINIA VILLAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

comunicaciones para evitar su progreso con fines ilícitos, para la correcta prestación de los servicios públicos de telecomunicaciones y/o en aras de salvaguardar la seguridad ciudadana en los mismos, en beneficio y protección de los usuarios Para tal efecto, cumplen las disposiciones establecidas en el Reglamento de la presente norma.



6.2 El Ministerio de Transportes y Comunicaciones está facultado para establecer, a través del Reglamento del presente Decreto Legislativo, las condiciones y/o requisitos aplicables a los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto, así como, para establecer las obligaciones aplicables a estos.

Artículo 7. Gestión y administración de los sistemas de los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto

Los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto otorgan las facilidades al Ministerio de Transportes y Comunicaciones, para el acceso y monitoreo constante de sus sistemas de gestión, para verificar el cumplimiento de las obligaciones establecidas en el artículo 6, según corresponda, resguardando la inviolabilidad y el secreto de las telecomunicaciones.

CAPÍTULO IV POTESTAD FISCALIZADORA Y SANCIONADORA

Artículo 8. Potestad fiscalizadora, sancionadora y de imposición de medidas correctivas y cautelares del Ministerio de Transportes y Comunicaciones

8.1 El Ministerio de Transportes y Comunicaciones, de acuerdo a sus competencias y normas reglamentarias, tiene potestad para fiscalizar y sancionar a las empresas operadoras y a los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto por el incumplimiento de las obligaciones derivadas del presente Decreto Legislativo. El tipo de sanción a imponer es amonestación escrita o multa.

8.2 Las infracciones por el incumplimiento de las obligaciones derivadas del presente Decreto Legislativo se clasifican en leves, graves y muy graves, y se tipifican en su Reglamento.

8.3 Las infracciones son sancionadas, de acuerdo a las escalas de multas establecidas en la Ley N° 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL o norma que sustituya dicha escala de multas. En el caso de infracciones leves, el Ministerio de Transportes y Comunicaciones puede aplicar la sanción de amonestación escrita o multa, y para las infracciones graves y muy graves aplica la sanción de multa.

8.4 El Ministerio de Transportes y Comunicaciones puede aplicar medidas preventivas, cautelares y/o medidas correctivas, según correspondan.





ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA ZAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

Decreto Legislativo



8.5 En el ejercicio de la actividad de fiscalización, el Ministerio de Transportes y Comunicaciones se encuentra facultado para monitorear de manera constante las redes de las empresas operadoras y los sistemas de gestión de los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto, para verificar el cumplimiento de las obligaciones establecidas en los artículos 4, 5, 6 y 7, según corresponda, para la correcta prestación de los servicios públicos de telecomunicaciones, salvaguardar la seguridad ciudadana en los mismos y/o en otras situaciones análogas, en beneficio y protección de los usuarios, resguardando la inviolabilidad y el secreto de las telecomunicaciones e información protegida por ley.

Artículo 9. Financiamiento

La implementación del presente Decreto Legislativo se financia con el presupuesto institucional del Ministerio de Transportes y Comunicaciones sin demandar recursos adicionales al Tesoro Público, conforme a lo establecido en las leyes anuales de presupuesto del sector público.

Artículo 10. Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros y el Ministro de Transportes y Comunicaciones.

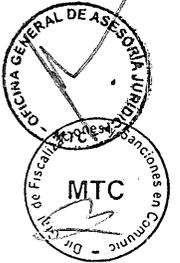
DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Vigencia

El presente Decreto Legislativo entra en vigencia a partir del día siguiente de la publicación del Reglamento de la presente norma en el diario oficial El Peruano.

SEGUNDA. Reglamentación

El Ministerio de Transportes y Comunicaciones en un plazo no mayor a noventa (90) días calendario contado desde la publicación de la presente norma, mediante Decreto Supremo, aprueba el Reglamento correspondiente.



ES COPIA FIEL DEL ORIGINAL

MAGALY VIRGINIA WILLAFUERTE FALCON
SECRETARIA DEL CONSEJO DE MINISTROS

DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA

ÚNICA. Modificación de Disposiciones Complementarias Finales de la Ley N° 32323, Ley que modifica la Ley N° 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM

Se modifica la Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley N° 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM, en los siguientes términos:

“ÚNICA. Normativa adicional

Para la aplicación del numeral 58.3 del artículo 58 de la Ley N° 29571, Código de Protección y Defensa del Consumidor, incorporado por la presente ley, el Poder Ejecutivo establece la normativa adicional que otorgue la numeración telefónica especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas y mensajes de texto (spam) que reciben, así como los mecanismos de validación de la información transmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de la presente ley.

Para el cumplimiento de la mencionada normativa adicional, el Ministerio de Transportes y Comunicaciones y el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI ejercen la facultad fiscalizadora y sancionadora, en el ámbito de sus funciones y competencias”.

POR TANTO:

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

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

.....
JOSÉ ENRIQUE JERÍ ORÉ
Presidente de la República

.....
ERNESTO JULIO ÁLVAREZ MIRANDA
Presidente del Consejo de Ministros

.....
ALDO MARTÍN PRIETO BARRERA
Ministro de Transportes y Comunicaciones





Firmado digitalmente por:
RIOS AQUINO Jaime Erick
FAU 20131379944 hard
Motivo: Doy V° B°
Fecha: 02/02/2026 19:15:30-0500



Firmado digitalmente por:
DÍAZ UBILLÚS Patricia
Verónica FAU 20131379944 soft
Motivo: En señal de
conformidad
Fecha: 02/02/2026 20:00:34-0500

EXPOSICIÓN DE MOTIVOS

DECRETO LEGISLATIVO QUE ESTABLECE REGLAS, MEDIDAS Y/O MECANISMOS PARA EL ADECUADO USO DE LA NUMERACIÓN EN LLAMADAS Y MENSAJES DE TEXTO Y SU TRAZABILIDAD, A FIN DE EVITAR EL ANONIMATO Y COMUNICACIONES ILÍCITAS EN PERJUICIO DE LOS USUARIOS DE LOS SERVICIOS PÚBLICOS DE TELECOMUNICACIONES

I. Objeto

El presente decreto legislativo tiene por objeto establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana.

II. Finalidad

Las medidas aprobadas por el presente decreto legislativo tienen por finalidad permitir la identificación y/o veracidad del número de origen de la comunicación, así como, evitar o mitigar prácticas de enmascaramiento o manipulación del recurso numérico que conlleva al progreso de llamadas y mensajes de texto ilícitos y los efectos negativos que generan en la sociedad.

III. Antecedentes

Conforme a los numerales 1, 22 y el segundo párrafo del numeral 4 del artículo 2 de la Constitución Política del Perú, toda persona tiene derecho, a la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar; así como, a gozar de un ambiente equilibrado y adecuado al desarrollo de su vida, y a que el Estado promueva el uso de las tecnologías de la información y la comunicación en todo el país.

El artículo 44 de la Constitución Política del Perú establece que son deberes primordiales del Estado, 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.

Ahora bien, los artículos 4, 5 y 6 de la Ley N° 29370, Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones (en adelante, LOF del MTC) establecen que este Ministerio es competente de manera exclusiva en materia de infraestructura y servicios de comunicaciones, disponiendo las funciones rectoras y específicas de competencias exclusivas correspondientes.

Asimismo, la Disposición Preliminar del Texto Único Ordenado de la Ley de Telecomunicaciones aprobado por Decreto Supremo N° 013-93-TCC (en adelante, el TUO de la Ley de Telecomunicaciones), declara de necesidad pública el desarrollo de las Telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional.

Por su parte, el artículo 2 del TUO de la Ley de Telecomunicaciones, declara de interés nacional la modernización y desarrollo de las telecomunicaciones, dentro del marco de libre competencia, y establece que su fomento, administración y



Firmado digitalmente por:
ANGULO REYES Mario
Nolberto FAU 20131379944 hard
Motivo: En señal de
conformidad
Fecha: 02/02/2026 20:06:44-0500



Firmado digitalmente por:
AREQUIPEÑO TAMARA Luis 1
Alberto FAU 20376082114 soft
Motivo: En señal de
conformidad
Fecha: 02/02/2026 20:18:24-0500

control corresponde al Estado de acuerdo a dicha Ley. Asimismo, en su artículo 3 establece el derecho que tiene toda persona de usar y prestar servicios de telecomunicaciones en la forma señalada en las disposiciones que regulan la materia.

Los numerales 1, 2 y 3 del artículo 75 del TUO de la Ley de Telecomunicaciones, establecen además de las atribuciones señaladas en la LOF del MTC, son funciones del Ministerio de Transportes y Comunicaciones (MTC), fijar la política de telecomunicaciones a seguir y controlar sus resultados; elaborar y proponer la aprobación de los reglamentos y planes de los distintos servicios contemplados en la Ley y expedir resoluciones relativas a los mismos; otorgar y revocar concesiones, autorizaciones, permisos, licencias y controlar su correcta utilización; entre otras.

Mediante la Resolución Suprema N° 022-2002-MTC, se aprobó el Plan Técnico Fundamental de Numeración (en adelante, PTFN), documento que contiene los planes técnicos fundamentales, que establecen las pautas y lineamientos técnicos y básicos que aseguran la integración e implementación de los servicios de telecomunicaciones en el territorio nacional.

De acuerdo con la parte introductoria del PTFN, la numeración en los servicios públicos de telecomunicaciones es un recurso escaso que debe ser usado eficientemente, por lo cual dicho plan establece los criterios para el adecuado uso de los números asignados en la red pública nacional de telecomunicaciones. Asimismo, como la numeración está asociada directamente con los procesos demarcación y encaminamiento, el PTFN proporciona las pautas correspondientes para el desarrollo de estos procesos. Además, la adecuada administración y oportuna supervisión del cumplimiento del PTFN, deben asegurar una regular e imparcial asignación de los recursos numéricos para el beneficio mutuo de los usuarios y operadores de los servicios públicos.

En el numeral 1. Objetivos del PTFN se menciona que la referida norma técnica tiene como uno de sus objetivos, establecer las bases para una adecuada administración, supervisión y uso de la numeración, a través de una eficiente asignación, así como definir las estructuras de numeración para la prestación de los servicios públicos de telecomunicaciones. Adicionalmente, cabe destacar que constituye uno de los objetivos del PTFN, facilitar al abonado, en lo posible, el reconocimiento de los diferentes servicios y sus proveedores.

Por su parte, el artículo 106 del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado mediante Decreto Supremo N° 020-2007-MTC (en adelante, TUO del Reglamento de la Ley de Telecomunicaciones), establece que los contratos de interconexión deben sujetarse, entre otros, a lo establecido por los planes técnicos fundamentales contenidos en el Plan Nacional de Telecomunicaciones, así como a las disposiciones que dicte el Organismo Supervisor de la Inversión en Telecomunicaciones (OSIPTEL). Asimismo, dicho artículo establece que, los contratos de interconexión deberán contemplar, entre otros aspectos, las características de las señales transmitidas o recibidas incluyendo arreglos de encaminamiento, transmisión, sincronización, señalización, **numeración**, tarifas y calidad de servicio y seguridad de telecomunicaciones.

Asimismo, los numerales 5 y 6 del artículo 258 del TUO del Reglamento de la Ley de Telecomunicaciones, establecen que constituye infracciones muy graves la utilización de numeración sin la debida asignación por parte del órgano

competente del MTC o de una distinta a la asignada, así como, la utilización de señalización o numeración en condiciones distintas a las contempladas en el respectivo plan técnico, respectivamente.

De otro lado, mediante la Ley N° 32323 se modificó la Ley N° 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM, estableciendo que, para garantizar la protección del consumidor contra los métodos comerciales agresivos o engañosos, el Estado establece las reglas para el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones. Asimismo, la única disposición complementaria final establece que la aplicación del numeral 58.3 del artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor, incorporado por dicha ley, el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración telefónica especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas (spam) que reciben, así como los mecanismos de validación de la información transmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de la presente ley.

De acuerdo a ello, el legislador ha señalado en el Dictamen recaído en el proyecto de Ley N° 13280/2025-PE, Proyecto de 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 institucional¹ que, a fin de ampliar la prohibición de las comunicaciones SPAM, que en el numeral 58.3 garantiza al consumidor el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones, y de conformidad a su única disposición complementaria final se otorgue numeración especial a los proveedores, los métodos de seguridad y técnicas de validación para que los usuarios puedan identificar las llamadas que reciben, así como los mecanismos de validación de información transmitida, que si bien está referido a las llamadas spam, la identificación de debería aplicarse para toda llamada o mensaje de texto.

Asimismo, la Dirección General de Fiscalizaciones y Sanciones en Comunicaciones del MTC, en el marco de sus funciones, ha realizado distintas acciones de fiscalización a diversas empresas operadoras, con la finalidad de verificar el cumplimiento de las obligaciones establecidas en el marco legal y reglamentario, así como las condiciones técnicas y operativas correspondientes, relacionadas a la trazabilidad de las comunicaciones cursadas entre dichas empresas.

IV. Marco jurídico y las habilitaciones en cuyo ejercicio se dicta

Conforme el artículo 104 de la Constitución Política del Perú el Congreso puede delegar en el Poder Ejecutivo la facultad de legislar, mediante decretos legislativos, sobre la materia específica y por el plazo determinado establecidos en la ley autoritativa.

En esa línea, el 15 de diciembre de 2025 se publicó 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", mediante la cual el Congreso de la República ha delegó en el Poder Ejecutivo la facultad de legislar sobre las citadas

¹ Dictamen que sirvió de sustento para la aprobación 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".

materias por el plazo de 60 días calendario contados a partir de la entrada en vigencia de la citada ley.

En específico, el numeral 2.1.17 del artículo 2 de la Ley N° 32527, dispone que el Poder Ejecutivo está facultado para legislar en materia de seguridad y lucha contra la criminalidad organizada, a fin de dictar medidas para:

- Establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones.

Cabe indicar que, según lo establece la Primera Disposición Complementaria Final de la citada Ley N° 32527, las medidas que se emitan en el marco de lo dispuesto en la presente ley no afectan la autonomía y competencias del Poder Legislativo, de los gobiernos regionales y locales ni de los organismos constitucionales autónomos que reconoce la Constitución Política del Perú. Tampoco vulneran derechos fundamentales ni inciden sobre procesos judiciales en trámite. La inobservancia de lo dispuesto en la presente disposición genera responsabilidad política o funcional, según corresponda.

De acuerdo a ello, el Poder Ejecutivo se encuentra facultado a emitir el presente Decreto Legislativo en el marco de la delegación de facultades dispuesta por la Ley N° 32527, dado que las medidas que se establecen tiene por finalidad la identificación y/o veracidad del número de origen de la comunicación, así como, evitar o mitigar prácticas de enmascaramiento o manipulación del recurso numérico que conlleva al progreso de llamadas y mensajes de texto ilícitos y los efectos negativos que generan en la sociedad.

Por tanto, considerando el marco jurídico habilitante, a continuación, se sustenta el presente Decreto Legislativo, el cual, establece reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones.

V. Fundamento Técnico de la Propuesta Normativa

5.1. Identificación del problema público

5.1.1. Contexto general y panorama internacional

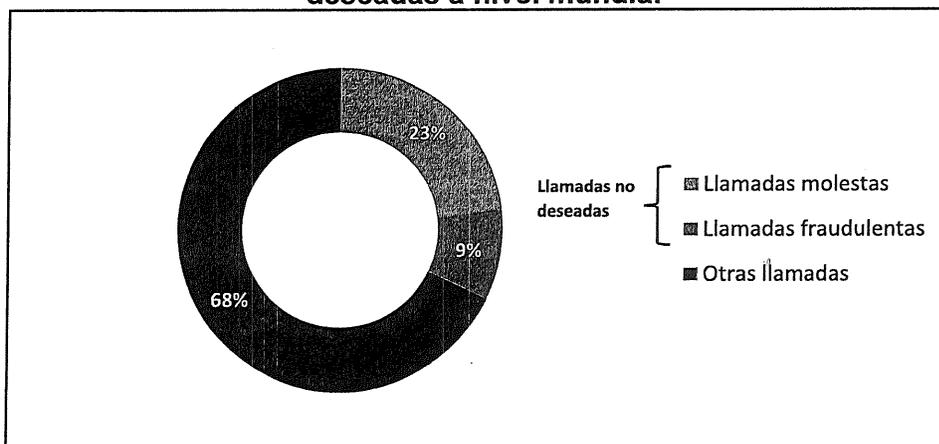
A nivel internacional, de acuerdo al Global Call Threat Report² (Hiya, 2025), durante el segundo trimestre del 2025, se observaron 13.7 mil millones de llamadas spam³ y 2.3 mil millones de llamadas fraudulentas a nivel global, lo que significa que se generaron más de 150 millones de llamadas no deseadas cada día. Estas cifras evidencian que se trata de un problema de alcance global.

Asimismo, conforme al reporte de Hiya, el 23% de las llamadas entrantes a nivel mundial fueron etiquetadas como llamadas molestas y el 9% como llamadas fraudulentas, ello significa que aproximadamente un 32% de las llamadas a nivel mundial, son llamadas no deseadas.

² Hiya. (2025). Global Call Threat Report Q2 2025. <https://es.hiya.com/global-call-threat-report>

³ De acuerdo a la metodología del reporte, spam se define como llamadas no deseadas e incluye tanto llamadas fraudulentas como llamadas molestas.

Gráfico 1. Participación del volumen de llamadas entrantes no deseadas a nivel mundial



Fuente: Hiya. (2025). Global Call Threat Report Q2 2025.
Elaboración: DGPRC-MTC

Este asunto de las llamadas no deseadas, entre llamadas molestosas y llamadas por fraude, se ha convertido en un problema global, debido a que a nivel internacional se tiene que, para el segundo trimestre de 2025, por ejemplo, en países como Estados Unidos, aproximadamente 4 de cada 10 llamadas no se encuentran en la libreta de contactos de un usuario, donde el 40% son llamadas molestosas y el 1% son llamadas por fraude; mientras que, en Canadá, la situación es algo distinta, pues el 19% de las llamadas son llamadas molestosas y el 8% son llamadas por fraude.

Por otra parte, en Estados Unidos, durante el primer trimestre de 2025⁴, las llamadas fraudulentas se concentraron principalmente en estafas relacionadas con Medicare. En estos casos, más que sustraer dinero de forma directa, los estafadores buscan obtener el número de Medicare de las personas para facturar fraudulentamente al gobierno estadounidense por supuestos servicios de salud. Asimismo, en ese mismo período, se registraron estafas vinculadas a seguros médicos, en las que los usuarios reportaron llamadas no solicitadas que ofrecían supuestas opciones de atención médica a bajo costo.

Durante el segundo trimestre de 2025⁵, las estafas más comúnmente reportadas continuaron siendo las relacionadas con Medicare, mediante las cuales los estafadores inducen a los ciudadanos a revelar su número de afiliación y otra información personal sensible, utilizada posteriormente para facturar de manera fraudulenta por supuestos servicios de salud. Adicionalmente, en este período se observó un incremento de las estafas fiscales, lo que evidencia una diversificación de las modalidades de fraude telefónico.

De otro lado, en Canadá (Hiya, 2025), durante el primer trimestre de 2025, las estafas asociadas a Amazon constituyeron el tipo de llamada fraudulenta más frecuente. No obstante, en el segundo trimestre del mismo año, las estafas bancarias y vinculadas a tarjetas de crédito pasaron a ocupar el primer lugar, mientras que las estafas de Amazon descendieron al segundo puesto.

De acuerdo a Hiya, para el segundo trimestre 2025, las tasas más altas de llamadas no deseadas en Europa las lideraron Francia y España, con tasas de

⁴ Hiya. (2025). Global Call Threat Report Q1 2025.

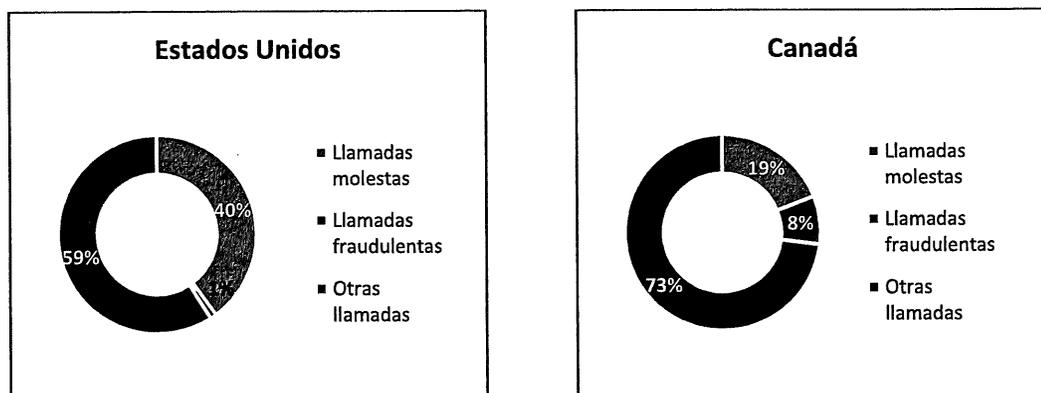
⁵ Hiya. (2025). Global Call Threat Report Q1 2025.

spam del 62% (58% de llamadas molestosas y 4% de llamadas por fraude) y 51% (34% de llamadas molestosas y 17% de llamadas por fraude), respectivamente.

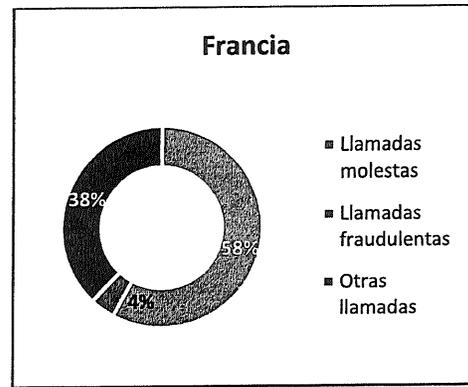
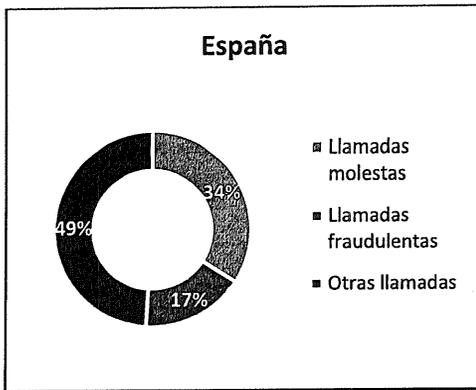
En España, más de la mitad de las llamadas provenientes de números no registrados en la libreta de contactos corresponden a llamadas no deseadas. Los usuarios no solo enfrentan un elevado volumen de este tipo de comunicaciones, sino también una alta incidencia de llamadas fraudulentas, cuya tasa es aproximadamente cuatro veces superior a la registrada en Francia. Durante el segundo trimestre de 2025, las estafas telefónicas más frecuentes en España fueron aquellas en las que los delincuentes se hacían pasar por compañías del sector energético. Asimismo, se registró una alta incidencia de estafas laborales y de empleo, en las que se suplantó a plataformas de búsqueda de trabajo como Indeed e InfoJobs, ofreciendo falsas oportunidades laborales con el objetivo de obtener información personal. De igual manera, persistieron las llamadas fraudulentas en las que se hacía pasar por entidades bancarias.

Por otro lado, Francia es el país europeo que recibe el mayor volumen de llamadas no deseadas, sin embargo, presenta una menor proporción de llamadas fraudulentas en comparación con España. Durante el mismo período, las estafas más reportadas estuvieron relacionadas con supuestos servicios de electricidad y energía, así como con fraudes bancarios. Adicionalmente, en el cuarto trimestre de 2023 se identificó en Francia la aparición de una nueva modalidad de estafa denominada "Hello mom", en la que el estafador se hace pasar por un hijo o familiar cercano mediante un mensaje SMS, indicando que su teléfono está dañado y solicitando continuar la comunicación por WhatsApp, seguido de una petición urgente de dinero (Hiya, 2023)⁶.

Gráfico 2. Porcentaje del volumen de llamadas entrantes no deseadas respecto del total de llamadas de no contactos II Trimestre 2025



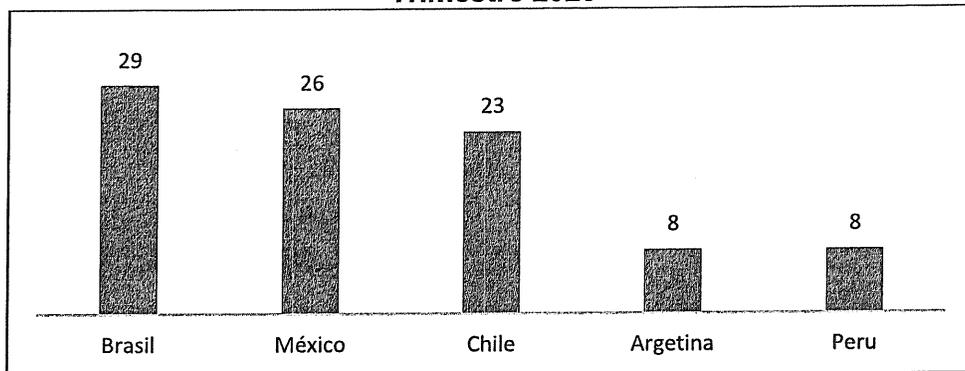
⁶ Hiya. (2025). Global Call Threat Report Q4 2023.



Fuente: Hiya. (2025). Global Call Threat Report Q2 2025.
Elaboración: DGPRC-MTC.

Para el caso latinoamericano, de acuerdo a Hiya, durante el segundo trimestre de 2025, Brasil se ubicó como el país con la mayor cantidad de llamadas no deseadas por persona no solo en Latinoamérica, sino en los países incluidos en el reporte, mientras que, Perú se ubicó como el quinto país latinoamericano con la mayor cantidad en promedio de llamadas no deseadas por persona.

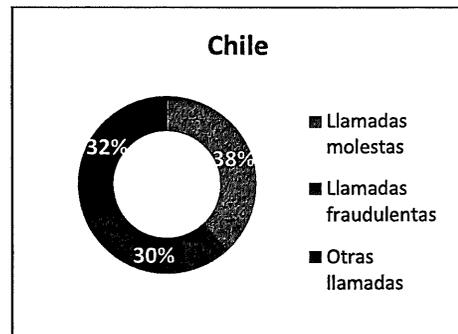
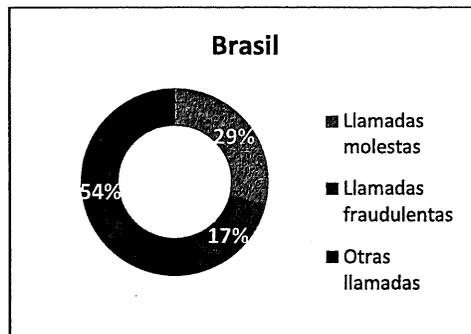
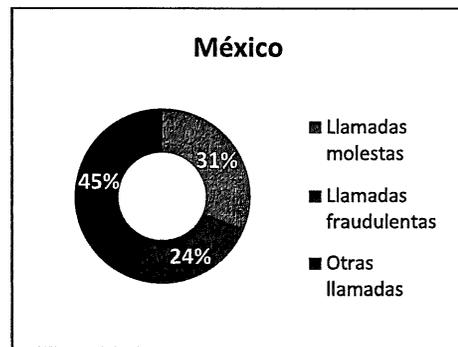
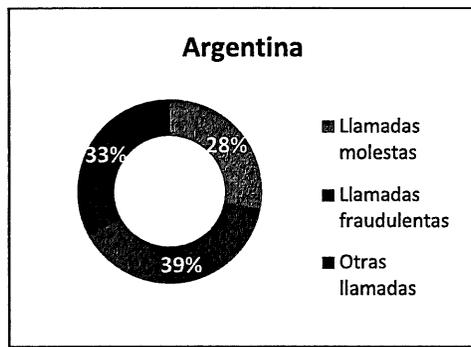
Gráfico 3. Llamadas spam por persona en países de América Latina, II Trimestre 2025



Fuente: Hiya. (2025). Global Call Threat Report Q2 2025.
Elaboración: DGPRC-MTC.

En esa línea, de acuerdo con el reporte de Hiya, si bien Brasil concentra el mayor volumen absoluto de llamadas no deseadas, al analizar la proporción de llamadas provenientes de números que no figuran en la libreta de contactos del usuario, se observa que Argentina presenta la mayor tasa de llamadas con fines fraudulentos. En particular, aproximadamente el 39% de las llamadas no deseadas provenientes de números desconocidos correspondieron a intentos de fraude. Le siguen Chile, con una tasa del 30%, México con el 24% y Brasil con el 17%, lo que evidencia diferencias significativas en la incidencia del fraude telefónico entre los países de la región.

Gráfico 4. Porcentaje de llamadas por fraude en países de América Latina, II Trimestre 2025



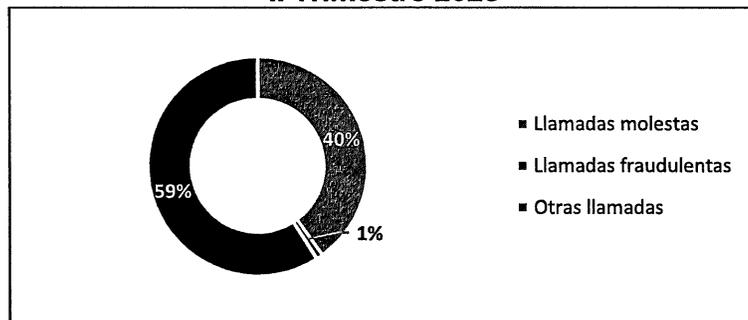
Fuente: Hiya. (2025). Global Call Threat Report Q2 2025.
Elaboración: DGPRC-MTC.

Para complementar el diagnóstico anterior se desarrolla con mayor detalle los siguientes países:

Estados Unidos

Como se indicó previamente, de acuerdo al Global Call Threat Report, elaborado por Hiya para el segundo trimestre de 2025, Estados Unidos presentó una tasa del 40% del total de llamadas entrantes que no están en los contactos, como llamadas molestas y un 1% como llamadas por fraude. No obstante, se debe señalar que, las llamadas fraudulentas se mantienen bajo control porque la mayoría de los operadores estadounidenses las bloquean a nivel de red para que nunca lleguen al teléfono del destinatario.

Gráfico 5. Porcentaje de llamadas entrantes no deseadas II Trimestre 2025



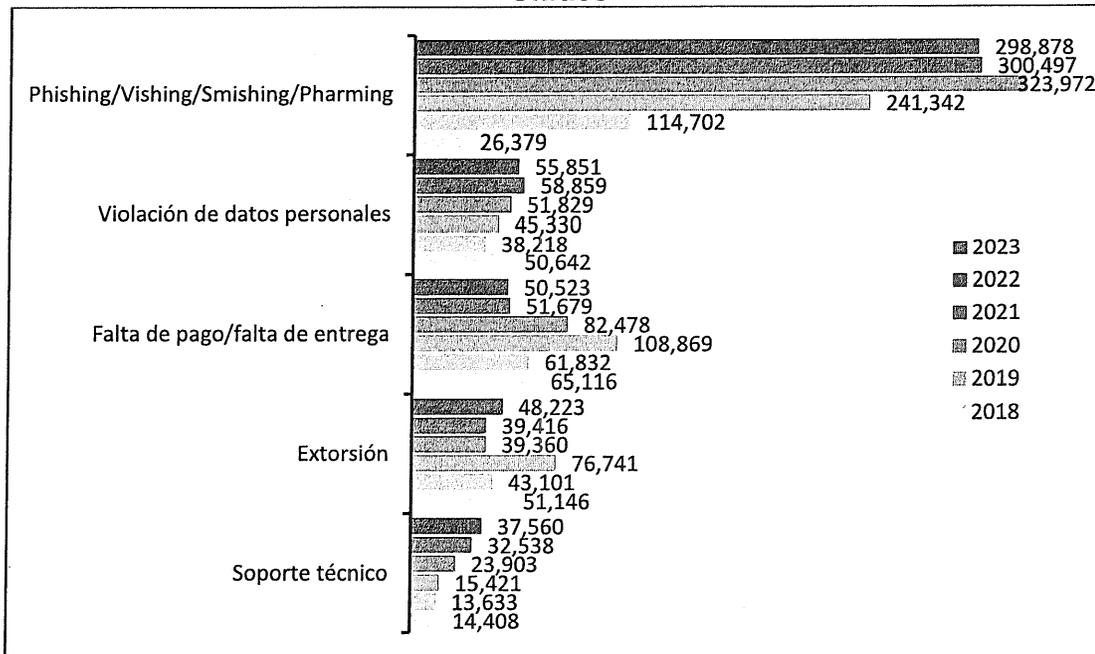
Fuente: Hiya. (2025). Global Call Threat Report Q2 2025.

Elaboración: DGPRC-MTC.

Esta fuerte presencia de llamadas y mensajes fraudulentos se puede evidenciar a su vez en las denuncias existentes por este tipo de delito.

De acuerdo al documento Internet Crime Report 2023 del Federal Bureau of Investigation (FBI)⁷, el principal crimen digital está relacionado a actividades de ingeniería social, tales como el *phishing*, *vishing* y *smishing*, las cuales han presentado un mayor crecimiento en los últimos cinco años, donde se registró para el 2023, un incremento en las denuncias por *phishing/vishing/smishing/pharming* de más de 1,000% respecto del 2018⁸.

Gráfico 6. Crecimiento de los cinco principales delitos digitales en Estados Unidos



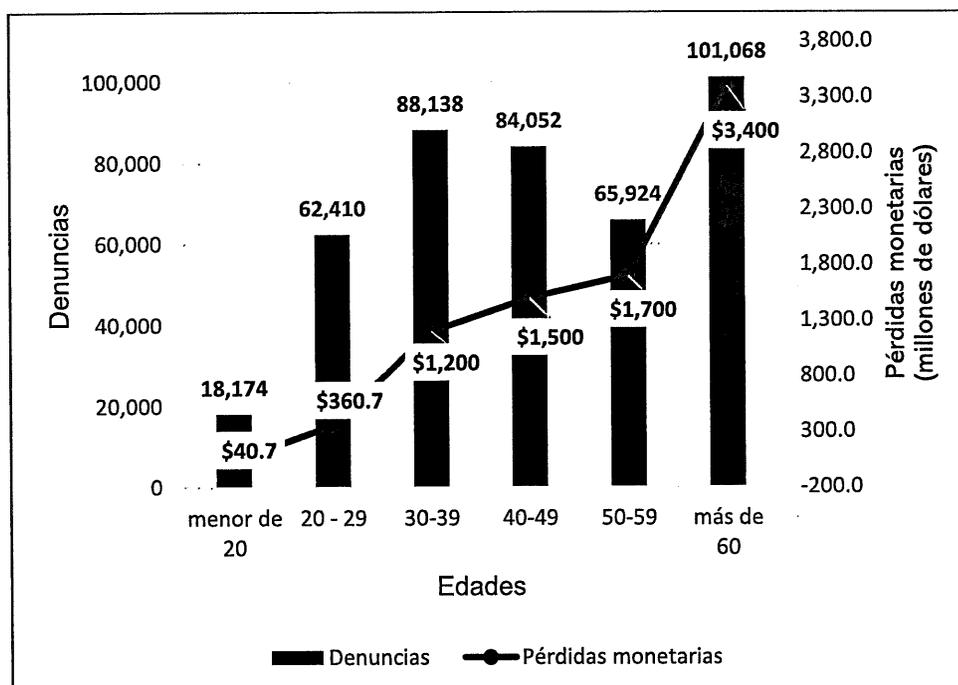
Fuente: Internet Crime Report 2023. Internet Crime Report 2021.
Elaboración: DGPRC-MTC.

Asimismo, el documento indica que el grupo de personas que presentó la mayor cantidad de víctimas de delitos digitales fueron las personas mayores de 60 años, quienes a su vez tuvieron las mayores pérdidas por estos delitos.

Gráfico 7. Víctimas de delitos digitales según grupos de edad en Estados Unidos, 2023

⁷ Federal Bureau of Investigation. (2024). Internet Crime Report 2023. Recuperado de https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

⁸ Federal Bureau of Investigation. (2022). Internet Crime Report 2021. Recuperado de https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf



Fuente: Internet Crime Report 2023.
Elaboración: DGPRC-MTC.

Además, indican que los *call centers* ilegales defraudan miles de personas cada año, suplantando la identidad a través de servicios de apoyo técnico al cliente, así como, de trabajadores del gobierno. Estos se dirigen principalmente a las personas mayores, con efectos devastadores. Casi la mitad de las víctimas dicen tener más de 60 años (40%) y experimentan el 58% de las pérdidas (más de 770 millones de dólares).

Respecto a las pérdidas monetarias de las víctimas por *phishing/vishing/smishing/pharming/spoofing* durante el 2023, estas ascendieron a más de 18.7 millones de dólares.

Siguiendo esa línea de análisis, conforme al reporte de Robokiller⁹ para Estados Unidos, se tiene registrado que para el 2022, los estafadores enviaron 225,700 millones de mensajes de texto no deseados, presentando un incremento del 157% respecto a la cantidad de mensajes de texto no deseados enviados en el 2021. Ello a su vez generó pérdidas estimadas de 20,600 millones de dólares, presentando un incremento del 105% respecto de las pérdidas estimadas en el 2021. De otro lado, durante el primer semestre de 2023, se estiman pérdidas monetarias por mensajes de texto de aproximadamente 13 mil millones de dólares¹⁰.

Por lo tanto, se evidencia que, incluso en un país desarrollado como Estados Unidos, este tipo de fraude tecnológico ha comprometido significativamente la seguridad de la información de los ciudadanos, generando grandes pérdidas económicas. Este contexto resalta la urgencia y necesidad de implementar acciones robustas para proteger a la población y restablecer la confianza en los sistemas de comunicación, un desafío que no es exclusivo de un solo país, sino que es una preocupación global que requiere atención inmediata.

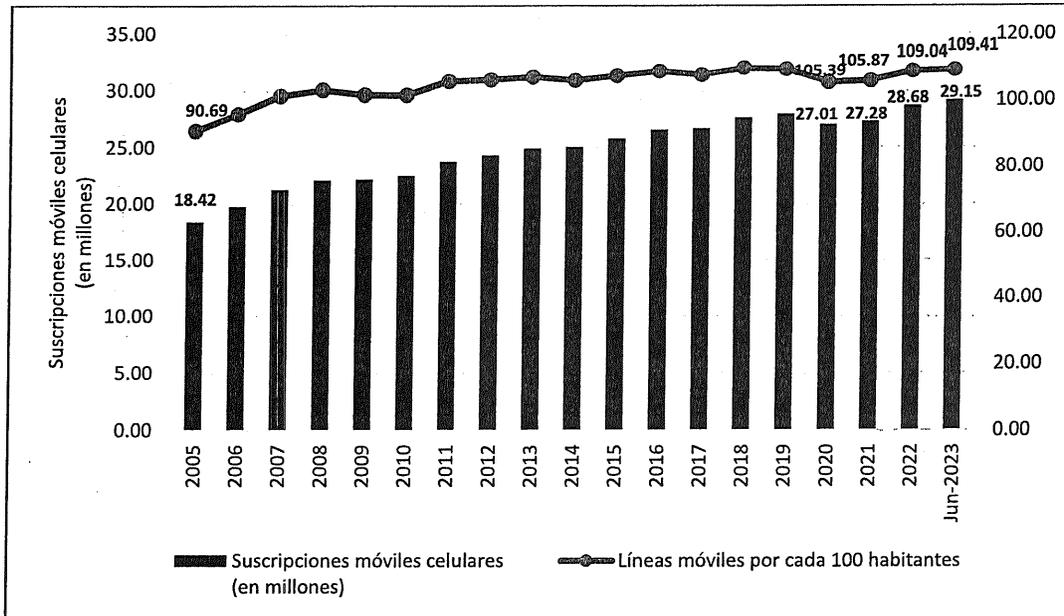
⁹ Robokiller. (2022). The Robokiller phone scam report | 2022 insights & analysis. Recuperado de <https://www.robokiller.com/robokiller-2022-phone-scam-report>

¹⁰ Robokiller (2023). The Robokiller Phone Scam Report | 2023 mid-year Insights & Analysis. Recuperado de <https://www.robokiller.com/robokiller-2023-mid-year-phone-scam-report>

Australia

Por su parte, Australia que ha presentado un crecimiento constante en el número de líneas móviles celulares en los últimos 18 años, durante el periodo del 2020 al 2022 ha presentado un crecimiento aproximado del 6% en el número de líneas móviles, similar al crecimiento presentado por el Perú en dicho periodo. Al primer semestre de 2023, la cantidad de líneas móviles celulares asciende a 29.15 millones, indicando un nivel de penetración de 109.41 líneas móviles por cada 100 habitantes. Al igual que Perú, Australia evidencia la existencia de más líneas móviles por habitantes.

Gráfico 8. Suscripciones móviles celulares (en millones) y Penetración a nivel nacional



Fuente:

Mobile-cellular subscriptions. DataHub. ITU.

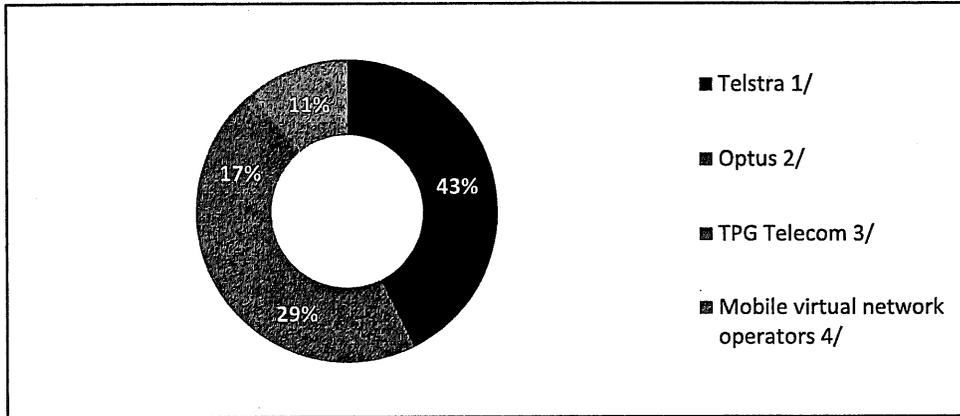
Internet activity report For the period ending 30 June 2023. ACCC.

National, state and territory population. June 2023. Australian Bureau of Statistics.

Elaboración: DGPRC-MTC.

En ese contexto, también se tiene que el mercado móvil australiano presenta características similares al peruano, puesto que, además, son tres los operadores que comprenden una participación de más del 80% del mercado móvil. Para el caso australiano, los tres principales operadores concentran el 89% del total de líneas móviles en servicio, siendo el operador Telstra quien tiene una participación del 43% de líneas móviles en operación.

**Gráfico 9. Participación del mercado móvil australiano (% líneas móviles en operación)
A junio de 2023**



Notas:

1/ Incluye marcas propias y secundarias de Telstra.

2/ Incluye marcas propias y secundarias de Optus.

3/ Incluye marcas propias y submarcas de TPG Telecom.

4/ Es la suma de los servicios mayoristas prepago y pospago.

Fuente: Internet activity report For the period ending 30 June 2023. ACCC.

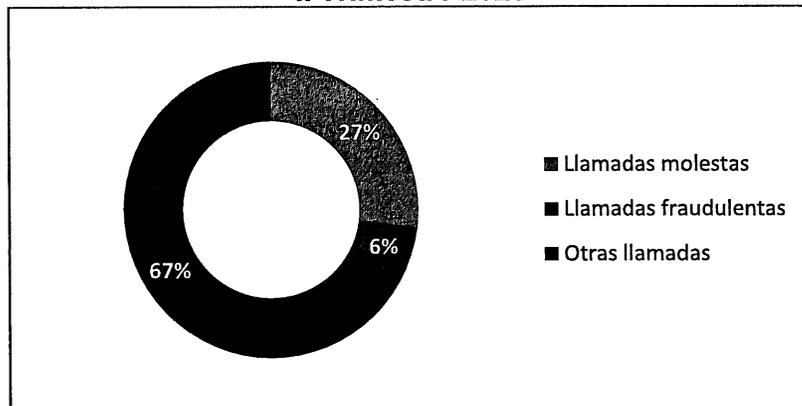
Disponible en: <https://www.accc.gov.au/by-industry/telecommunications-and-internet/telecommunications-industry-record-keeping-and-reporting-rules/internet-activity-record-keeping-rule/june-2023-report>

Elaboración: DGPRC-MTC.

Conforme se extiende el uso de los teléfonos móviles y la tecnología, Australia ha presentado problemas por fraude informático, ya sea a través de las llamadas o mensajes de texto fraudulentos.

De acuerdo al Global Call Threat Report, elaborado por Hiya, para el segundo trimestre de 2025, alrededor de 6 de cada 10 llamadas no identificadas son llamadas por fraude.

**Gráfico 10. Porcentaje de llamadas por fraude del total de llamadas de llamadas no deseadas de números que no son contactos
II Trimestre 2025**



Fuente: Hiya. (2025). Global Call Threat Report Q2 2025.

Elaboración: DGPRC-MTC.

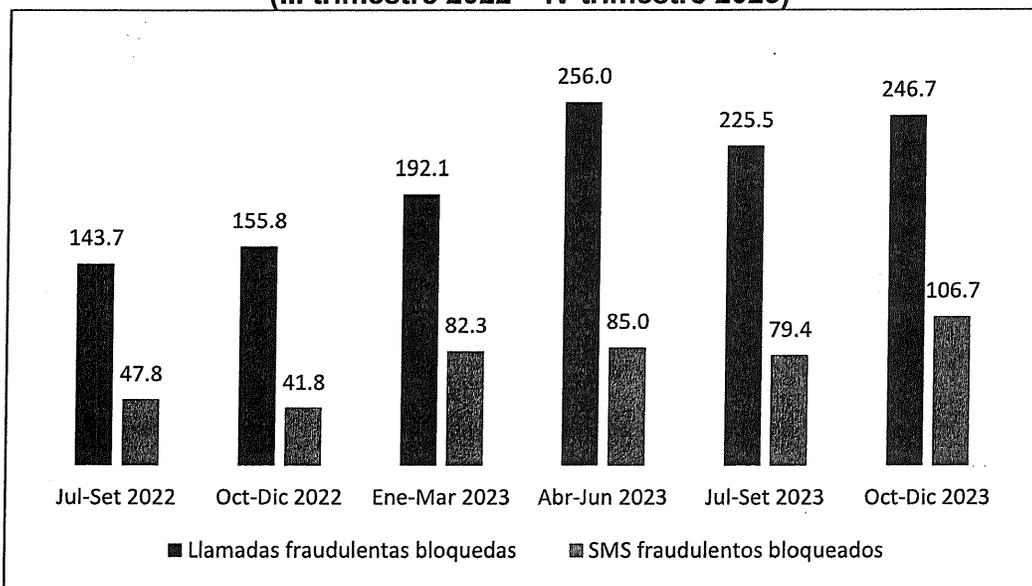
Asimismo, conforme al Intelligence Report Q4 2022-23¹¹ elaborado por the Australian Communications and Media Authority (the ACMA), tan solo durante el

¹¹ Australian Communications and Media Authority. (2023). Phone scams: Intelligence report Q4 2022-23.

segundo trimestre de 2023, se han bloqueado más de 250 millones de llamadas por fraude y más de 85 millones de mensajes de texto fraudulentos. Respecto del total de bloqueo de llamadas fraudulentas, el reporte indica que el 82% del bloqueo de llamadas corresponde a bloqueos por “Números australianos no válidos o no asignados” o “Números internacionales no válidos (código de país o longitud de dígitos no asignados)”; mientras que en el caso de los sms bloqueados, el 42% de los bloqueos en dicho trimestre corresponden a bloqueos por “SMS bloqueados que se originan en los propios clientes de los operadores” o a “SMS bloqueados recibidos de operadores de tránsito o de origen”.

En esa línea, desde diciembre de 2020, se han bloqueado más de 1,800 millones de llamadas fraudulentas, y desde julio de 2022, se han bloqueado otros 443 millones de mensajes SMS fraudulentos¹²¹³. De esta manera, estas cifras impresionantes no solo confirman la existencia, sino también el creciente problema de este tipo de actividades fraudulentas. Por lo que, el volumen significativo de comunicaciones bloqueadas refleja la eficacia de las medidas implementadas en Australia para proteger a los consumidores de estas amenazas persistentes y disruptivas.

Gráfico 11. Cantidad de llamadas y sms fraudulentos bloqueados (III trimestre 2022 – IV trimestre 2023)



Fuente: Australian Communications and Media Authority. (2024). Action on scams, spam, and telemarketing: October to December 2023. Elaboración: DGPRC-MTC.

Panorama Nacional

Siguiendo este análisis y conforme al panorama internacional, queda claro que las amenazas asociadas con las prácticas ilícitas en las comunicaciones, ya sea mediante llamadas o mensajes de texto, no son exclusivas de países desarrollados como Estados Unidos o aquellos con mercados móviles similares

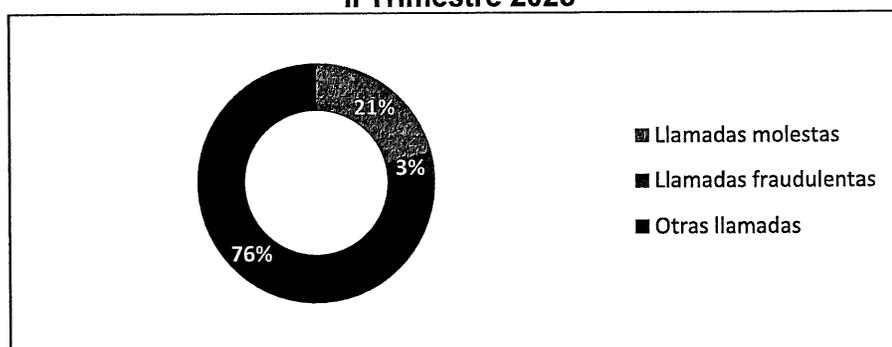
¹² Australian Communications and Media Authority. (2023). Action on scams, spam, and telemarketing: April to June 2023. Recuperado de <https://www.acma.gov.au/publications/2023-08/report/action-scams-spam-and-telemarketing-april-june-2023>

¹³ Australian Communications and Media Authority. (2024). Action on scams, spam, and telemarketing: October to December 2023. Recuperado de <https://www.acma.gov.au/publications/2024-02/report/action-scams-spam-and-telemarketing-october-december-2023>

como Australia; sino que estas también afectan significativamente al escenario local.

En el Perú, durante el segundo trimestre de 2025, el panorama de las comunicaciones no deseadas reveló un dato alarmante: un incremento en la tasa de llamadas fraudulentas, pasando de 1% en el 2023 a 3% en el segundo trimestre de 2025¹⁴. En efecto, este incremento en el porcentaje de fraudes telefónicos no solo subraya la magnitud del problema, sino que también resalta el considerable riesgo que estas prácticas representan para la seguridad y la privacidad de la población. Es así que, la presencia de llamadas fraudulentas es un claro indicativo de que los estafadores están utilizando activamente este medio para engañar y obtener beneficios ilícitos, lo que requiere una respuesta urgente y medidas robustas para proteger a la población.

Gráfico 12. Porcentaje de llamadas por fraude del total de llamadas de llamadas no deseadas de números que no son contactos II Trimestre 2025



Fuente: Global Call Threat Report. Insights into today's worldwide spam problem. Q2 2025. Hiya.

Elaboración: DGPRC-MTC.

Asimismo, de acuerdo al informe anual llamado Truecaller Insights 2021¹⁵, Perú fue el segundo país más afectado por las llamadas no deseadas durante el 2021, con un promedio de 18.02 llamadas al mes por usuario. De igual manera, durante el 2019¹⁶, Perú se volvió a ubicar como el segundo país más afectado por llamadas spam, con una cifra que asciende a 30.9 llamadas al mes por usuario, sin embargo, en el 2020, se ubicó en el puesto 14 con un total de 12.8 llamadas al mes por usuario, evidenciando de igual forma, la gran presencia de este tipo de llamadas.

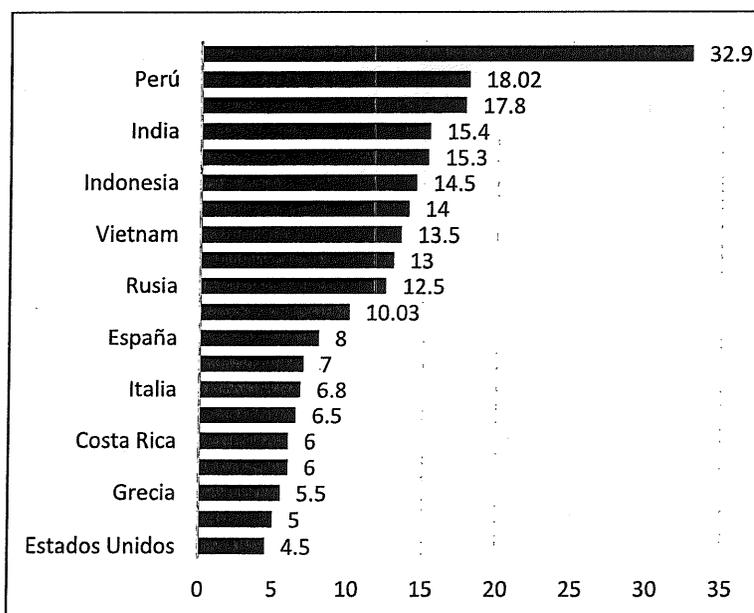
Gráfico 13. Top 20 de los países afectados por llamadas spam en 2021

¹⁴ Hiya. (2025). Global Call Threat Report Q2 2025.

¹⁵ Truecaller. (2022). Truecaller insights: Top 20 Countries Affected By Spam Calls in 2021. 2021 Global Spam & Scam Report. Recuperado de <https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021>

¹⁶ Truecaller. (2019). Truecaller Insights: Top 20 Countries Affected by Spam Calls & SMS in 2019. The top 20 Countries Affected by Spam Calls & SMS in 2019. Recuperado de <https://www.truecaller.com/blog/insights/truecaller-insights-top-20-countries-affected-by-spam-calls-sms-in-2019>

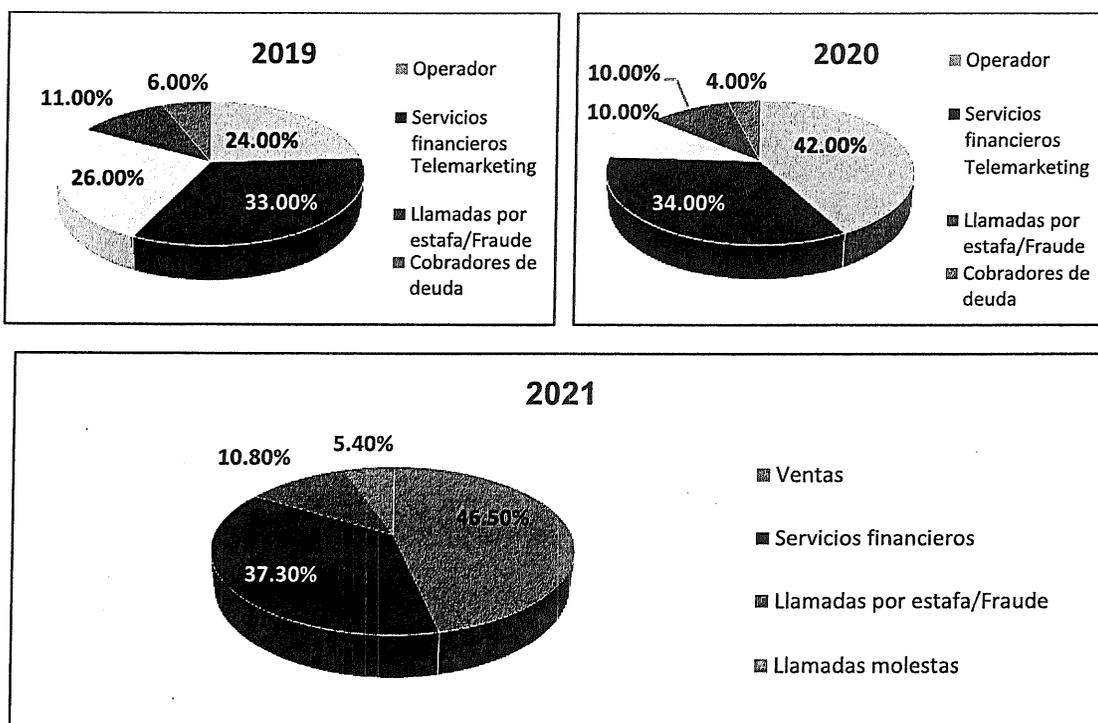
Truecaller. (2020). Truecaller Insights: Top 20 Countries Affected by Spam Calls in 2020. 2020 Global Spam & Scam Report. Extraído de <https://www.truecaller.com/blog/insights/truecaller-insights-top-20-countries-affected-by-spam-calls-in-2020-2>



Fuente: 2021 Global Spam & Scam Report. Truecaller Insights: Top 20 Countries Affected By Spam Calls In 2021. Elaboración: DGPRC-MTC.

En esa línea, de acuerdo a los informes Truecaller Insights para los años 2019, 2020 y 2021, se observa que, para el Perú, la participación de las llamadas categorizadas como fraude o estafa ha representado entre el 10% y 11% del total de llamadas marcadas como *spam*, lo que indica que este tipo de llamadas ha presentado un comportamiento constante y presente durante esos tres años.

Gráfico 14. Participación de las llamadas *spam* por categorías



Fuente:

Truecaller. (2022). Truecaller insights: Top 20 Countries Affected By Spam Calls in 2021. 2021 Global Spam & Scam Report.

Truecaller. (2020). Truecaller Insights: Top 20 Countries Affected by Spam Calls in 2020. 2020 Global Spam & Scam Report.

Truecaller. (2019). Truecaller Insights: Top 20 Countries Affected by Spam Calls & SMS in 2019. The top 20 Countries Affected by Spam Calls & SMS in 2019.

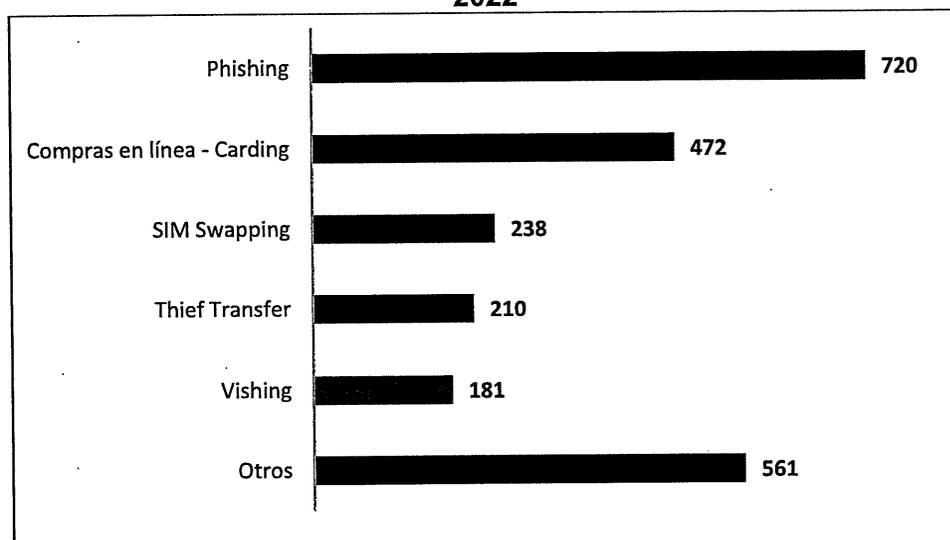
Elaboración: DGPRC-MTC.

Bajo este contexto, existe una fuerte presencia de llamadas fraudulentas no solo a nivel internacional, sino también a nivel nacional como se ha expuesto en las líneas precedentes, lo cual a su vez se evidencia en las denuncias por este tipo de delito.

En el Perú, la ola de fraudes informáticos se ha vuelto muy recurrente, tan es así que, durante el 2022, según datos de la División de Alta Tecnología (Divindat), se registraron 2,382 denuncias por causas de fraude informático¹⁷, lo cual lo convierte en el delito informático más denunciado en ese año.

Si bien el *phishing* es la modalidad de fraude más frecuente, otras modalidades de fraude están tomando relevancia como el *vishing*, donde el 8% de las denuncias presentadas por fraude, correspondían a esta modalidad.

Gráfico 15. Denuncias por modalidad de fraude 2022



Fuente: DIVINDAT

Elaboración: DGPRC-MTC.

Asimismo, conforme a lo indicado por el Ministerio Público, hasta el 31 de octubre de 2022, se han atendido 9,403 casos de delitos informáticos solo en Lima Centro y 16 distritos de la capital¹⁸, donde las modalidades de delitos más frecuentes fueron los fraudes informáticos y las estafas agravadas, que se aplican por la modalidad de *vishing*, *phishing* y *smishing*.

¹⁷ <https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru>

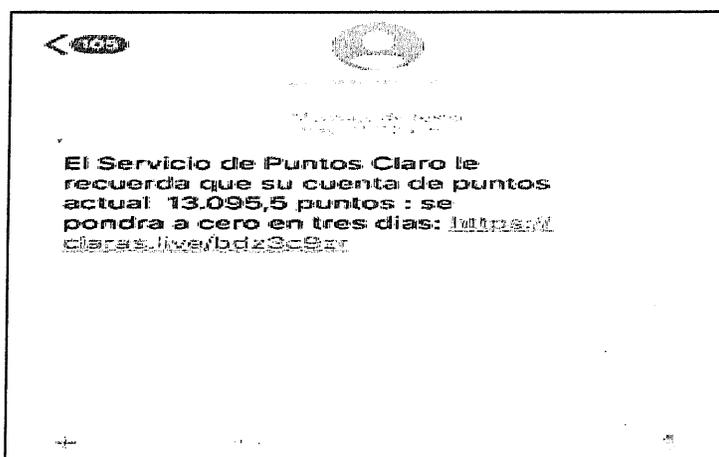
¹⁸ <https://www.linkedin.com/pulse/en-el-2022-ministerio-p%C3%BAblico-recibi%C3%B3-casi-10-mil-denuncias-/?originalSubdomain=es>

Además, de acuerdo a la División de Estafas y Otras Defraudaciones (Divieod) de la Policía Nacional del Perú (PNP), durante los meses de enero y mayo del 2023, se recibieron 3,410 denuncias por estafa en Lima Metropolitana¹⁹, donde las llamadas suplantando la identidad de un familiar fue el método más común de estafa, representando el 16% de las denuncias presentadas en dicho periodo y, de otro lado, las denuncias por suplantación de identidad representaron el 10%.

En esa línea, estas denuncias por estafa generan perjuicios económicos a los ciudadanos, tan es así que, las estafas por llamada familiar representaron pérdidas económicas de S/ 391,576.60 y, por otro lado, las pérdidas económicas por suplantación de identidad ascendieron a S/ 1,067,886.94.

En este contexto, una de las principales empresas operadoras de telecomunicaciones en Perú ha emitido una alerta sobre una creciente campaña de *smishing* que afecta a sus usuarios²⁰. Esta estrategia maliciosa se manifiesta a través de mensajes de texto que informan sobre el supuesto vencimiento de una popular promoción de la operadora. Estos mensajes de texto engañosos invitan a los usuarios a ingresar a un enlace que simula ser la tienda virtual de la operadora, con el objetivo de sustraer información personal sensible, principalmente los datos de las tarjetas de crédito o débito de los usuarios, por lo que, aquellos que puedan ser víctimas de esta trampa están en riesgo de sufrir significativas pérdidas económicas debido al fraude.

Gráfico 16. Campaña de smishing a usuarios de América Móvil



Fuente: Cornejo, D. (2024). La República. Recuperado de <https://larepublica.pe/sociedad/2024/05/01/nueva-modalidad-de-estafa-a-usuarios-de-claro-asi-obtienen-datos-personales-para-robar-informacion-claro-puntos-claro-club-76386>

En resumen, las modalidades por fraude a través de las llamadas telefónicas y mensajes de texto han tomado relevancia en el contexto nacional, tan es así que el porcentaje de llamadas por fraude ha presentado una tasa de entre el 10% y 11% del total de llamadas *spam*, tasa que ha sido superior a la de muchos países de Sudamérica, siendo superado solo por Brasil, incluso Perú ha presentado una

¹⁹ https://elcomercio.pe/lima/la-llamada-telefonica-o-mensaje-de-un-supuesto-familiar-es-la-estafa-mas-utilizada-en-lima-metropolitana-de-que-formas-operan-los-delincuentes-informe-ecdata-delincuencia-delitos-crimen-seguridad-pnp-policia-nacional-del-peru-noticia/?ref=ecr#google_vignette

²⁰ Cornejo, D. (2024). Esta es la nueva modalidad de estafa a clientes de Claro: ¿cómo operan para robar datos personales? La República. Recuperado de <https://larepublica.pe/sociedad/2024/05/01/nueva-modalidad-de-estafa-a-usuarios-de-claro-asi-obtienen-datos-personales-para-robar-informacion-claro-puntos-claro-club-76386>

mayor tasa de llamadas por fraude que países desarrollados como Estados Unidos

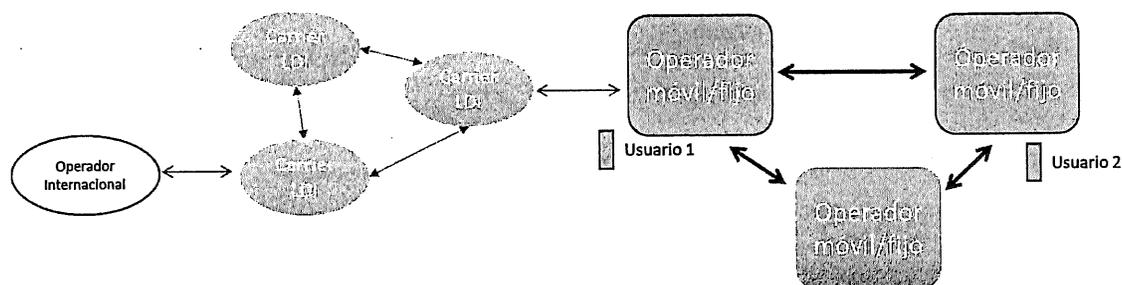
5.1.2. Análisis de escenarios de fraude en las comunicaciones

Del análisis realizado y de las relaciones de interconexión existentes actualmente, se derivan algunos escenarios o rutas potenciales a través de las cuales se concretarían algunas comunicaciones ilícitas. En los siguientes gráficos se han ejemplificado algunos de los supuestos que han sido advertidos durante el análisis y desarrollo del presente proyecto normativo.

a) Fraude sobre Larga Distancia Internacional (LDI)

El gráfico 17 muestra que, en el caso de las llamadas internacionales, estas pueden originarse en un operador de larga distancia debidamente habilitado; sin embargo, al ser transportadas por múltiples carriers intermedios, es posible que el número de origen sea reescrito o normalizado de forma indebida, ya sea por limitaciones o características técnicas particulares, para ocultar el origen real, reducir costos de terminación o eludir mecanismos de control, presentándose finalmente al usuario como una llamada local o como proveniente de una entidad legítima, generando finalmente que no se valide la fuente original de la comunicación.

Gráfico 17. Fraude sobre Larga Distancia Internacional

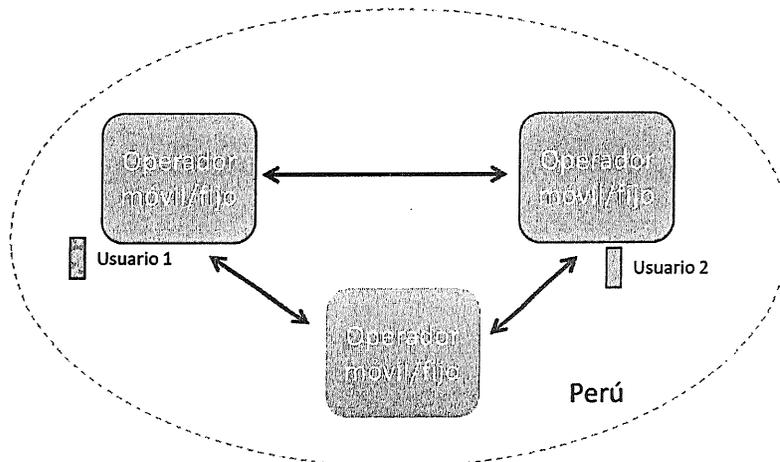


Elaboración: DGPRC-MTC

b) Fraude en el Ámbito Local

Para el caso de las comunicaciones en el ámbito nacional, estas se originan y terminan dentro del territorio peruano, transitando por una o más redes de empresas operadoras mediante acuerdos o mandatos de interconexión, como se muestra en el siguiente gráfico. Si bien, en principio, esta condición supone mayor trazabilidad y control, no se encuentra exenta del riesgo asociado a la manipulación de la numeración y a la generación de comunicaciones ilícitas.

Gráfico 18. Fraude en el ámbito local

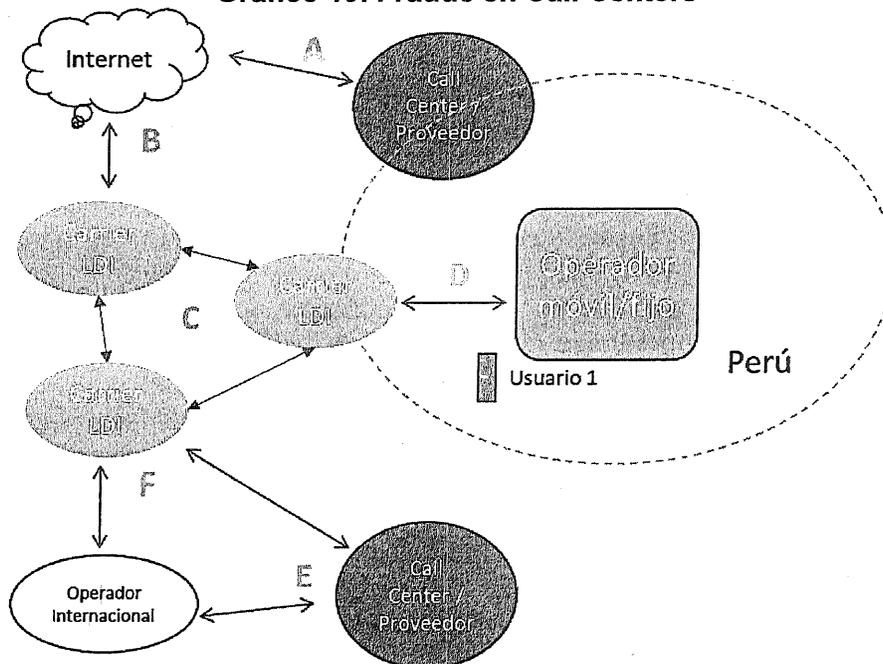


Elaboración: DGPRC-MTC

c) Fraude en Call Centers

Adicionalmente a los escenarios de transporte y tránsito de comunicaciones, resulta relevante considerar los casos vinculados al funcionamiento de call centers nacionales e internacionales, los cuales, debido a su naturaleza operativa y a los volúmenes de tráfico que gestionan, pueden constituir un vector significativo para la generación y propagación de comunicaciones ilícitas cuando no existen mecanismos adecuados de control y autenticación del origen.

Gráfico 19. Fraude en Call Centers



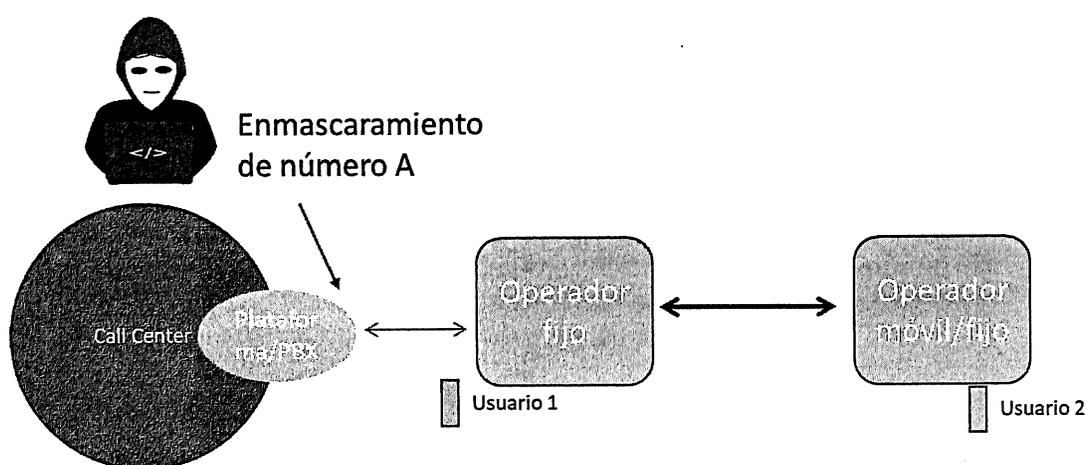
Elaboración: DGPRC-MTC

En particular, tal como se muestra en el gráfico anterior, los call centers internacionales suelen originar llamadas utilizando plataformas de voz sobre IP o

sistemas de marcación automática (ruta A – B – C – D), interconectándose con operadores de larga distancia internacional o carriers de tránsito (ruta E – F – C – D) para la entrega de las comunicaciones hacia redes móviles o fijas nacionales. En estos casos, el identificador de número A²¹ puede ser configurado libremente en la señalización, permitiendo que el tráfico se presente con numeración nacional, numeración perteneciente a entidades financieras u organismos públicos, o incluso con números inexistentes o reservados con el objetivo de incrementar la tasa de respuesta del usuario final y facilitar esquemas de fraude.

De forma similar, en el ámbito de los call centers locales, pueden presentarse escenarios en los que, aun contando con numeración asignada de manera legítima, se haga un uso indebido de esta mediante técnicas de enmascaramiento del número de origen, reutilización masiva de rangos numéricos, o empleo de plataformas de marcación (o PBX) que permiten alterar el identificador de número A. Estas prácticas dificultan la trazabilidad de las comunicaciones y pueden generar confusión en los usuarios, especialmente cuando el número presentado coincide con el de terceros ajenos a la comunicación o con el de empresas reconocidas. Esto se presenta en el siguiente gráfico.

Gráfico 20. Fraude en call centers de interconexión directa a un operador



Elaboración: DGPRC-MTC

Asimismo, existen configuraciones híbridas en las que un call center opera físicamente en territorio nacional, pero enruta sus comunicaciones a través de plataformas o carriers ubicados en el extranjero, lo que fragmenta la cadena de responsabilidad técnica y facilita la introducción de tráfico con características de ruta gris o con numeración adulterada. En tales casos, la comunicación puede ingresar a la red nacional como tráfico local, pese a haberse originado y procesado parcialmente fuera del país, lo que acrecienta el riesgo de suplantación y dificulta la aplicación de controles.

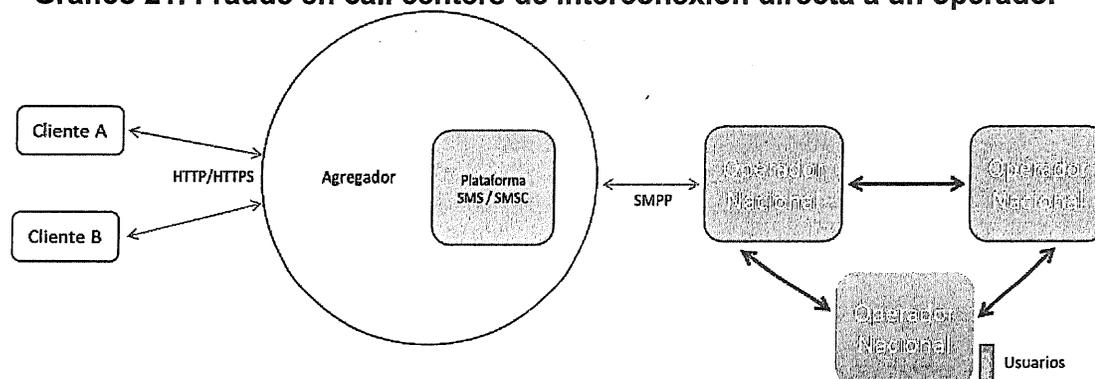
d) Fraude en mensajería SMS

En el ámbito de mensajería SMS, en determinados escenarios de interconexión y mediante el uso de plataformas y/o aplicaciones o sistemas informáticos se generan mensajes hacia usuarios finales en los cuales, debido a las características técnicas de dichas comunicaciones, la identidad del emisor no puede ser validada directamente por la empresa operadora de

²¹ Número A: Se refiere al número de abonado asignado al llamante o remitente, generado por el operador donde este abonado se encuentra registrado o ha adquirido su servicio.

telecomunicaciones. En este tipo de escenarios intervienen diversos actores que constituyen los agentes vinculados en la trazabilidad de las comunicaciones. Desde una perspectiva técnica – operativa o funcional, considerando que individualmente cada uno de estos actores no puede determinar el origen de las comunicaciones, estos agentes deben complementarse con el fin de obtener la trazabilidad de las comunicaciones con fines ilícitos.

Gráfico 21. Fraude en call centers de interconexión directa a un operador



Elaboración: DGPRC-MTC

Estos fenómenos evidencian que la problemática del fraude en las telecomunicaciones no puede abordarse exclusivamente desde el punto de origen del tráfico, sino que requiere controles técnicos a lo largo de la cadena de la comunicación (origen, en tránsito y destino). En tal sentido, resulta necesario establecer disposiciones que permitan a las empresas operadoras implementar mecanismos de gestión de red orientados a preservar la integridad del identificador de número A, verificar la coherencia entre la numeración presentada y la ruta de procedencia, detectar rutas irregulares y bloquear de manera preventiva las comunicaciones cuya autenticidad no pueda ser verificada. Del mismo modo, las medidas propuestas en la presente norma no buscan limitar la actividad legítima de los call centers, ni del mercado de mensajería subyacente, sino prevenir el uso irregular de la numeración y asegurar que las comunicaciones que alcanzan al usuario final cuenten con parámetros de origen verificables y consistentes.

e) Fraudes basados en parámetros técnicos como direcciones IP

En los escenarios tradicionales de llamadas y mensajes de texto con fines ilícitos, también se cuenta con escenarios en los que una comunicación ilícita o fraudulenta se origina en una aplicación o plataforma OTT, como Whatsapp, en estos casos, las autoridades competentes son los responsables de realizar la investigación correspondiente, es en el transcurso de dicha investigación en la que se requiere la identificación y correlación de diversos parámetros técnicos (como por ejemplo: IMSI, IMEI, nombre de usuario, dirección IP, nodo, sector, azimut, entre otros) y datos o registros de usuarios en las redes de telecomunicaciones.

Desde un punto de vista técnico, las plataformas OTT no cuentan con acceso directo a la red de acceso ni a información de origen de la comunicación (localización de los dispositivos finales). En ese sentido, la participación de los operadores en estos procesos se limita, a proporcionar información técnica de los registros de sus servicios (registro de conexiones, tales como direcciones IP, marcas de tiempo y datos técnicos asociados a las sesiones de sus usuarios), cuando esta sea requerida por la autoridad competente en el marco de un procedimiento judicial, debidamente documentado. Dicha información puede

incluir, entre otros, la asociación temporal entre una dirección IP y un abonado, equipo o punto de acceso, siempre respetando los principios de legalidad, proporcionalidad y finalidad específica de la investigación.

Por lo tanto, la oportuna cooperación de las empresas operadoras de telecomunicaciones con las autoridades competentes para la identificación del origen de las comunicaciones, se sustenta en la necesidad de complementar los procesos formales de investigación digital, particularmente aquellos iniciados por plataformas de servicios de comunicaciones OTT, como WhatsApp, en el marco de la prevención, detección e investigación de actividades ilícitas. Esta interacción permite tener la trazabilidad de la comunicación tanto en las redes de telecomunicaciones, como en las redes IP.

Sobre las acciones de fiscalización realizadas por la DGFSC

La Dirección General de Fiscalizaciones y Sanciones en Comunicaciones (DGFSC) del Ministerio de Transportes y Comunicaciones en el marco de sus funciones y de la problemática identificada sobre la trazabilidad de los mensajes A2P (Application to person) realiza labores de fiscalización a diversas empresas operadoras móviles y fijas para la verificación del cumplimiento de las obligaciones establecidas en el marco legal y reglamentario, así como las condiciones técnicas y operativas correspondientes a los servicios que brindan.

La fiscalización en mención consta de pruebas de envío y recepción de SMS P2P (Person to Person) y A2P entre las redes de la empresa operadoras vía interconexión. Las empresas operadoras móviles indicaron que no realizan el envío de SMS A2P entre ellas vía interconexión.

En su accionar la DGFSC verificó que se viene haciendo uso del protocolo SMPP (Short Message Peer-to-Peer) el cual es un protocolo estándar de telecomunicaciones para el intercambio de SMS. Asimismo, se observó que las empresas operadoras móviles no envían a la empresa operadora fija el mensaje de señalización de mensaje de recepción o de mensaje recibido.

De las labores de fiscalización realizadas por la DGFSC a las empresas operadoras móviles y fijas se observó que a nivel de trazas se puede identificar las direcciones IP de los puntos de interconexión dado por las concesionarias a otras que ingresan a su red, lo cual es rastreable e identificable hasta dicho punto de interconexión, ello a pesar de que las direcciones IP son dinámicas.

En tal sentido, según lo informado por la DGFSC, podría ser factible la identificación del origen o destino de los mensajes enviados o recibidos a través de la consulta de los registros (log) de las trazas de señalización de las direcciones IP de los puntos de interconexión entre operadores.

5.1.3. Delimitación del problema público

El desarrollo acelerado de las tecnologías de la información y las comunicaciones ha permitido una expansión sin precedentes en la conectividad y el acceso a los servicios de telecomunicaciones. Sin embargo, este mismo progreso ha sido aprovechado de manera indebida por organizaciones y personas que utilizan las redes de telecomunicaciones para la comisión de actividades ilícitas, tales como fraudes telefónicos, estafas mediante mensajes de texto (SMS), suplantación de identidad y otras prácticas que vulneran la confianza de los usuarios y afectan la seguridad del país.

Ante este escenario, resulta indispensable que el Estado, adopte medidas normativas, técnicas y operativas que fortalezcan la integridad y la confiabilidad de las redes públicas de telecomunicaciones, protegiendo tanto a los usuarios y entidades como a la infraestructura crítica nacional.

El presente marco normativo se enmarca en dicho propósito, busca establecer medidas y obligaciones orientadas a prevenir, detectar y mitigar las comunicaciones ilícitas que utilizan las redes de telecomunicaciones como medio para su ejecución, coadyuvando así a una mayor transparencia, trazabilidad e identificación en las llamadas y mensajes de texto.

De otra parte, el incremento sostenido de las comunicaciones con fines ilícitos mediante el uso de las redes de telecomunicaciones constituye un desafío creciente para el Estado, los operadores y la ciudadanía. Los delincuentes emplean técnicas cada vez más sofisticadas que les permiten manipular o enmascarar los identificadores de las llamadas y mensajes de texto, simulando provenir de entidades legítimas con el objetivo de engañar a los usuarios y obtener información personal, financiera o de autenticación.

Entre las acciones que conllevan a la realización de llamadas y mensajes ilícitos o sospechosos, se destacan las siguientes:

- 1) **Suplantación de identidad en llamadas y mensajes (spoofing):** Manipulación del número A o del remitente alfanumérico para aparentar una identidad distinta a la real, dificultando la trazabilidad y favoreciendo la comisión de fraudes.
- 2) **Uso de numeración no asignada o irregular:** Envío de comunicaciones desde rangos de numeración que no han sido otorgados o que se encuentran restringidos.
- 3) **Ausencia de autenticación y control del identificador de origen:** Las redes legadas y la falta de interoperabilidad en la señalización dificultan la validación del número A en las fronteras internacionales o entre operadores nacionales.
- 4) **Limitada capacidad de monitoreo y bloqueo de tráfico ilícito:** No todos los operadores cuentan con plataformas tecnológicas (como firewalls de llamadas o SMS, o sistemas de autenticación digital) que permitan analizar patrones sospechosos y bloquear en tiempo real las comunicaciones con fines ilícitos.
- 5) **Afectación a los usuarios y pérdida de confianza:** Los usuarios enfrentan diariamente intentos de fraude o suplantación mediante llamadas o mensajes falsos, lo que deteriora la percepción de seguridad en las redes de telecomunicaciones, generando insatisfacción por parte de los usuarios y afectando la credibilidad de las instituciones que son falsamente utilizadas como fachada.
- 6) **Impacto en la integridad del sistema de numeración nacional:** El uso indebido de la numeración y la ausencia de mecanismos de autenticación robustos debilitan la administración eficiente del recurso numérico, afectando su función como elemento esencial para la identificación y trazabilidad de las comunicaciones.

En ese sentido, el problema público identificado a resolver es la alta incidencia en las comunicaciones con fines ilícitos a través de llamadas telefónicas y mensajes de texto cursados en las redes de telecomunicaciones. Según el informe Truecaller Insights 2021, el Perú se posicionó como el segundo país más afectado

por llamadas no deseadas, con un promedio de 18.02 llamadas spam por usuario al mes, de las cuales el 10.8% son llamadas por estafa o fraude, que al año hacen más de mil millones de llamadas por este tipo de actividades ilícitas.

Por lo tanto, el Estado necesita evaluar acciones de intervención regulatoria o no regulatoria para establecer obligaciones claras en materia de autenticación, trazabilidad, validación de numeración y reporte de las mismas, garantizando que los operadores adopten medidas proporcionales y efectivas que permitan proteger al usuario final, preservar la integridad de la red y asegurar la confianza en el ecosistema digital nacional.

5.1.4. Revisión de la experiencia internacional sobre medidas técnicas y regulatorias adoptadas en el marco de la lucha contra las comunicaciones ilícitas

A continuación, se presenta un resumen de las principales medidas técnicas y regulatorias adoptadas por diversos países en el marco de la lucha contra las comunicaciones ilícitas.

➤ Canadá

Respecto a medidas para combatir comunicaciones con fines ilícitos, de acuerdo a lo establecido por la Comisión Canadiense de Radio, Televisión y Telecomunicaciones (CRTC), los teleoperadores que realizan llamadas están obligados a identificarse, así como a identificar a sus clientes. En noviembre de 2018, la CRTC también exigió a los operadores y proveedores de servicios de telecomunicaciones que implementaran el bloqueo universal de llamadas a nivel de red, de la siguiente manera:

Los proveedores de servicios telefónicos que aún no ofrezcan un sistema de filtrado de llamadas opcional deben bloquear todas las llamadas con identificadores de llamadas que:

- Superen los 15 dígitos, o
- No sean marcables según el Plan de Numeración de América del Norte (por ejemplo, las llamadas del número "999-999-9999" se bloquearían antes de llegar al suscriptor).
- La opción de filtrado de llamadas que utilicen, debe ser capaz de detectar llamadas sospechosas e interceptarlas (ya sea enviándolas directamente al buzón de voz o solicitando a la persona que llama que introduzca una entrada en el teclado de su teléfono para comunicarse con el cliente)²².

En abril de 2021, la CRTC ordenó a los proveedores de servicios de telecomunicaciones implementar la tecnología STIR/SHAKEN para combatir las llamadas falsas.

Con esta solución tecnológica los proveedores podrán autenticar y verificar la información de identificación de llamadas (ID) para llamadas de voz basadas en el Protocolo de Internet (IP) certificando si la identidad de la persona que llama es confiable, ello como condición para la oferta y prestación de servicios de

²² Ver norma: <https://crtc.gc.ca/eng/phone/telemarketing/identit.htm>

telecomunicaciones²³. En noviembre de 2021, el CRTC anunció la implementación de las referidas medidas²⁴.

➤ **Brasil**

La Agencia Nacional de Telecomunicaciones (Anatel), organismo regulador de telecomunicaciones en el país, ha venido adoptando acciones para combatir las comunicaciones no deseadas, al emitir cuatro medidas cautelares sucesivas (Orden de Decisión N° 160/2022/COGE/SCO, de junio de 2022, Orden de Decisión N° 250/2022/COGE/SCO, de octubre de 2022, Orden de Decisión N° 103/2023/COGE/SCO, de abril de 2023 y Orden de Decisión n° 22/2024/RCTS/SRC, de abril de 2024), Anatel determinó que los proveedores de servicios de telecomunicaciones fijos (STFC) y proveedores de servicios móviles (SMP) bloquean las llamadas originadas por usuarios que configuran un uso inadecuado del servicio telefónico caracterizado por un volumen excesivo de llamadas diarias cortas.

Entre las principales medidas adoptadas para mitigar las comunicaciones no deseadas se tienen:

- Proveedores bloquean a los usuarios que realicen más de 100 mil llamadas diarias de hasta tres segundos. (Decisión N° 160/2022/COGE/SCO)
- Proveedores bloquean temporalmente las llamadas de usuarios que generen al menos 100.000 (cien mil) llamadas en un día, considerando el número total de accesos asignados a la persona jurídica, y en las que el número total de llamadas cortas represente una proporción igual o superior al 85% del total de llamadas. (Orden de Decisión n° 250/2022/COGE/SCO)
- Mediante la Decisión No. 103/2023/COGE/SCO se prorrogó la vigencia de las medidas establecidas en la Decisión No. 250/2022/COGE/SCO.
- Otra medida introducida fue ordenar a las empresas prestadoras de servicios de telecomunicaciones la creación de la plataforma de consulta²⁵, a través de la cual los ciudadanos interesados podrán consultar la identificación del titular de determinados códigos de acceso de telefonía fija (STFC) y telefonía celular (SMP), cuando este sea una persona jurídica.
- Posteriormente, la Orden de Decisión N° 22/2024/RCTS/SRC ajustó el concepto de llamadas cortas, considerando ahora todas aquellas completadas con una duración de hasta 6 segundos (con desconexión en el origen o destino). En las tres Decisiones anteriores, el concepto se limitaba a llamadas de hasta 3 segundos, con desconexión únicamente por parte del originador.

Medidas para la identificación de llamadas:

Para evitar llamadas no deseadas a los consumidores y mejorar la relación entre estos y el sector del telemarketing, el 24 de noviembre de 2021, ANATEL publicó la Ley N° 10.413 (Procedimiento Operativo para el Uso de Recursos de Numeración), que estableció el prefijo 0303 para el servicio de telemarketing activo. Esta medida se aplica a las llamadas de telemarketing que ofrecen productos y servicios, como líneas telefónicas fijas o teléfonos celulares. Tanto los proveedores de servicios de telecomunicaciones como los proveedores de

²³ Ver decisión Stir/shaken: <https://crtc.gc.ca/eng/archive/2021/2021-123.htm>

²⁴ Ver comunicado de prensa: <https://www.canada.ca/en/radio-television-telecommunications/news/2021/11/canadians-to-benefit-from-new-caller-id-technology-to-combat-spoofed-calls.html>

²⁵ Ver web de consulta brasileña sobre llamadas: <https://qualempresameligou.com.br/>

servicios de telemarketing activos (usuarios de la red de telecomunicaciones) están sujetos a las sanciones del artículo 173 de la Ley n.º 9.472, de 16 de julio de 1997 (advertencia, multa, suspensión temporal, caducidad y declaración de incompetencia).

El 27 de septiembre de 2022, la Ley N.º 13.672²⁶ derogó y sustituyó a la Ley N.º 10.413, manteniendo la obligatoriedad del uso del prefijo 0303 para el ejercicio de actividades activas de telemarketing e incorporando además el uso del prefijo 0500 para identificar a las entidades sin fines de lucro. El nuevo procedimiento prohíbe el reenvío de tráfico de llamadas originadas por recursos no asignados, vacantes o en cuarentena, así como el cambio del número del usuario que origina la llamada, asimismo determinan el establecimiento, por parte de los proveedores de telecomunicaciones, de procesos de control y administración de los recursos de numeración, a fin de garantizar su uso adecuado y eficiente.

➤ Reino Unido

En Reino Unido, el regulador de comunicaciones Ofcom (Office of Communications) actualizó la normativa relacionada a los datos de identidad de la línea llamante (CLI)²⁷ y que los operadores deben cumplir, como identificar y bloquear llamadas con datos CLI que no sean válidos, que no identifiquen de forma única a la persona que llama o que no contengan un número que se pueda marcar. Estos nuevos requisitos están enfocados especialmente sobre la manera en cómo se presentan los números de teléfono (CLI) cuando se recibe una llamada, especialmente para aquellas procedentes del extranjero.

Entre las principales medidas se tienen:

- El formato de una CLI debe ser un número de 10 u 11 dígitos;
- Identificación de números que no deben usarse como CLI, la información de asignación de numeración de Ofcom y la lista de no originarios (DNO).
- Debe ser un número marcable, es decir, un número en servicio que permita realizar una devolución de llamada o una llamada posterior.
- Prohibición del uso de 09 números no geográficos como CLI.
- Las llamadas de fuentes internacionales que presenten números CLI del Reino Unido falsamente se bloquearán a menos que cumplan determinados criterios.
- Excepciones legítimas: Algunas situaciones permiten el CLI del Reino Unido en una llamada internacional, como:
 - Un usuario de un móvil del Reino Unido realiza una llamada mientras está en roaming en el extranjero.
 - Una llamada a un usuario móvil del Reino Unido que se encuentra actualmente en el extranjero.
 - Usuarios comerciales del Reino Unido verificados que realizan llamadas desde ubicaciones fuera del Reino Unido.
- Las empresas que utilizan soluciones VoIP o basadas en la nube para usuarios internacionales deben verificar la legitimidad de sus usuarios para evitar ser bloqueados.

²⁶ Ver norma <https://informacoes.anatel.gov.br/legislacao/atos-de-numeracao/1741-ato-13672>

²⁷ Ver directrices sobre CLI de Ofcom: <https://www.ofcom.org.uk/phones-and-broadband/phone-numbers/calling-line-identification>

- Los proveedores de VoIP pueden requerir autenticación adicional, como seguimiento de ubicación o enlace troncal SIP seguro.

Estas nuevas medidas orientadas para la presentación del CLI están diseñadas para reducir las llamadas fraudulentas y aumentar la confianza de los usuarios en los números de teléfono del Reino Unido.

Nuevas reglas para bloquear mensajes fraudulentos

Recientemente Ofcom publico una consulta pública para comentarios hasta el 28 de enero de 2026, sobre una propuesta de nuevas normas y directrices para operadores de redes móviles y agregadores de mensajería empresarial, estableciendo los pasos que se espera adopten para combatir las estafas de mensajería móvil.²⁸

Entre las medidas consideradas para abordar las estafas en mensajería, se distinguen por aquellas originadas por particulares y por empresas, el regulador propone que los operadores de telefonía móvil deben:

- Establecimiento de límites de volumen para las tarjetas SIM prepago, dificultando el uso de soluciones como SIMbox por parte de los estafadores.
- Los proveedores deben reportar estafas a clientes y terceros, como las fuerzas del orden, para evitar el envío de mensajes y enlaces web desde números identificados como fraudulentos.
- Los proveedores deben identificar y bloquear los mensajes fraudulentos que circulan en sus redes detectando identificadores de remitentes, enlaces web y números de teléfono maliciosos.
- Los operadores o agregadores que envían mensajes masivos comerciales deben realizar verificaciones eficaces de "Conozca a su Cliente" (KYC) a los nuevos remitentes para identificar y evitar delincuentes. De igual manera, se deben realizar verificaciones de "Conozca su Tráfico", que incluyen la revisión de la actividad de la cuenta y la investigación inmediata de las denuncias de fraude.
- Evitar el uso de identificadores alfanuméricos. Los proveedores deben contrastar los identificadores de remitente de las empresas con la información recopilada sobre ellas.
- Cuando se identifiquen actividades fraudulentas, los operadores deben erradicar a los delincuentes que utilizan servicios de mensajería empresarial y exigir responsabilidades a las empresas si no han realizado las comprobaciones adecuadas.
- Bloquear los mensajes fraudulentos en tránsito. Los proveedores deben actuar según los reportes de estafa de usuarios y terceros para detectar y bloquear enlaces web y números de teléfono maliciosos.

➤ Irlanda

²⁸ Ver documento propuesto: <https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/consultation-combatting-mobile-messaging-scams>

Irlanda publicó un documento de consulta que propone medidas que busca mitigar los daños de las llamadas no solicitadas o con fines ilícitos a fin de restablecer la confianza de los usuarios en las comunicaciones de voz²⁹:

- Una lista de No Originar (“DNO”) se refiere a números de teléfono que nunca se utilizan para llamadas salientes. Por ejemplo, ciertos bancos proporcionan números para que los consumidores se comuniquen con ellos, pero nunca se comunican con un consumidor utilizando el mismo número. En consecuencia, cualquier llamada que parezca provenir de estos números es falsa y, por lo tanto, debe bloquearse automáticamente.
- Una lista de Números Protegidos (“PN”) se refiere a números de teléfono que ComReg no ha asignado a ningún operador o empresa y, por lo tanto, cualquier llamada que los presente es falsa y, por lo tanto, debe bloquearse.
- El bloqueo de llamadas CLI móvil identificaría y bloquearía llamadas molestas provenientes de redes internacionales que se presentan con identificadores de llamadas móviles irlandeses, a menos que la persona que llama sea genuina y se sepa que está en el extranjero. Estas llamadas intentan engañar a los clientes haciéndoles creer que la llamada proviene de alguien en Irlanda desde su teléfono móvil.
- El bloqueo de llamadas CLI fijas funciona de la misma manera que el bloqueo de llamadas CLI móviles, pero bloquea las llamadas molestas que falsifican números geográficos (p. ej., 01, 061) y/o los números no geográficos que utilizan las empresas (p. ej., 0818).

➤ **Estados Unidos**

En Estados Unidos el Congreso estadounidense aprobó la Ley para el Control del Ataque de Pornografía y Marketing No Solicitado (CAN-SPAM) y su reglamento³⁰ en 2003, estableciendo límites para la adopción del spam en todo el país. La ley que establece las reglas para el correo electrónico comercial, define los requisitos para mensajes comerciales, da a los destinatarios el derecho a pedir que se les deje de enviar este tipo de información y detalla fuertes sanciones por su violación.

Tanto los mensajes transaccionales como los relativos a mercadotecnia están bajo la jurisdicción de la Ley CAN-SPAM. Los correos electrónicos transaccionales sólo están obligados a transmitir información veraz, pero los correos electrónicos de carácter comercial están sujetos además a los siguientes requerimientos:

- Evitar engañar al destinatario
- Incluir una dirección postal en el cuerpo del correo electrónico
- Proveer un enlace para anular la suscripción
- Honrar las solicitudes de exclusión voluntaria en un plazo de 10 días
- Responsabilidad de los emisores y sus agencias

Por otro lado, la Communications Commission (FCC), regulador de telecomunicaciones norteamericano y la Federal Trade Commission (FTC) han implementado varias políticas para combatir las llamadas y los mensajes de texto ilícitos:

²⁹ Ver documento de consulta: <https://www.comreg.ie/media/2023/06/ComReg-2352e.pdf>

³⁰ Ver norma <https://www.ftc.gov/legal-library/browse/rules/can-spam-rule>

- STIR/SHAKEN³¹: Es un sistema que autentica las llamadas para combatir la suplantación de identidad (caller ID spoofing). El sistema permite verificar que las llamadas provienen realmente del número que dicen tener, ayudando a reducir las estafas telefónicas.
- Regulaciones contra el Robo de Identidad y Estafas por SMS: A través de la Truth in Caller ID Act³², se prohíbe la suplantación de identidad y el uso de información falsa en las llamadas. También, se ha trabajado en la promoción de aplicaciones y tecnologías que bloquean o etiquetan los mensajes sospechosos de ser estafas.
- Regulación de los SMS comerciales: A través de la Telephone Consumer Protection Act (TCPA)³³, las llamadas automáticas y los mensajes no solicitados están regulados, y las empresas deben obtener el consentimiento explícito del consumidor para enviarlos.

Desde la Ley Traced del 2019, la FCC inició un conjunto de disposiciones para disuadir y combatir las llamadas automáticas (robocallers) entre las que incluía sanciones y el desarrollo de tecnologías de autenticación de llamadas por parte de los proveedores de servicios de voz. En octubre de 2020, se ordenó a los proveedores de voz intermedios y de terminación de EE.UU. que no aceptaran llamadas utilizando números de EE.UU. directamente de proveedores de origen extranjero que no figuran en la base de datos de Mitigación de Robocalls (RMD).

Para combatir las robocallers originadas en el extranjero, la FCC colocó a los proveedores de puerta de enlace bajo el régimen anti-robocall con un nuevo conjunto de reglas en el 2022.

Las nuevas reglas exigen que:

- Los proveedores de puerta de enlace apliquen el protocolo de verificación de identificación de llamadas anti-robocall existente, conocido como STIR/SHAKEN a todas las llamadas originadas en el extranjero no autenticadas (solo tráfico IP de voz) que muestran números de identificación de llamadas (CLI) utilizando el plan de numeración de EE. UU.
- El desarrollo y envío de planes de mitigación de tráfico a la Base de Datos de Mitigación de Robocalls.
- Se responda a los esfuerzos para rastrear las llamadas automáticas ilegales hasta su origen dentro de las 24 horas.
- El bloqueo de cualquier llamada que el proveedor de puerta de enlace pueda identificar claramente como conductos para el tráfico ilegal.
- Se tomen medidas razonables y efectivas para garantizar que el proveedor de servicios de voz extranjero inmediato ascendente no esté utilizando la puerta de enlace para traer un alto volumen de tráfico ilegal a una red de EE. UU.

➤ **Australia**

En Australia, se aprobó un código de la industria de las telecomunicaciones para la reducción de llamadas y mensajes de texto fraudulentos³⁴, desarrollado por la

³¹ Ver <https://www.fcc.gov/call-authentication>

³² Ver <https://www.fcc.gov/document/rules-and-regulation-implementing-truth-caller-id-act-2009>

³³ Ver norma <https://www.fcc.gov/sites/default/files/tcpa-rules.pdf>

³⁴ Ver código: https://www.austelco.org.au/wp-content/uploads/2025/06/C661_2022.pdf

industria de las telecomunicaciones, aborda el problema de las estafas mediante llamadas telefónicas y mensajes de texto cortos (SMS). El código “establece procesos para identificar, rastrear, bloquear e interrumpir llamadas y SMS fraudulentos”, su cumplimiento es voluntario, a menos que la Autoridad Australiana de Medios y Comunicaciones (ACMA) lo exija.

Según el código, los operadores y proveedores de servicios de telecomunicaciones deben hacer todo lo posible para identificar, rastrear, bloquear e interrumpir dichas llamadas y mensajes. Abarca las llamadas y los mensajes de texto originados tanto en Australia como a nivel internacional, para ello los operadores deben utilizar todos los acuerdos contractuales disponibles para obtener la asistencia del operador internacional correspondiente con el fin de detener y bloquear futuras comunicaciones fraudulentas identificadas hacia Australia. Asimismo, se incluye normas y procesos para combatir la suplantación de identidad y el uso indebido de identificadores alfanuméricos de remitente.

El gobierno australiano realizó en febrero de 2024 una consulta sobre un Marco de Código contra Estafas³⁵ que propone nuevos códigos obligatorios para el sector privado, incluidas las empresas de telecomunicaciones.

➤ España

España es uno de los principales países de Europa en implementar medidas regulatorias para combatir comunicaciones no deseadas, especialmente las llamadas comerciales invasivas, mensajes de spam, correos electrónicos publicitarios sin consentimiento y suplantaciones de identidad (phishing y smishing). Entre las principales medidas legislativas se tienen:

Ley General de Telecomunicaciones (Ley 11/2022)³⁶, por el cual se prohíbe expresamente las llamadas comerciales no deseadas (spam telefónico), a menos que el usuario haya dado su consentimiento previo y expreso; y cuyas principales medidas son:

- Reforzar los derechos de los usuarios frente a las comunicaciones intrusivas.
- Exigir que los operadores garanticen la identificación clara de las llamadas comerciales.
- Las personas tienen derecho a oponerse al tratamiento de sus datos con fines de marketing en cualquier momento.

Ley de protección de datos o LOPDGDD (Ley Orgánica 3/2018)³⁷

- Exige el consentimiento explícito para enviar comunicaciones publicitarias electrónicas (correo, SMS, llamadas).
- El usuario tiene derecho a acceder, rectificar y borrar sus datos, así como a oponerse al uso de sus datos para fines comerciales.
- Sanciona a empresas que no respeten estas normas (la AEPD impone multas que pueden superar los 100.000 €).

Ley de Servicios de la Sociedad de la Información (LSSI - Ley 34/2002)³⁸, cuyas principales medidas son:

³⁵ Ver <https://treasury.gov.au/consultation/c2023-464732>

³⁶ Ver norma: <https://www.boe.es/buscar/doc.php?id=BOE-A-2022-10757>

³⁷ Ver norma: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>

³⁸ Ver norma: <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

- Regular el envío de comunicaciones comerciales electrónicas (emails, SMS, etc.).
- Establecer que este tipo de comunicaciones solo pueden enviarse si el usuario las ha solicitado o existe una relación contractual previa.
- Las empresas deben incluir un método sencillo para darse de baja en cada mensaje.

En febrero de 2025, Ministerio para la Transformación Digital y de la Función Pública publicó la Orden TDF/149/2025³⁹ por el cual se establecen medidas para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos y para garantizar la identificación de la numeración utilizada para la prestación de servicios de atención al cliente y realización de llamadas comerciales no solicitadas. Entre los principales objetivos de la Orden, se tiene:

- Combatir la manipulación del identificador de línea llamante (CLI): La orden introduce mecanismos para evitar fraudes relacionados con la manipulación del CLI en llamadas y mensajes.
- Garantizar la identificación de la numeración utilizada en servicios de atención al cliente y llamadas comerciales no solicitadas: Establece medidas para asegurar que la numeración utilizada en estos servicios sea claramente identificable y esté debidamente registrada
- Bloqueo de llamadas y mensajes fraudulentos: Los operadores deben bloquear llamadas y mensajes que presenten numeración no atribuida, asignada o adjudicada, incluyendo numeración vacía, así como aquellos con origen internacional que utilicen numeración del plan nacional de numeración, salvo en casos de itinerancia internacional
- Registro de alias comerciales: Se establece la obligación de registrar los alias utilizados en servicios de mensajería (SMS/MMS/RCS) en un registro gestionado por la Comisión Nacional de los Mercados y la Competencia (CNMC).

Con estas medidas el gobierno español busca reforzar la protección de los usuarios frente a fraudes y mejorar la transparencia en las comunicaciones comerciales.

5.2. Medidas consideradas para la solución del problema público

- **Las empresas operadoras adoptan medidas y/o mecanismos técnicos y/u operativos para evitar el progreso⁴⁰ de llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos; así como, para permitir a los abonados y usuarios advertir sobre dichas comunicaciones.**

Se propone la presente medida para enfrentar la problemática de las llamadas y mensajes de texto con fines ilícitos, las cuales serán aplicables para los

³⁹ Ver norma: <https://www.boe.es/buscar/doc.php?id=BOE-A-2025-2870>

⁴⁰ En la propuesta normativa se emplea la palabra "progreso" haciendo referencia a un flujo a través de un sistema. Se considera que, en el ámbito de las telecomunicaciones, el progreso de una comunicación se refiere a la secuencia de estados por los que esta pasa. Al decir que el enmascaramiento "conlleva al progreso", el texto se refiere a permitir que la comunicación atraviese todas sus fases. Por lo tanto, el progreso alude al proceso de navegación de los datos a través de la red.

Si una comunicación "progresa", significa que se le ha permitido:

- Ingresar a la red (origen).
- Ser transportada a través de nodos, routers y demás equipos de red (tránsito).
- Llegar al destino final en la red o ser derivada hacia otra (terminación).

operadores, comprendiendo a las personas naturales o jurídicas que poseen un título habilitante o registro para prestar el servicio público de telefonía fija o móvil; así como, el registro de valor añadido para prestar el servicio de almacenamiento y retransmisión de datos, lo que también alcanza a los operadores móviles virtuales (OMV).

Diversas organizaciones, tales como, UIT, ETSI, FCC, GSMA y otras, han desarrollado distintas recomendaciones relacionadas a la gestión de tráfico fraudulento, prevención de suplantación de comunicaciones, el formato que debe seguir un número telefónico internacional, entre otros. Todas estas recomendaciones están orientadas a prevenir llamadas y/o mensajes de texto ilícitos y serán recogidas de forma referencial, a efectos de que las empresas operadoras las tomen en cuenta para sus labores de monitoreo y/o investigación con el propósito de asegurar la trazabilidad de las comunicaciones, según corresponda. En este contexto, se entiende que la adecuada gestión técnica de las redes por parte de las empresas operadoras constituye un elemento esencial para garantizar la seguridad de los usuarios, así como para prevenir afectaciones a las redes de telecomunicaciones.

En esa línea de ideas, por ejemplo, la recomendación UIT-T E.164 define el formato internacional estándar de los números telefónicos; además, establece el plan internacional de numeración para las telecomunicaciones públicas, definiendo la estructura y funcionalidad de los números utilizados en las telecomunicaciones internacionales. Un número que no cumple con este formato podría ser falso o inválido, y se considera sospechoso.

Por lo tanto, partiendo de esta y otras recomendaciones, se plantea que el operador, a través de diversas medidas y/o mecanismos técnicos, operativos, comerciales, contractuales, entre otros, pueda detectar patrones anómalos y/o potencialmente maliciosos que presenten las comunicaciones cursadas en su red y pueda evitar el progreso de llamadas y/o mensajes de texto para fines ilícitos, o en su defecto, adopte medidas que puedan advertir al usuario sobre el verdadero origen de dichas comunicaciones.

- **Las empresas operadoras implementan medidas tecnológicas para impedir que se concreten las llamadas y/o mensajes de texto con fines ilícitos.**

Esta medida considera que el operador debe contar con plataformas tecnológicas que garanticen el bloqueo de las llamadas y/o mensajes de texto que presenten ciertas características acorde a las recomendaciones internacionales.

Estas plataformas tecnológicas deben monitorear activamente el tráfico de red a través del uso de herramientas de analítica avanzada, tales como algoritmos de machine learning e inteligencia artificial, con mínima o nula intervención humana y, dependiendo de las reglas configuradas en ella, bloquear llamadas y/o mensajes de texto identificados como ilícitos. Dichas reglas o técnicas de filtrado analizan diversos patrones o características de los mensajes para determinar si este es legítimo o no. Estos patrones pueden ser hallados mediante filtros automáticos o heurísticos, análisis de listas de reputación y no implican inspección humana ni acceso deliberado al contenido privado, sino que se hallan a través de un procesamiento automatizado de metadatos y coincidencias de patrones, garantizando el principio de inviolabilidad del secreto de las comunicaciones.

La implementación, por parte de las empresas operadoras, de este tipo de plataformas tecnológicas ha sido abordada y recomendada por algunos

estándares internacionales⁴¹. Estos mecanismos son esenciales para prevenir fraudes, la defensa de las redes móviles y proteger a los usuarios de amenazas como llamadas y mensajes falsificados, phishing, smishing y suplantación de identidad.

Las plataformas tecnológicas monitorean y filtran el tráfico en tiempo real a fin de detectar patrones asociados, por ejemplo, a:

- Spoofing (suplantación del número A) y/o manipulación del número A.
- Wangiri⁴² (llamadas de corta duración).
- Tráfico desde rangos no asignados o mal formateados.
- Envío de URLs identificadas como maliciosas.

Tanto los fraudes por voz y mensajes de texto afectan la seguridad del usuario, la confianza en el servicio y la integridad de las telecomunicaciones. La implementación de estas plataformas tecnológicas permite a los operadores cumplir con obligaciones de protección al consumidor y ciberseguridad, siendo una práctica estándar en mercados regulados y recomendada como requisito por organismos técnicos y autoridades regulatorias.

Cabe precisar que, las medidas tecnológicas deben salvaguardar la inviolabilidad y el secreto de las telecomunicaciones, así como la protección de datos personales, acorde al marco normativo vigente correspondiente, para lo cual el operador debe implementar las medidas que fueran necesarias.

- **Las empresas operadoras adoptan medidas que coadyuven a determinar el origen de las llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos.**

La Recomendación UIT-T M.3362 describe los requisitos para la gestión antifraude en redes de telecomunicaciones, incluyendo la detección, monitoreo y mitigación del fraude, así como la gestión de información relacionada con fraude. Además, aborda escenarios de fraude como llamadas molestosas y llamadas y/o mensajes de texto con suplantación de identidad (*spoofing*). Esta recomendación enfatiza la importancia de compartir información sobre fraudes detectados.

El enmascaramiento del identificador de llamadas (*spoofing*), es una técnica común en fraudes. La GSMA, a través de iniciativas como Call Check, ofrece servicios para que los operadores verifiquen la probabilidad de que una comunicación sea fraudulenta o que el identificador del número A haya sido falsificado. Estas herramientas permiten a los operadores detectar y mitigar comunicaciones con identificadores enmascarados, basándose en información reportada por los usuarios y análisis técnicos.

En esa línea, se busca que los operadores, a fin de realizar un apropiado tratamiento e investigación sobre la posible existencia de llamadas y/o mensajes de texto ilícitos o sospechosos en sus redes, realicen acciones de investigación que coadyuven a determinar el origen de estas comunicaciones, en diferentes escenarios, con el objetivo de combatir el anonimato de las mismas, así como determinar responsabilidades en los casos correspondientes.

⁴¹ GSMA FS.11: recomienda el uso de plataformas tecnológicas para prevenir fraude por SMS y llamadas.

UIT-T M.3362: establece un marco para la gestión antifraude que incluye monitoreo de voz y mensajes en tiempo real.

UIT-T X.805: define la necesidad de implementar puntos de control y medidas de seguridad a lo largo de las capas de red, incluyendo plataformas tecnológicas de filtrado para comunicaciones de extremo a extremo.

⁴² https://www.europol.europa.eu/sites/default/files/documents/wangiri_final_2.pdf

Por otro lado, la retroalimentación de usuarios es clave para alimentar listas negras o sistemas de reputación de números. Esta actividad se considera una forma de detección colaborativa de amenazas. Los usuarios pueden “coadyuvar” en la detección de, por ejemplo, números que intenten obtener información o que presenten enmascaramiento, ambas acciones suelen involucrar técnicas de *spoofing* para ocultar la verdadera identidad del originador. El reporte del usuario complementa los sistemas de detección, sean manuales o automáticos, u otros que el operador considere.

- **Las empresas operadoras proporcionan y otorgan las facilidades al Ministerio de Transportes y Comunicaciones – MTC, para el acceso y monitoreo constante de sus redes, para verificar el cumplimiento de las obligaciones, según corresponda, para la correcta prestación de los servicios públicos de telecomunicaciones, salvaguardar la seguridad ciudadana en los mismos y/o en otras situaciones análogas, en beneficio y protección de los usuarios.**

El acceso que las empresas operadoras deben proporcionar al MTC a sus redes de telecomunicaciones tiene como finalidad exclusiva la fiscalización y supervisión del cumplimiento normativo, ello no supone una intervención directa en la operación de las redes ni acceso al contenido de las comunicaciones de los usuarios.

Desde un punto de vista técnico, la verificación del cumplimiento de obligaciones vinculadas a la correcta prestación de los servicios públicos de telecomunicaciones, así como a la mitigación de situaciones que puedan afectar la seguridad ciudadana o los derechos de los usuarios, requiere que la autoridad sectorial cuente con capacidad de acceso oportuno y condicionado a información técnica y a mecanismos de monitoreo debidamente sustentados en la normativa correspondiente, únicamente cuando resulte necesario y previa solicitud expresa. Dicho acceso se circunscribe a información técnica y funcionalidades de supervisión, tales como indicadores de desempeño, alarmas de red, estadísticas de tráfico, registros de eventos y resultados de sistemas de control implementados por los operadores (por ejemplo, firewalls, sistemas de detección de tráfico ilícito o plataformas de monitoreo), excluyendo en todo momento el acceso al contenido de las comunicaciones, en concordancia con el principio de secreto de las telecomunicaciones.

Asimismo, el carácter de “constante” debe entenderse no como una conexión operativa continua o intrusiva, sino como la disponibilidad técnica garantizada por parte de los operadores para que el MTC pueda ejercer sus funciones de fiscalización en el momento en que lo requiera, de manera proporcional, razonable y debidamente justificada. En tal sentido, la obligación de proporcionar facilidades de acceso no implica transferencia de control, gestión directa de la red ni responsabilidad operativa alguna por parte del MTC, sino que constituye un mecanismo habilitante de fiscalización. En este caso, la fiscalización se orienta a:

- Verificar el cumplimiento de las obligaciones normativas vigentes.
- Supervisar la implementación de medidas técnicas de protección de los usuarios.
- Coadyuvar a la detección y mitigación de situaciones que afecten la seguridad ciudadana.
- Fortalecer la transparencia y trazabilidad de las comunicaciones.

- **Los agentes vinculados en la trazabilidad de las llamadas y mensajes de texto coadyuvan y/o participan en la identificación de la trazabilidad de las referidas comunicaciones para evitar su progreso con fines ilícitos, para la correcta prestación de los servicios públicos de telecomunicaciones y/o en aras de salvaguardar la seguridad ciudadana en los mismos, en beneficio y protección de los usuarios. Para tal efecto, cumplen las disposiciones establecidas en el Reglamento de la presente norma.**

En el mercado peruano existen servicios de mensajería masiva, los mismos que se caracterizan porque los mensajes no se originan en un abonado identificado en la red móvil o fija, sino en aplicaciones, plataformas tecnológicas o sistemas informáticos pertenecientes a empresas o entidades públicas o privadas. Dichos sistemas acceden a las redes de telecomunicaciones a través de agentes o agregadores de mensajería, utilizando protocolos (SMPP) o interfaces basadas en HTTP/REST. En este modelo, el campo correspondiente al remitente del mensaje (etiqueta ingresada cuando el mensaje es generado) es definido en la capa de aplicación y, por diseño de los estándares de mensajería SMS, no cuenta con mecanismos nativos de autenticación por parte de la red del operador que cursa o termina el mensaje.

En consecuencia, la identidad real del emisor no puede ser validada directamente por el operador de telecomunicaciones. Dicho esto, desde un punto de vista técnico, los operadores móviles y/o fijos sí cuentan con la capacidad de realizar una trazabilidad funcional y operativa de la ruta de este tipo de mensajes dentro del ámbito de sus redes, mas no una identificación del remitente. Esta trazabilidad se materializa y limita a través del control de los puntos de interconexión (PDI) de mensajería, a lo largo de los cuales se recibe dicho tráfico desde operadores, agregadores o plataformas debidamente identificadas y autorizadas. En otras palabras, los operadores pueden asociar cada flujo de mensajes a un PDI específico, lo que permite identificar con precisión el operador, agregador o plataforma (en suma, el agente) que inyectó el tráfico en sus redes.

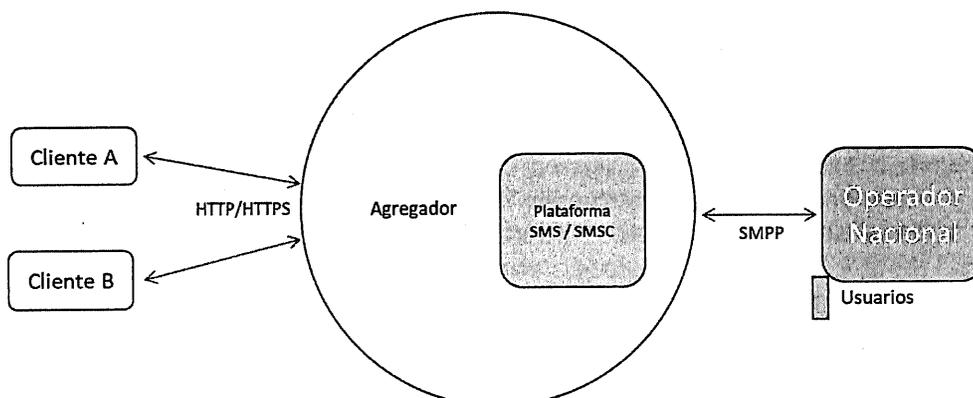
Por lo expuesto, los operadores móviles y/o fijos, técnicamente, no pueden realizar una validación de identidad final del emisor de los mensajes descritos, ni la autenticación del remitente de estos a través de parámetros técnicos tales como el identificador o etiqueta de número A o la dirección IP asociada. En este caso, la dirección IP identifica infraestructura de red y no a la entidad que originó y envió el mensaje, pudiendo además ser dinámica, compartida entre múltiples clientes o sujeta a mecanismos técnicos que permiten incrementar su disponibilidad.

Por otro lado, la trazabilidad completa de este tipo de servicio de mensajes, entendida como la capacidad de identificar al emisor real del mensaje, recae en los agregadores de mensajería que mantienen interconexión directa con los operadores de telecomunicaciones. Estos actores cuentan con la información, ya sea técnica y/o contractual, necesaria para asociar cada mensaje con una empresa, entidad o aplicación emisora específica.

En particular, los agregadores disponen, además de los contratos comerciales de volumen de tráfico, de mecanismos de autenticación de clientes, registros de conexión, configuración de remitentes autorizados y trazas de envío que permiten identificar el origen lógico del mensaje. Por ello, constituyen el punto central para la investigación y atribución de responsabilidades en caso de detección de mensajes ilícitos o fraudulentos.

Tal como se muestra en la siguiente figura, que ha sido simplificada con fines explicativos, los agentes vinculados en la comunicación pueden identificar la ruta por la cual recibieron el mensaje y/o llamadas, es decir, conocen qué entidad, directamente conectada a su red, fue la que le entregó dicha comunicación. En esa misma línea, dichos agentes conocen el origen lógico de la comunicación.

Gráfico 22. Diagrama de trazabilidad de la comunicación



Fuente: DGPRC-MTC

Por ende, tanto los operadores, como los agregadores, que en el presente ejemplo serían los agentes vinculados, se complementan con el fin de obtener la trazabilidad de las comunicaciones con fines ilícitos, por tanto, se justifica la inclusión de dichos actores dentro de la regulación del proyecto normativo.

En ese sentido, desde una perspectiva técnica – operativa o funcional, los operadores de telecomunicaciones son responsables de la detección, monitoreo y mitigación de mensajes ilícitos, fraudulentos o sospechosos dentro de sus redes, así como de la preservación de evidencia técnica, el reporte a las autoridades competentes y la coordinación necesaria para extender la investigación hasta el origen del tráfico. Por su parte, los agregadores de mensajería son responsables de autenticar a sus clientes, validar y registrar los remitentes utilizados, investigar el origen real de los mensajes ilícitos, disponer el cese inmediato del tráfico fraudulento y colaborar de manera oportuna y eficaz con los operadores y las autoridades correspondientes.

- **Reforzar las facultades de fiscalización y sanción a cargo del Ministerio de Transportes y Comunicaciones**

El artículo 5 de la LOF del MTC dispone que el MTC tiene, entre otras funciones rectoras, formular, planear, dirigir, coordinar, ejecutar, fiscalizar, supervisar y evaluar la política nacional y sectorial bajo su competencia, aplicable a todos los niveles de gobierno; así como, dictar normas y lineamientos técnicos para la adecuada ejecución, supervisión y evaluación de las políticas, la gestión de los recursos del sector, así como para el otorgamiento y reconocimiento de derechos, la sanción, la fiscalización y ejecución coactiva en materias de su competencia.

Por su parte, el numeral 2 del artículo 8 de la LOF del MTC establece que, en el marco de sus competencias el MTC cumple la función específica de, cumplir y hacer cumplir el marco normativo relacionado con su ámbito de competencia, ejerciendo la potestad sancionadora correspondiente.

De acuerdo al artículo 86 del TUO de la Ley de Telecomunicaciones es responsable de la comisión de infracciones administrativas tipificadas en la referida Ley: (1) quien realiza actividades normadas por la presente Ley careciendo de la respectiva autorización o concesión; (2) quien realiza actividades en contra de lo dispuesto en la presente Ley, aun contando en la respectiva autorización o concesión; y, (3) el usuario de los servicios de telecomunicaciones por la mala utilización de los servicios, así como por el empleo de los mismos en perjuicio de terceros.

Asimismo, el numeral 9) del artículo 87 del TUO de la Ley de Telecomunicaciones establecen que, constituyen infracciones muy graves, el incumplimiento de las normas de la referida Ley, sus reglamentos y disposiciones de la autoridad, que sean tipificadas como muy graves por el reglamento.

Asimismo, el artículo 116 del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado mediante Decreto Supremo N° 020-2007-MTC (en adelante, TUO del Reglamento de la Ley de Telecomunicaciones), establece la obligación de brindar facilidades para las inspecciones y verificaciones, entre ellas, la de proporcionar la información que el Ministerio les solicite, respecto de materias de su competencia, en la forma y plazo que este indique. Ello sin perjuicio de la obligación de presentar la información adicional que requieran para el análisis de casos específicos.

Aunado a lo anterior, el artículo 130 del TUO del Reglamento de la Ley de Telecomunicaciones, establece las diferentes obligaciones de los concesionarios de servicios públicos de telecomunicaciones, entre ellas, la de presentar al MTC la información que este le solicite, y en general brindar las facilidades para efectuar sus labores de inspección y verificación.

Conforme a la Segunda Disposición Complementaria Final de la Ley N° 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL, el MTC aplicará la escala de multas contenida en el Artículo 25 de la referida Ley.

De acuerdo al artículo 25 de la Ley N° 27336, en caso de infracciones leves puede sancionarse con amonestación escrita, de acuerdo a las particularidades del caso. Asimismo, dispone que los límites máximos de las multas correspondientes serán los siguientes: la infracción leve hasta una multa de 100 UIT, la infracción grave hasta una multa de 500 UIT, y la infracción muy grave hasta una multa de 1000 UIT.

Por su parte, el artículo 2 del ROF del MTC, establece que, el MTC ejerce jurisdicción en el ámbito nacional, regional y local, como ente rector del sector Transportes y Comunicaciones, en el marco de sus competencias exclusivas y compartidas que le otorga la ley, comprendiendo, la competencia exclusiva en infraestructura y servicios de comunicaciones y la competencia compartida en promoción de la infraestructura de telecomunicaciones y el planeamiento de los servicios de telecomunicaciones de alcance regional.

Dicho reglamento establece las siguientes competencias y funciones del órgano de línea:

“Artículo 164.- Dirección General de Fiscalizaciones y Sanciones en Comunicaciones

La Dirección General de Fiscalizaciones y Sanciones en Comunicaciones es el órgano de línea responsable de la conducción de los actos y diligencias correspondientes a la fiscalización del cumplimiento de las normas y de los títulos habilitantes en la prestación de servicios y actividades de comunicaciones; y, a la sanción, en caso de su incumplimiento; así como, al control del uso del espectro radioeléctrico. Depende del Despacho Viceministerial de Comunicaciones”.

El artículo 166 del ROF del MTC, establece que son unidades orgánicas de la Dirección General de Fiscalizaciones y Sanciones en Comunicaciones (DGFSC) las siguientes: la Dirección de Fiscalizaciones de Cumplimiento de Normativa en Comunicaciones, la Dirección de Fiscalizaciones de Cumplimiento de Títulos Habilitantes en Comunicaciones, y la Dirección de Sanciones en Comunicaciones.

En ese ámbito, se tiene el Reglamento de Fiscalización y Sanción en la prestación de servicios y actividades de comunicaciones de competencia del MTC aprobado por Decreto Supremo N° 028-2019-MTC (en adelante, Reglamento de Fiscalización y Sanción) que tiene por objeto, regular el ejercicio de las funciones de fiscalización y de sanción atribuidas al MTC de acuerdo a las normas que rigen la prestación de los servicios de comunicaciones y actividades conexas de su competencia, así como el dictado de medidas correctivas y cautelares, con el propósito de que los administrados bajo su ámbito cumplan con el marco normativo y contractual en materia de comunicaciones a nivel nacional, acorde al Artículo I de su Título Preliminar.

Atendiendo a dichas facultades y funciones, se ha identificado la necesidad de reforzar la potestad fiscalizadora, sancionadora y de imposición de medidas correctivas y cautelares del MTC, a efectos generar un cumplimiento más eficiente de las obligaciones previstas en el marco normativo.

De acuerdo a ello, se ha dispuesto que las infracciones por el incumplimiento de las obligaciones derivadas del presente Decreto Legislativo se clasifican en leves, graves y muy graves, y se tipifican en su Reglamento.

Asimismo, en el ejercicio de la actividad de fiscalización, el MTC se encuentra facultado para monitorear de manera constante las redes de las empresas operadoras y los sistemas de gestión de los agentes, para verificar el cumplimiento de las obligaciones establecidas en los artículos 4, 5, 6 y 7, según corresponda, para la correcta prestación de los servicios públicos de telecomunicaciones, salvaguardar la seguridad ciudadana en los mismos y/o en otras situaciones análogas, en beneficio y protección de los usuarios, resguardando la inviolabilidad y el secreto de las telecomunicaciones e información protegida por ley.

- **Ampliar la prohibición de las comunicaciones SPAM para los mensajes de texto**

Se ha identificado la necesidad de ampliar la prohibición de las comunicaciones SPAM para los mensajes de texto, conforme ha sido desarrollado por el legislador en el numeral 3.1.19 del Dictamen recaído en el proyecto de ley 13280/2025-PE, Proyecto de 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, a efectos de sustentar la medida aprobada.

Al respecto, el legislador ha señalado que, si consideramos que de conformidad a la Ley 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM, que en el numeral 58.3 garantiza al consumidor el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones, y de conformidad a su única disposición complementaria final se otorgue numeración especial a los proveedores los métodos de seguridad y técnicas de validación para que los usuarios puedan identificar las llamadas que reciben, así como los mecanismos de validación de información transmitida, que si bien está referido a las llamadas spam, la identificación de debería aplicarse para toda llamada o mensaje de texto.

En ese sentido, resulta necesario modificar la Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM para mensajes de texto.

Asimismo, para el cumplimiento de la mencionada normativa adicional, es necesario la participación del Ministerio de Transportes y Comunicaciones y el INDECOPI para ejercer la facultad fiscalizadora y sancionadora, en el ámbito de sus funciones y competencias.

5.3. Análisis sobre la necesidad, viabilidad y oportunidad de la norma (Legal)

a) Análisis de necesidad de la norma

La necesidad del Marco Normativo se sustenta en que mediante su aprobación se contribuirá con la seguridad nacional en el ámbito del orden interno, orden público y seguridad ciudadana, evitando que se establezcan comunicaciones ilícitas a través de llamadas y mensajes de texto, lo cual, a su vez, coadyuvará a disminuir la comisión de ilícitos penales vinculados al uso de los servicios de telecomunicaciones, como el fraude, la extorsión, sicariato, secuestro, criminalidad organizada, entre otros.

Asimismo, las medidas que se plantean están orientadas a que, a través de configuraciones y habilitaciones técnicas en las redes de telecomunicaciones, de mecanismos de investigación, de coordinación, verificación y de implementación de plataformas tecnológicas, se logre evitar que los usuarios reciban llamadas y mensajes de texto con fines ilícitos.

b) Análisis de viabilidad de la norma

El Proyecto de Norma resulta viable, toda vez que se han formulado acorde al marco normativo vigente, tal como lo dispuesto en la Constitución Política del Perú, el TUO de la Ley de Telecomunicaciones, el TUO del Reglamento de la Ley de Telecomunicaciones, la LOF del MTC, entre otras normas, según lo desarrollado en la presente exposición de motivos en las secciones III. Antecedentes y IV. Marco jurídico y las habilitaciones en cuyo ejercicio se dicta.

Asimismo, las medidas establecidas se consideran factibles de ser aplicadas técnicamente por las empresas operadoras y agentes vinculados, además de ser las más eficientes dada la situación actual de la problemática relacionada a las comunicaciones ilegales mediante llamadas y mensajes de texto, los costos que les corresponde asumir a los actores involucrados y los diferentes

factores que influyen en dicha problemática. En ese sentido, resulta viable que se emita el Proyecto de Norma.

c) Análisis de oportunidad de la norma

La emisión de la presente norma se considera oportuna puesto que, debido a que la problemática de las comunicaciones ilegales mediante llamadas y mensajes de texto acarrea distintos perjuicios para el orden interno, orden público y seguridad ciudadana, urge la adopción de medidas orientadas a prevenir, controlar y/o mitigar la misma, por lo que es oportuna la emisión del Proyecto de Norma que precisamente contiene disposiciones dirigidas a enfrentar la mencionada problemática.

d) Precisión del nuevo estado que genera la norma

Conforme se señaló anteriormente, existe un incremento de distintos tipos de actos ilícitos, tales como fraudes, estafas, extorsiones, amenazas o suplantación de identidad, que utilizan los servicios de telefonía y mensajes de texto (SMS) como medio delictivo. En ciertos casos, para cometer dichos ilícitos, se realiza el enmascaramiento del número de origen, tanto en llamadas como en mensajes de texto.

Actualmente, nuestra legislación no cuenta con un marco normativo que establezca reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana. Dicha omisión constituye una desventaja para permitir la identificación y/o veracidad del número de origen de la comunicación, así como, evitar o mitigar prácticas de enmascaramiento o manipulación del recurso numérico que conlleven al progreso de llamadas y mensajes de texto ilícitos y los efectos negativos que generan en la sociedad, propósito que se busca implementar con el presente decreto legislativo.

En ese sentido, se busca la reducción de la inseguridad ciudadana mediante el control efectivo del recurso numérico, así como, promover la identificación precisa y trazabilidad de cada comunicación realizada. Por su parte, generar confianza permitiendo la mitigación de riesgos de enmascaramiento y manipulación de identidad. Finalmente, se implementan medidas de prevención, para el bloqueo estratégico al progreso de llamadas y mensajes con fines ilícitos.

Por lo que, sobre la base de dicha explicación, se propone establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana.

e) Objetivo relacionado con el problema público identificado

El objetivo principal del presente Decreto Legislativo, es reducir progresivamente la incidencia de llamadas y mensajes de texto con fines ilícitos, alcanzando una reducción acumulada de por lo menos 40% al año

2030, mediante el establecimiento de reglas y mecanismos que fortalezcan la trazabilidad y el uso adecuado del recurso de numeración. Este objetivo se orienta, a su vez, a fines específicos tales como: (i) incrementar la protección de la población frente a las comunicaciones con fines ilícitos; (ii) Incrementar la confianza de los servicios públicos de telecomunicaciones; (iii) fortalecer la capacidad institucional del estado; y (iv) reducir los impactos asociados a las pérdidas económicas derivadas de la vulneración de datos personales, ocasionadas por comunicaciones con fines ilícitos a través de llamadas telefónicas y mensajes de texto en las redes de telecomunicaciones. De esta manera, la propuesta normativa guarda coherencia directa entre el problema identificado, los objetivos perseguidos y las medidas regulatorias planteadas.

VI. Propuesta normativa

Del Capítulo I: Disposiciones Generales

Artículo 1 del decreto legislativo:

El desarrollo acelerado de las tecnologías de la información y las comunicaciones ha permitido una expansión sin precedentes en la conectividad y el acceso a los servicios de telecomunicaciones. Sin embargo, este mismo progreso ha sido aprovechado de manera indebida por organizaciones y personas que utilizan las redes de telecomunicaciones para la comisión de actividades ilícitas, tales como fraudes telefónicos, estafas mediante mensajes de texto (SMS), suplantación de identidad y otras prácticas que vulneran la confianza de los usuarios y afectan la seguridad del país.

Ante este escenario, resulta indispensable que el Estado, adopte medidas normativas, técnicas y operativas que fortalezcan la integridad y la confiabilidad de las redes públicas de telecomunicaciones, protegiendo tanto a los usuarios y entidades como a la infraestructura crítica nacional.

El presente marco normativo se enmarca en dicho propósito, busca establecer medidas y obligaciones orientadas a prevenir, detectar y mitigar las comunicaciones ilícitas que utilizan las redes de telecomunicaciones como medio para su ejecución, coadyuvando así a una mayor transparencia, trazabilidad e identificación en las llamadas y mensajes de texto.

En ese sentido, en el artículo bajo análisis se establece que el presente Decreto Legislativo tiene por objeto establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana.

Artículo 2 del decreto legislativo:

Conforme a la problemática descrita en los considerandos precedentes, resulta necesaria la intervención del estado para establecer obligaciones claras en materia de autenticación, trazabilidad, validación de numeración y reporte de las mismas, garantizando que los operadores adopten medidas proporcionales y efectivas que permitan proteger al usuario final, preservar la integridad de la red y asegurar la confianza en el ecosistema digital nacional.

En ese sentido, el artículo 2 del Decreto Legislativo establece que el referido marco normativo tiene como finalidad permitir la identificación y/o veracidad del número de origen de la comunicación, así como, evitar o mitigar prácticas de enmascaramiento o manipulación del recurso numérico que conlleva al progreso de llamadas y mensajes de texto ilícitos y los efectos negativos que generan en la sociedad.

Artículo 3 del decreto legislativo:

Conforme a lo señalado en el numeral 5.3 de la presente exposición de motivos, la presente norma es aplicable a las empresas operadoras y los agentes vinculados en la trazabilidad de las llamadas y mensajes de texto.

Asimismo, el numeral 3.2 establece que, para efectos del presente proyecto de Decreto Legislativo, se considera como agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto a toda persona natural o persona jurídica que interviene en el enrutamiento o encaminamiento⁴³ de las comunicaciones y/o cuenta con información de la trazabilidad de las mismas.

Conforme a lo desarrollado en el numeral 5.3 de la presente Exposición de Motivos, los operadores móviles y/o fijos no se encuentran en capacidad técnica de validar la identidad final del emisor de los mensajes ni de autenticar al remitente a partir de parámetros como el número A o la dirección IP, en tanto estos identifican infraestructura de red y no a la entidad que origina el envío, pudiendo además ser dinámicos, compartidos o sujetos a mecanismos técnicos que dificultan su atribución.

En contraste, la trazabilidad efectiva del servicio de mensajería recae en los agentes vinculados que mantienen interconexión directa con los operadores, quienes disponen de información técnica y contractual que permite asociar cada mensaje con un emisor específico.

De acuerdo a ello, estos actores se constituyen en el punto central para la autenticación de clientes, la validación y registro de remitentes, la investigación del origen de mensajes ilícitos, el cese del tráfico fraudulento y la colaboración oportuna con los operadores y las autoridades competentes.

En tal sentido, tanto los operadores, como los agentes vinculados, se complementan con el fin de obtener la trazabilidad de las comunicaciones con fines ilícitos, por tanto, se justifica la inclusión de dichos actores dentro de la regulación del proyecto normativo.

Del Capítulo II: Obligaciones de las empresas operadoras de servicios públicos de telecomunicaciones para identificar la trazabilidad de las comunicaciones y evitar su progreso con fines ilícitos

Artículo 4 del decreto legislativo:

El artículo 4 de la presente norma contempla las obligaciones generales que deberán cumplir las empresas operadoras de servicios públicos de telecomunicaciones con relación al uso inadecuado del recurso numérico y para evitar las llamadas y mensajes de texto con fines ilícitos, conforme a lo siguiente:

⁴³ Conforme se describe en la Recomendación ITU-T E.170.

- Las empresas operadoras adoptan medidas y/o mecanismos técnicos y/u operativos para evitar el progreso de llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos; así como, para permitir a los abonados y usuarios advertir sobre dichas comunicaciones.

Al respecto, cabe indicar que, diversas organizaciones, tales como, UIT, ETSI, FCC, GSMA y otras, han desarrollado distintas recomendaciones relacionadas a la gestión de tráfico fraudulento, prevención de suplantación de comunicaciones, el formato que debe seguir un número telefónico internacional, entre otros. Todas estas recomendaciones están orientadas a prevenir llamadas y/o mensajes de texto ilícitos y serán recogidas de forma referencial, a efectos de que las empresas operadoras las tomen en cuenta para sus labores de monitoreo y/o investigación con el propósito de asegurar la trazabilidad de las comunicaciones, según corresponda.

Por lo tanto, partiendo de esta y otras recomendaciones, se plantea que el operador, a través de diversas medidas y/o mecanismos técnicos, operativos, comerciales, contractuales, entre otros, pueda detectar patrones anómalos y/o potencialmente maliciosos que presenten las comunicaciones cursadas en su red y pueda evitar el progreso de llamadas y/o mensajes de texto para fines ilícitos, o en su defecto, adopte medidas que puedan advertir al usuario sobre el verdadero origen de dichas comunicaciones.

- Las empresas operadoras implementan medidas tecnológicas para impedir que se concreten comunicaciones con fines ilícitos. Asimismo, dichas empresas podrán implementar medidas adicionales a lo dispuesto de forma precedente.

Esta medida considera que el operador debe contar con plataformas tecnológicas que garanticen el bloqueo de las llamadas y/o mensajes de texto que presenten ciertas características acorde a las recomendaciones internacionales.

Estas plataformas tecnológicas deben monitorear y filtrar el tráfico en tiempo real a fin de detectar patrones asociados, por ejemplo, a:

- Spoofing (suplantación del número A) y/o manipulación del número A.
 - Wangiri (llamadas de corta duración).
 - Tráfico desde rangos no asignados o mal formateados.
 - Envío de URLs identificadas como maliciosas.
- Las empresas operadoras adoptan medidas que coadyuven a determinar el origen de las llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos.

Al respecto, se busca que los operadores, a fin de realizar un apropiado tratamiento e investigación sobre la posible existencia de llamadas y/o mensajes de texto ilícitos o sospechosos en sus redes, realicen acciones de investigación que coadyuven a determinar el origen de estas comunicaciones, en diferentes escenarios, con el objetivo de combatir el anonimato de las mismas, así como determinar responsabilidades en los casos correspondientes.

- Asimismo, se dispone que las medidas, mecanismos y/o disposiciones mencionadas anteriormente, son desarrolladas y determinadas en el Reglamento del Decreto Legislativo.

Artículo 5 del decreto legislativo

El **artículo 5** de la presente norma dispone que las empresas operadoras proporcionan y otorgan las facilidades al Ministerio de Transportes y Comunicaciones – MTC, para el acceso y monitoreo constante de sus redes, para verificar el cumplimiento de las obligaciones establecidas en el artículo 4, según corresponda, para la correcta prestación de los servicios públicos de telecomunicaciones, salvaguardar la seguridad ciudadana en los mismos y/o en otras situaciones análogas, en beneficio y protección de los usuarios, resguardando la inviolabilidad y el secreto de las telecomunicaciones.

Así, conforme a lo desarrollado en el numeral 5.3 de la presente exposición de motivos, diversas organizaciones, tales como, UIT, ETSI, FCC, GSMA y otras, han desarrollado distintas recomendaciones relacionadas a la gestión de tráfico fraudulento, prevención de suplantación de comunicaciones, el formato que debe seguir un número telefónico internacional, entre otros.

De acuerdo a ello, resulta pertinente señalar que todas estas recomendaciones están orientadas a prevenir llamadas y/o mensajes de texto ilícitos y serán recogidas de forma referencial, a efectos de que las empresas operadoras las tomen en cuenta para sus labores de monitoreo y/o investigación con el propósito de asegurar la trazabilidad de las comunicaciones, según corresponda.

En este contexto, se entiende que la adecuada gestión técnica de las redes por parte de las empresas operadoras constituye un elemento esencial para garantizar la seguridad de los usuarios, así como para prevenir afectaciones a las redes de telecomunicaciones, por lo cual, resulta necesario que las empresas operadoras proporcionen y otorguen al MTC el acceso y monitoreo constante de sus redes, para verificar el cumplimiento de sus obligaciones.

Del Capítulo III: Obligaciones de los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto

Artículo 6 del decreto legislativo

El **artículo 6** dispone que los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto coadyuvan y/o participan en la identificación de la trazabilidad de las referidas comunicaciones para evitar su progreso con fines ilícitos, para la correcta prestación de los servicios públicos de telecomunicaciones y/o en aras de salvaguardar la seguridad ciudadana en los mismos, en beneficio y protección de los usuarios. Para tal efecto, deben cumplir con las disposiciones establecidas en el Reglamento del decreto legislativo.

Asimismo, se dispone que el Ministerio de Transportes y Comunicaciones está facultado para establecer, a través del Reglamento del presente Decreto Legislativo, las condiciones y/o requisitos aplicables a los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto, así como, para establecer las obligaciones aplicables a estos

Conforme a lo desarrollado en el numeral 5.3 de la presente exposición de motivos, los operadores móviles y/o fijos, técnicamente, no pueden realizar una

validación de identidad final del emisor de los mensajes descritos, ni la autenticación del remitente de estos a través de parámetros técnicos tales como el identificador o etiqueta de número A o la dirección IP asociada. En este caso, la dirección IP identifica infraestructura de red y no a la entidad que originó y envió el mensaje, pudiendo además ser dinámica, compartida entre múltiples clientes o sujeta a mecanismos técnicos que permiten incrementar su disponibilidad.

Por otro lado, la trazabilidad completa de este tipo de servicio de mensajes, entendida como la capacidad de identificar al emisor real del mensaje, recae en los agregadores de mensajería que mantienen interconexión directa con los operadores de telecomunicaciones. Estos actores cuentan con la información, ya sea técnica y/o contractual, necesaria para asociar cada mensaje con una empresa, entidad o aplicación emisora específica.

En particular, los agregadores disponen, además de los contratos comerciales de volumen de tráfico, de mecanismos de autenticación de clientes, registros de conexión, configuración de remitentes autorizados y trazas de envío que permiten identificar el origen lógico del mensaje. Por ello, constituyen el punto central para la investigación y atribución de responsabilidades en caso de detección de mensajes ilícitos o fraudulentos.

Bajo dicho contexto, los agregadores de mensajería son responsables de autenticar a sus clientes, validar y registrar los remitentes utilizados, investigar el origen real de los mensajes ilícitos, disponer el cese inmediato del tráfico fraudulento y colaborar de manera oportuna y eficaz con los operadores y las autoridades correspondientes.

Artículo 7 del decreto legislativo

El **artículo 7** del proyecto normativo, establece que los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto otorgan las facilidades al MTC, para el acceso y monitoreo constante de sus sistemas de gestión, para verificar el cumplimiento de las obligaciones establecidas en el artículo 6, según corresponda, resguardando la inviolabilidad y el secreto de las telecomunicaciones.

Al respecto, cabe señalar que la trazabilidad completa del servicio de mensajes, entendida como la capacidad de identificar al emisor real del mensaje, recae en los agregadores de mensajería que mantienen interconexión directa con los operadores de telecomunicaciones. Estos actores cuentan con la información, ya sea técnica y/o contractual, necesaria para asociar cada mensaje con una empresa, entidad o aplicación emisora específica.

En particular, los agregadores disponen, además de los contratos comerciales de volumen de tráfico, de mecanismos de autenticación de clientes, registros de conexión, configuración de remitentes autorizados y trazas de envío que permiten identificar el origen lógico del mensaje. Por ello, constituyen el punto central para la investigación y atribución de responsabilidades en caso de detección de mensajes ilícitos o fraudulentos.

Tal como se muestra en el gráfico 22 de la presente Exposición de Motivos, los agentes vinculados en la comunicación pueden identificar la ruta por la cual recibieron el mensaje y/o llamadas, es decir, conocen qué entidad, directamente conectada a su red, fue la que le entregó dicha comunicación. En esa misma línea, dichos agentes conocen el origen lógico de la comunicación.

En ese sentido, tanto los operadores del servicio público de telecomunicaciones y los agentes vinculados, se complementan con el fin de obtener la trazabilidad de las comunicaciones con fines ilícitos, por tanto, se justifica la inclusión de dichos actores dentro de la regulación del proyecto normativo a través del artículo 7.

Del Capítulo IV: Potestad fiscalizadora y sancionadora

Artículo 8 del decreto legislativo

El **artículo 8** del proyecto normativo, se encuentra relacionado a la **supervisión y fiscalización** que la Dirección General de Fiscalizaciones y Sanciones en Comunicaciones (DGFSC) del MTC, tiene a su cargo la supervisión y fiscalización del cumplimiento de lo establecido en la presente norma, en el marco de sus competencias, para lo cual rige lo establecido en la Ley y su Reglamento; así como, el Reglamento de Fiscalización Sanción.

Asimismo, con relación a las **infracciones y sanciones** se dispone que, las infracciones en las que incurran las empresas operadoras y los agentes vinculados a la trazabilidad de las llamadas y/o mensajes de texto, previstas en los artículos 4 y 6 del proyecto de Decreto Legislativo, respectivamente, se clasifican en leves, graves y muy graves, y se tipifican en su Reglamento.

Al respecto, cabe precisar que el Ministerio de Transportes y Comunicaciones cuenta con atribuciones expresas de fiscalización, supervisión y sanción en materia de telecomunicaciones, conforme a su Ley de Organización y Funciones, al TUO de la Ley de Telecomunicaciones y su Reglamento. Dicho marco reconoce al MTC como ente rector del sector y le atribuye la potestad de dictar normas, fiscalizar su cumplimiento y ejercer la potestad sancionadora respecto de los administrados bajo su competencia.

Asimismo, el TUO de la Ley de Telecomunicaciones y su Reglamento establecen obligaciones específicas para los concesionarios y demás agentes del sector, incluyendo el deber de brindar facilidades para las labores de inspección, verificación y provisión de información requerida por la autoridad. Estas obligaciones se complementan con un régimen de infracciones y sanciones que habilita al MTC a clasificar conductas infractoras y aplicar medidas correctivas, cautelares y sanciones, conforme a los principios de legalidad y tipicidad.

En ese contexto, resulta necesario reforzar y precisar normativamente el ejercicio de la potestad fiscalizadora y sancionadora del MTC respecto de las obligaciones previstas en el presente Decreto Legislativo, particularmente en materia de trazabilidad de comunicaciones. Ello permitirá asegurar un cumplimiento efectivo del marco regulatorio, fortalecer la protección de los usuarios y contribuir a la seguridad ciudadana, garantizando en todo momento la inviolabilidad y el secreto de las telecomunicaciones y de la información protegida por ley.

Artículo 9 del decreto legislativo

El **artículo 9** del proyecto normativo, establece que la implementación del presente Decreto Legislativo se financia con el presupuesto institucional del Ministerio de Transportes y Comunicaciones sin demandar recursos adicionales al Tesoro Público, conforme a lo establecido en las leyes anuales de presupuesto del sector público.

En materia presupuestal, el artículo 9 del proyecto tiene por finalidad precisar el régimen de financiamiento aplicable a la implementación de las medidas orientadas al adecuado uso de la numeración, la trazabilidad y la reducción del anonimato en llamadas y mensajes de texto, evitando que el Decreto Legislativo sea interpretado como una habilitación implícita para generar gastos no previstos o como un mandato abierto de asignación de recursos adicionales. Ello es concordante con la Segunda Disposición Complementaria Final de la Ley N° 32527 que establece que las habilitaciones y modificaciones presupuestarias que requieran las materias delegadas se tramitan conforme a la Ley de Presupuesto y que las medidas cuya implementación demande recursos económicos “se ejecutan con cargo al presupuesto aprobado para cada sector”, bajo responsabilidad.

En ese sentido, el artículo 9 dispone que las acciones a cargo del Ministerio de Transportes y Comunicaciones se financian con su presupuesto institucional, sin demandar recursos adicionales al Tesoro Público, lo cual es coherente con el marco de programación y ejecución presupuestaria vigente. Ello se sustenta en que la norma propuesta no crea nuevas entidades, programas presupuestales ni unidades orgánicas a cargo del Estado, sino que se apoya en funciones de supervisión, fiscalización y control ya asignadas al MTC. Asimismo, las principales medidas técnicas y operativas para prevenir y reducir las comunicaciones ilícitas recaen en las empresas operadoras y en los agentes vinculados a la trazabilidad de las comunicaciones, conforme a lo que se desarrolle reglamentariamente, por lo que la implementación de la norma no genera impacto presupuestal adicional ni compromete la sostenibilidad del Presupuesto del Sector Público.

Primera Disposición Complementaria Final

Se dispone que el proyecto normativo entra en vigencia a partir del día siguiente de la publicación del Reglamento de la presente norma en el diario oficial El Peruano

Segunda Disposición Complementaria Final

Se dispone que un plazo máximo de noventa (90) días hábiles contados desde la publicación del presente Decreto Legislativo, el Poder Ejecutivo, con refrendo del MTC aprueba mediante decreto supremo la norma reglamentaria.

Primera disposición complementaria modificatoria del decreto legislativo:

La presente disposición establece la modificación Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM.

En tal sentido, se efectúa la modificación antes señalada en virtud a la necesidad de ampliar la prohibición de las comunicaciones SPAM para los mensajes de texto, conforme ha sido desarrollado por el legislador en el numeral 3.1.19 del Dictamen recaído en el proyecto de ley 13280/2025-PE, Proyecto de 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, a efectos de sustentar la medida aprobada.

Al respecto, el legislador ha señalado que, si consideramos que de conformidad a la Ley 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del

Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM, que en el numeral 58.3 garantiza al consumidor el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones, y de conformidad a su única disposición complementaria final se otorgue numeración especial a los proveedores los métodos de seguridad y técnicas de validación para que los usuarios puedan identificar las llamadas que reciben, así como los mecanismos de validación de información transmitida, que si bien está referido a las llamadas spam, la identificación de debería aplicarse para toda llamada o mensaje de texto.

En ese sentido, resulta necesario incorporar la modificación de la Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM para mensajes de texto.

Asimismo, para el cumplimiento de la mencionada normativa adicional, es necesario la participación del Ministerio de Transportes y Comunicaciones y el INDECOPI para ejercer la facultad fiscalizadora y sancionadora, en el ámbito de sus funciones y competencias.

VII. Análisis de impactos cuantitativos y/o cualitativos de la norma

Teniendo en cuenta, la creciente proliferación de llamadas y mensajes de texto con fines ilícitos, representa un problema de seguridad pública que afecta a millones de usuarios en el país, comprometiendo la confianza en los servicios de telecomunicaciones.

Asimismo, con el aumento de la conectividad se han incrementado amenazas a la seguridad y la privacidad de individuos y empresas.

Por lo tanto, para responder de forma efectiva, en esta sección se aborda la identificación de los costos y beneficios asociados; además, concluye con un análisis multicriterio que nos permite seleccionar con mayor efectividad la alternativa más adecuada, no solo en términos de efectividad, sino también de su impacto económico, viabilidad técnica e institucional, y sostenibilidad a largo plazo.

Alternativa 1: Statu quo

La situación actual se mantiene, es decir, no existen facultades sancionadoras ni fiscalizadoras claras para el MTC, las obligaciones técnicas no están unificadas y los operadores no tienen un marco legal claro para identificar la trazabilidad de las comunicaciones, combatir su anonimato y evitar las comunicaciones ilícitas.

Para el Estado

Beneficios:

- Mantener la situación actual no genera costos regulatorios adicionales.
- Evita costos inmediatos de diseño, implementación y supervisión adicionales (capacitaciones, herramientas de monitoreo, protocolos, etc.).
- Las entidades continúan trabajando con los instrumentos actuales.

Costos:

- El Estado no cuenta con obligaciones homogéneas de gestión de red, ni con trazabilidad sistemática del origen de las comunicaciones ilícitas, es decir, no cuenta con herramientas legales para enfrentar esta problemática.
- El Estado mantiene un rol reactivo, dependiendo de denuncias, investigaciones penales y esfuerzos aislados.
- Se dificulta la generación de información estructurada, tales como estadísticas, patrones, análisis de riesgo, lo que limita el diseño de futuras políticas públicas.
- Persistencia de altos costos en seguridad ciudadana.
- Incremento progresivo en la carga del sistema judicial y policial por denuncias de fraude y otras modalidades delictivas basadas en telecomunicaciones.
- Pérdida de efectividad y legitimidad institucional, ya que la recurrencia del fenómeno refuerza la percepción de incapacidad estatal para contener la criminalidad digital asociada a telecomunicaciones que conlleva a un costo reputacional institucional.
- Perú continúa rezagado frente a estándares internacionales de lucha contra las llamadas y mensajes de texto fraudulentos.
- Se reduce la capacidad preventiva del sistema de telecomunicaciones, permitiendo que estructuras delictivas utilicen canales legítimos para fines ilícitos.

Para las empresas operadoras y agentes vinculados

Beneficios:

- No existen exigencias legales para combatir el anonimato de las comunicaciones y evitar las comunicaciones ilícitas.
- No se generan inversiones de adecuación tecnológica ni costos regulatorios explícitos en el corto plazo.
- Mantienen flexibilidad total para aplicar medidas según su propio criterio y priorización.

Costos

- Exposición continua a vulneraciones de red y pérdida de reputación y confianza frente a los usuarios.
- Mientras se mantenga el volumen de comunicaciones ilícitas, las empresas seguirán afrontando reclamos, quejas, solicitudes de bloqueo, aclaraciones, etc.
- Afectación de la imagen de marca, la satisfacción del cliente y la fidelización, lo cual puede traducirse en pérdidas de ingresos y mayores tasas de abandono de clientes.
- Costos operativos por gestionar casos de fraude sin herramientas técnicas.
- Pérdida de confianza de usuarios y empresas.
- Ante la persistencia del problema, en el futuro podrían exigirse soluciones más costosas e invasivas, sin un diseño gradual ni flexible.
- Algunos invierten en mitigación y otros no, lo que genera asimetría debilitando la efectividad sistémica.

- Se posponen ajustes, pero incrementa el riesgo de regulaciones más duras a futuro.

Para la población

Beneficios:

- No se identifican beneficios para la población.

Costos:

- Persistencia de altos niveles de llamadas y mensajes de texto con fines ilícitos.
- La población continúa asumiendo pérdidas económicas directas, consecuencia de fraudes, estafas, extorsiones, entre otras actividades ilícitas que involucren las telecomunicaciones.
- Aumento de costos psicológicos y emocionales, como consecuencia de ansiedad, inseguridad y desconfianza al recibir llamadas o mensajes de texto desconocidos.
- Desincentivo al uso de canales digitales y de servicios financieros por la pérdida de confianza en el uso de los servicios de telecomunicaciones de voz y mensajería.

Alternativa 2: No regulatoria (autorregulación + acuerdos voluntarios + campañas)

Esta alternativa consiste en implementar acuerdos voluntarios entre las empresas operadoras y agentes vinculados, tales como, mejores prácticas (de carácter técnico), coordinación para bloqueos/alertas, e intercambio de información; así como, campañas de información y educación al usuario lideradas por las empresas operadoras y/o el Estado, sin imponer obligaciones legales coercitivas ni régimen sancionador específico asociado al nuevo marco.

Para el Estado

Beneficios:

- Menor costo y menor complejidad jurídica que una intervención regulatoria, ya que puede ponerse en marcha más rápido mediante mesas técnicas, convenios, guías y campañas.
- Permite generar “aprendizaje” y diagnóstico operacional, lo que será útil si luego se regula con mayor precisión.

Costos

- Existe una efectividad incierta, ya que, al no haber coerción ni incentivos sancionadores, el cumplimiento puede ser parcial, desigual o reversible, lo que genera un riesgo alto de free-riding.
- El Estado no cuenta con obligaciones homogéneas de gestión de red, ni con trazabilidad sistemática del origen de las comunicaciones ilícitas, es decir, no cuenta con herramientas legales para enfrentar esta problemática.

- La coordinación voluntaria tiene límites ante actores con capacidades heterogéneas o incentivos distintos, por lo que, el Estado puede terminar asumiendo costos de coordinación permanentes.
- Campañas educativas reducen vulnerabilidad, pero no resuelven el problema de fondo cuando el emisor ilícito puede falsificar origen, es decir, mitigan conducta del usuario, no necesariamente la capacidad del delincuente.
- Perú continúa rezagado frente a estándares internacionales de lucha contra las llamadas y mensajes de texto fraudulentos.

Para las empresas operadoras y agentes vinculados

Beneficios:

- Flexibilidad para diseñar soluciones sin rigidez normativa, pueden priorizar acciones o estrategias sencillas y de bajo esfuerzo, tales como, filtros, listas negras, alertas, y adaptarlas rápidamente.
- Leve mejora reputacional por acciones visibles con campañas y coordinaciones sectoriales.
- Menor riesgo de sanción por incumplimiento normativo, ya que, no hay obligación legal nueva.

Costos

- Costos operativos voluntarios a través de inversiones y gastos en herramientas y personal sin garantía de que todos los actores hagan lo mismo, sin embargo, se mantiene el problema de coordinación y el riesgo de free-riding.
- Posible subinversión, ya que, cada actor puede invertir menos de lo socialmente óptimo porque los beneficios son difusos, produciéndose externalidades positivas no internalizadas.
- Si la estrategia se centra en campañas, puede trasladar parte del “costo de protección” al usuario (tiempo, esfuerzos de verificación), lo que no siempre es eficaz.

Para la población

Beneficios:

- Campañas pueden reducir pérdidas económicas en ciertos segmentos (usuarios más vulnerables) al mejorar reconocimiento de estafas.
- Algunas medidas voluntarias pueden reducir parte del tráfico malicioso, especialmente el más repetitivo.

Costos

- Protección desigual, ya que, los usuarios dependen de qué operador o agente implemente algo, y con qué calidad.
- Mayor carga sobre el usuario, puesto que, se enfatiza “autocuidado” sin asegurar integridad del origen (cuando hay spoofing, el usuario sigue viendo señales engañosas).
- Resultados potencialmente limitados en fraudes sofisticados, ya que, la persistencia del fenómeno erosiona confianza igualmente.

Alternativa 3: Alternativa regulatoria

Esta alternativa consiste en la implementación de reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, con la finalidad de evitar el anonimato y la realización de comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones.

Esta alternativa introduce un marco regulatorio obligatorio y exigible aplicable a las empresas operadoras de servicios públicos de telecomunicaciones y a los agentes vinculados en la trazabilidad de las llamadas y mensajes de texto, estableciendo obligaciones específicas de carácter técnico y operativo orientadas a: (i) prevenir el uso inadecuado del recurso de numeración; (ii) permitir la identificación y veracidad del número de origen de las comunicaciones, y (iii) coadyuvar a la trazabilidad de las llamadas y mensajes con indicios de ilicitud.

En particular, la norma dispone que las empresas operadoras adopten medidas y/o mecanismos técnicos y operativos para evitar el progreso de llamadas y mensajes de texto con fines ilícitos, implementar medidas tecnológicas de bloqueo o impedimento de dichas comunicaciones y adoptar acciones que permitan determinar su origen, conforme a lo que se desarrolle en el Reglamento. Asimismo, se establecen obligaciones para los agentes vinculados que participan en la cadena de cursado y trazabilidad de las comunicaciones, a fin de asegurar una respuesta integral y coordinada frente al problema.

Adicionalmente, se otorga al Ministerio de Transportes y Comunicaciones potestades de fiscalización, sanción y aplicación de medidas correctivas y cautelares, así como facultades de monitoreo de redes y sistemas de gestión, garantizando el respeto al secreto e inviolabilidad de las telecomunicaciones. Este esquema busca transitar de un enfoque predominantemente reactivo hacia un enfoque preventivo y sistémico, alineado con la lucha contra la inseguridad ciudadana y la protección de los usuarios.

Para el Estado

Beneficios:

- Fortalecimiento del marco normativo con rango de ley, ya que en este caso el Estado dispone de una norma con jerarquía suficiente para establecer obligaciones claras y exigibles a operadores y agentes vinculados, así como, atribuir de manera plena y expresa la potestad de fiscalizar, sancionar e imponer medidas correctivas y cautelares al MTC, lo que incrementa significativamente la efectividad y legitimidad de la intervención estatal.
- Fortalece la capacidad preventiva del Estado, al establecer obligaciones claras y verificables que reducen la dependencia de acciones ex post como denuncias e investigaciones posteriores.
- La norma permite construir una arquitectura regulatoria moderna, alineada con recomendaciones de UIT, GSMA y buenas prácticas internacionales.
- Mayor efectividad en la reducción de llamadas y mensajes de texto ilícitos, ya que la combinación de obligaciones técnicas, trazabilidad, fiscalización y sanciones graduadas genera un marco coherente de incentivos para el cumplimiento, lo que se traduce en una reducción más significativa de

comunicaciones ilícitas y, por tanto, de manera indirecta de la carga sobre seguridad, justicia y defensa del consumidor.

- Mejora la efectividad institucional frente a la criminalidad digital, a través del acceso y/o monitoreo a las redes del operador para una mayor verificación del cumplimiento de las obligaciones y en aras de salvaguardar la seguridad ciudadana.
- Generación de inteligencia regulatoria y capacidad de reacción, ya que se habilita de manera más efectiva al MTC a estructurar, vía reglamento, reportes, trazas técnicas y mecanismos de seguimiento a las comunicaciones ilícitas.
- Mejor coordinación interinstitucional y liderazgo sectorial, por lo que, el marco legal claro facilita que el MTC lidere la política frente a las comunicaciones ilícitas, pudiendo articular esfuerzos con otras entidades públicas, de ser necesario, lo que incrementa la coherencia de la respuesta estatal.

Costos

- Costos de implementación normativa y fiscalización.

Para las empresas operadoras y agentes vinculados

Beneficios:

- La implementación de medidas técnicas y operativas contra comunicaciones ilícitas permite que el operador se posicione como “red segura” o “proveedor responsable”, lo que refuerza la lealtad de clientes y la percepción de valor.
- Certeza jurídica y estándares claros de cumplimiento, lo que permite planificar inversiones y procesos internos con mayor seguridad.
- Reducción progresiva del tráfico ilícito y sus costos asociados, al establecer un marco robusto de obligaciones para evitar las comunicaciones ilícitas.
- Disminuye reclamos, quejas y carga de atención al cliente, a medida que disminuye el volumen de comunicaciones ilícitas cursadas por las redes.
- Competencia más simétrica, ya que un marco uniforme y exigible evita que algunos operadores, por falta de sanción creíble, inviertan menos en medidas de seguridad y se conviertan en refugios de tráfico ilícito. En ese contexto, esto genera un campo de juego más parejo entre empresas y reduce incentivos perversos.
- Reduce la exposición reputacional de los operadores.
- Mejora reputacional con clientes corporativos y usuarios finales.

Costos

- Costos de adecuación tecnológica, operativa y de cumplimiento, ya que la empresa debe implementar medidas y mecanismos técnicos y operativos para evitar el progreso de llamadas y mensajes de texto ilícitos, así como, herramientas de trazabilidad para identificar el origen de las comunicaciones con uso indebido de numeración.
- Costos asociados a la sujeción a fiscalización y sanciones graduadas, debido a que la presencia de un régimen sancionador más definido implica mayores controles internos, sin embargo, al existir gradualidad e incluso

medidas correctivas y cautelares, el modelo favorece la corrección progresiva antes que la sanción por sorpresa.

Para la población

Beneficios:

- Reducción efectiva de comunicaciones ilícitas, ya que el marco integral propuesto permitiría una mayor disminución del volumen de estas (al combinar tecnología, obligaciones, trazabilidad y sanciones) que las otras alternativas.
- Reducción de los niveles de ansiedad y fatiga asociadas a las llamadas y mensajes de texto recurrentes.
- Permite una mejora sustantiva en seguridad y tranquilidad, ya que la reducción de comunicaciones ilícitas mejora el bienestar de la población, reduciendo ansiedad, temor y desconfianza permanente frente a llamadas o mensajes desconocidos.
- Genera un fortalecimiento de la confianza en canales digitales y servicios formales, por lo que al percibir mayor seguridad en la numeración y en los canales de comunicación (mensajes de texto y llamadas), los ciudadanos están más dispuestos a usar servicios digitales (recupera la confianza en el canal telefónico y de mensajería).
- Se da una protección más inclusiva, ya que esta propuesta beneficia incluso a usuarios con equipos simples o sin aplicaciones avanzadas, porque el control y filtrado se da en la red del operador, no solo en el terminal, lo que es particularmente relevante para usuarios de menores ingresos o en zonas rurales, que suelen contar con dispositivos menos sofisticados.
- Limita la generación de pérdidas económicas, como consecuencia de una reducción de comunicaciones ilícitas.

Costos:

- Posibilidad de bloqueo erróneo de mensajes y llamadas legítimas, ya que como en todo sistema, existe la posibilidad de que algunas llamadas o mensajes legítimos sean bloqueados o marcados como sospechosos, sin embargo, esto puede mitigarse con ajustes progresivos, revisión de reglas y mecanismos de corrección.

Análisis Multicriterio

Por consiguiente, con la finalidad de evaluar las tres alternativas propuestas y dado que esta evaluación abarca una serie de aspectos tanto cuantitativos como cualitativos, siendo estos últimos particularmente no siempre posibles de medir, resulta apropiado utilizar el Análisis Multicriterio⁴⁴. Este método

⁴⁴ El análisis multicriterio, es una metodología que permite la elección de la mejor alternativa, a partir de la ponderación y agregación de diferentes criterios de evaluación, que son el reflejo de la valoración que se ha otorgado a la forma en que cada alternativa pretende resolver el problema.

Una vez definidos los criterios y ponderaciones, se procede a calificar cada alternativa asignándoles un puntaje ordinal. Posteriormente, se realiza la suma ponderada de estas calificaciones y se obtiene el total para cada alternativa. Finalmente, se elige la alternativa que obtenga el mayor puntaje ponderado como la mejor opción:

permite identificar y seleccionar la alternativa que, en su conjunto, logre el mayor puntaje de evaluación y ofrezca los mayores beneficios netos según los criterios establecidos.

En base a ello, para la evaluación del análisis multicriterio se consideran los siguientes criterios:

Efectividad de la intervención: Este criterio evalúa la capacidad de cada alternativa para cumplir con el objetivo central de prevenir, detectar y reducir las comunicaciones con fines ilícitos. Considera el grado en que cada opción incorpora medidas, mecanismos operativos y/o soluciones tecnológicas que permitan bloquear comunicaciones irregulares y asegurar la trazabilidad técnica del origen de dichas comunicaciones. Asimismo, analiza la fortaleza del diseño de cada alternativa para sostener resultados en el tiempo, especialmente frente a la evolución de nuevas modalidades delictivas, técnicas de suplantación o esquemas de fraude. Por lo que, constituye el atributo más relevante para resolver el problema público identificado, este criterio concentra el 50% de la ponderación total del análisis multicriterio.

Costo para las empresas: Este criterio considera, cuál de las alternativas genera o facilita ahorros en costos de inversión y regulación para las empresas, así como, los costos directos e indirectos que las empresas tendrán que asumir para cumplir con las regulaciones propuestas por cada alternativa. Obteniendo un puntaje mayor aquella alternativa que genere una menor carga financiera para las empresas o mayores ahorros para el cumplimiento normativo. En esa línea, este criterio tendrá un peso de 25% de la medida a implementar.

Costo regulatorio: Este criterio se enmarca en evaluar cuál de las alternativas genera menores costos de supervisión y fiscalización relacionadas al cumplimiento de las regulaciones impuestas. En otras palabras, este criterio busca evaluar cuál de las alternativas conlleva menores costos operativos y de gestión para el Estado, buscando eficiencia en la utilización de recursos públicos y agilidad en los procesos regulatorios. En esa línea, este criterio tendrá un peso de 25% de la medida a implementar.

Escala de criterios de evaluación

$$\text{Max} \left[V_i = w_1 V_{i1} + w_2 V_{i2} + \dots + w_n V_{in} = \sum_{j=1}^n w_j V_{ij} \right]$$

Donde w_n es la ponderación asignada al criterio n y V_{in} es la calificación o puntaje otorgado por el criterio n a la alternativa de solución i .

(Esta referencia comprende lo señalado en las "Metodologías para la evaluación de impactos del AIR Ex Ante").

+3	+2	+1	0	-1	-2	-3
Alta mejora respecto al escenario base.	Mejora moderada respecto al escenario base.	Ligera mejora respecto al escenario base.	No presenta un cambio sustancial en efectividad o costos con respecto al escenario base.	Ligera desmejora respecto al escenario base.	Desmejora moderada respecto al escenario base.	Importante desmejora respecto al escenario base.
----- - Ahorros importantes frente al escenario base	----- - Ahorros moderados frente al escenario base	----- --- Ligero ahorro frente al escenario base		----- --- Ligero incremento de costos respecto a escenario base	----- -- Incremento moderado de costos respecto a escenario base	----- --- Importante incremento de costos respecto a escenario base

Fuente: Informe N° 00110-GPRC/2020-OISPTL

Valoración de las alternativas

A partir de los criterios metodológicos expuestos, se evaluará el puntaje a asignar a la alternativa distinta al statu quo (para efectos de este análisis consideramos el statu quo como el escenario base donde no se implementa ninguna acción), con el fin de atender la problemática.

Criterio	Alternativa 1 (Statu quo)	Alternativa 2 (No regulatoria)	Alternativa 3 (Regulatoria)
Efectividad	Esta alternativa no incorpora ningún mecanismo adicional para prevenir, detectar o reducir el uso inadecuado de numeración con fines ilícitos. En ausencia de nuevas obligaciones, mecanismos de trazabilidad o capacidades sancionadoras, la efectividad del sistema se mantiene sin mejoras sustanciales. Se perpetúan las debilidades actuales, como falta de trazabilidad, limitada capacidad para detener comunicaciones ilícitas en tiempo real, ausencia de mecanismos correctivos y amplia asimetría de	La alternativa no regulatoria incorpora acciones de autorregulación, acuerdos voluntarios entre empresas operadoras y agentes vinculados, así como campañas de información y sensibilización dirigidas a los usuarios. Estas medidas pueden generar mejoras parciales en la detección de comunicaciones ilícitas y en la reducción de la vulnerabilidad de ciertos segmentos de usuarios, especialmente frente a esquemas de fraude menos sofisticados. No obstante, su efectividad es	La alternativa regulatoria introduce un marco obligatorio, homogéneo y exigible que establece reglas, medidas y mecanismos técnicos y operativos orientados específicamente a prevenir el uso indebido de la numeración, bloquear comunicaciones ilícitas y asegurar la trazabilidad técnica del origen de las llamadas y mensajes de texto. A diferencia de las otras alternativas, esta opción corrige de manera directa las principales fallas identificadas, como la fragmentación técnica, la falta de coordinación en la cadena de trazabilidad y los

	<p>información entre operadores y el Estado.</p> <p>En este escenario, las comunicaciones con fines ilícitos continúan siendo atendidas principalmente mediante acciones ex post, como denuncias e investigaciones posteriores, las cuales han demostrado ser insuficientes para contener el incremento sostenido del problema.</p> <p>Puntaje: 0</p>	<p>limitada y desigual, ya que depende del grado de adhesión voluntaria de los actores involucrados y de la capacidad individual de los usuarios para identificar comunicaciones fraudulentas. En ese sentido, la ausencia de obligaciones exigibles y de estándares técnicos comunes reduce la posibilidad de asegurar una trazabilidad integral del origen de las comunicaciones y dificulta la sostenibilidad de los resultados en el tiempo, especialmente frente a la rápida adaptación de la ingeniería social para actos ilícitos.</p> <p>Por estas razones, si bien esta alternativa representa una mejora marginal respecto al statu quo, no constituye una solución estructural ni plenamente efectiva.</p> <p>Puntaje: +1</p>	<p>incentivos insuficientes para la adopción de medidas preventivas.</p> <p>En ese contexto, el diseño de la alternativa incorpora obligaciones claras para empresas operadoras y agentes vinculados, facultades de fiscalización y sanción para el Estado, y un enfoque preventivo que permite anticiparse a nuevas modalidades de fraude, en lugar de reaccionar únicamente cuando el daño ya se ha producido. Asimismo, al establecer estándares comunes y mecanismos de supervisión, esta alternativa maximiza la probabilidad de generar resultados sostenibles en el tiempo, incluso frente a la evolución tecnológica de los esquemas delictivos</p> <p>En consecuencia, la alternativa regulatoria representa una mejora sustancial y estructural en la efectividad de la intervención, superando ampliamente al escenario base y a la alternativa no regulatoria.</p> <p>Puntaje: +3</p>
<p>Costo para las empresas</p>	<p>Esta alternativa mantiene las condiciones actuales y no introduce nuevas</p>	<p>La alternativa no regulatoria implica que las empresas operadoras y los</p>	<p>La alternativa regulatoria establece obligaciones exigibles para las</p>

	<p>obligaciones tecnológicas, operativas o regulatorias para los operadores, por lo que no demanda inversiones adicionales ni gastos de adecuación, monitoreo ni cumplimiento.</p> <p>Puntaje: 0</p>	<p>agentes vinculados asuman costos adicionales de manera voluntaria, asociados a la implementación de buenas prácticas, acuerdos sectoriales, mejoras parciales en sistemas de detección y bloqueo, así como a la participación en campañas de información y sensibilización dirigidas a los usuarios. Estos costos, si bien no son impuestos por una norma obligatoria, requieren la asignación de recursos financieros, humanos y tecnológicos adicionales respecto al statu quo.</p> <p>No obstante, dichos costos suelen ser acotados y heterogéneos, dado que dependen del nivel de compromiso de cada actor y no responden a estándares técnicos uniformes ni exigibles.</p> <p>En ese sentido, esta alternativa genera un incremento ligero de costos para las empresas, pero inferior al de una intervención regulatoria formal.</p> <p>Puntaje: -1</p>	<p>empresas operadoras y los agentes vinculados, lo que conlleva un incremento moderado de costos de cumplimiento en relación con el escenario base. Estos costos incluyen inversiones en infraestructura tecnológica, adecuaciones de sistemas y procesos, contratación o capacitación de personal especializado, gestión de reportes, atención de reclamos derivados de medidas preventivas y costos asociados a la supervisión y fiscalización. Sin embargo, podría generar menores costos netos ya que la propuesta incorpora un sistema regulatorio completo, predecible y equilibrado, que incluye herramientas que permitirían:</p> <ul style="list-style-type: none"> - Gradualidad de infracciones. - Medidas correctivas que permiten subsanar incumplimientos antes de sancionar. - Medidas cautelares que evitan perjuicios mayores sin llegar a procesos sancionadores. - Facultades de fiscalización basadas en regulación de mayor jerarquía, lo que reduce la
--	---	---	---

			<p>incertidumbre jurídica.</p> <p>Si bien estos costos son relevantes y superiores a los de las alternativas 1 y 2, no alcanzan un nivel que comprometa la sostenibilidad económica de las empresas ni la continuidad de los servicios, especialmente considerando el carácter progresivo de la implementación y la posibilidad de economías de escala y aprendizaje en el tiempo. Asimismo, parte de estos costos se ve compensada por reducciones futuras en costos operativos y reputacionales, como la disminución de reclamos y de tráfico ilícito en las redes.</p> <p>Puntaje: -2</p>
Costos regulatorios	<p>Bajo esta alternativa, no se introducen nuevas obligaciones regulatorias ni mecanismos adicionales de fiscalización.</p> <p>El Estado continúa operando bajo el mismo esquema actual, que presenta limitaciones importantes, pero que no implica un aumento ni una reducción en los costos regulatorios existentes.</p> <p>En ese sentido, no se generan nuevos</p>	<p>La alternativa no regulatoria implica un incremento ligero de costos regulatorios, asociado principalmente a funciones de coordinación, promoción, seguimiento y evaluación de acuerdos voluntarios, así como al diseño e implementación de campañas de información y sensibilización dirigidas a la población, estas actividades demandan recursos administrativos y de</p>	<p>La alternativa regulatoria implica un incremento de costos regulatorios para el Estado, derivados de la elaboración del reglamento, el fortalecimiento de capacidades técnicas, y el ejercicio de funciones de supervisión, fiscalización y sanción por parte del MTC. Estas actividades requieren recursos humanos especializados, herramientas de monitoreo y coordinación con</p>

	<p>procesos administrativos, ni nuevos sistemas de monitoreo, ni nuevas cargas de supervisión formal. Por ello, esta alternativa mantiene el nivel de costos regulatorios vigente y sin variaciones.</p> <p>Puntaje: 0</p>	<p>gestión por parte del Estado, aun cuando no exista un régimen formal de fiscalización ni sanción.</p> <p>Asimismo, el carácter voluntario de las medidas puede requerir esfuerzos recurrentes de articulación interinstitucional y sectorial, a fin de mantener la adhesión de los actores involucrados y monitorear resultados, lo que genera costos operativos adicionales respecto al statu quo. No obstante, dichos costos se consideran acotados, al no involucrar procesos complejos de supervisión técnica ni sancionadora.</p> <p>Puntaje: -1</p>	<p>otras entidades competentes.</p> <p>No obstante, dichos costos no se consideran elevados, por varias razones: (i) la norma se implementa dentro del marco de competencias ya existentes del MTC, (ii) el financiamiento se realiza con el presupuesto institucional, sin creación de nuevas entidades ni estructuras administrativas, y (iii) el enfoque preventivo y sistémico de la intervención permite reducir progresivamente los costos ex post asociados a la atención masiva de denuncias, investigaciones fragmentadas y acciones reactivas.</p> <p>En ese sentido, si bien la alternativa regulatoria genera un incremento ligero de costos regulatorios iniciales, estos se ven compensados por ganancias de eficiencia administrativa en el mediano plazo.</p> <p>Puntaje: -1</p>
--	---	---	---

Entonces, se realiza el análisis de puntuación otorgada a las alternativas por cada criterio:

Comparación entre alternativas

Criterios de evaluación	Ponderación	Alternativa 1	Alternativa 2	Alternativa 3
Efectividad	50%	0	1	3
Costos para las empresas	25%	0	-1	-2
Costos regulatorios	25%	0	-1	-1
Resultado de la evaluación		0	0	0.75

Criterios de evaluación	Ponderación	Alternativa 1	Alternativa 2	Alternativa 3
Efectividad	50%	0	1	3
Costos para las empresas	25%	0	-1	-2
Costos regulatorios	25%	0	-1	-1
Resultado de la evaluación		0	0	0.75

Criterios de evaluación	Ponderación	Alternativa 1	Alternativa 2	Alternativa 3
Efectividad	50%	0	1	3
Costos para las empresas	25%	0	-1	-2
Costos regulatorios	25%	0	-1	-1
Resultado de la evaluación		0	0	0.75

Tras evaluar estas alternativas propuestas para enfrentar las comunicaciones ilícitas, a través de un análisis integral que incluye un enfoque costo-beneficio y una evaluación multicriterio ponderada por criterios de efectividad, costo para las empresas y costo regulatorio, se concluye que la Alternativa 3, consistente en la alternativa regulatoria, es la más adecuada y costo-efectiva para abordar el problema público identificado.

Esta alternativa presenta un equilibrio óptimo entre impacto, viabilidad y sostenibilidad regulatoria. A diferencia del statu quo (Alternativa 1), que no introduce mejoras sustanciales ni costos adicionales, pero perpetúa el problema y, de la Alternativa 2 (No regulatoria) que implica costos recurrentes de coordinación con resultados inciertos, la Alternativa 3 logra mayores niveles de efectividad.

Por tanto, la Alternativa 3 no solo representa la opción más efectiva desde el punto de vista técnico y operativo, sino también la más adecuada en términos de costo-efectividad para todos los actores involucrados: el Estado, los operadores de telecomunicaciones y agentes vinculados y la ciudadanía, ya que termina ofreciendo un equilibrio entre efectividad, proporcionalidad y viabilidad técnica.

VIII. Análisis de impacto de la vigencia de la norma en la legislación nacional

El numeral 10.1 del artículo 10 del Reglamento de la Ley N° 26889, Ley Marco para la Producción y Sistematización Legislativa, aprobado por Decreto Supremo

N° 007-2022-JUS, señala que el análisis de impacto de la vigencia de la norma en la legislación nacional debe precisar si la propuesta normativa trata de innovar supliendo vacíos en el ordenamiento jurídico o si trata de una propuesta que modifica o deroga normas vigentes.

Sobre el particular, en el proyecto de norma se han incorporado reglas, medidas y/o mecanismos que permitan identificar la trazabilidad de las comunicaciones, así como, determinar responsabilidades para combatir su anonimato y evitar las comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones.

Cabe resaltar que el articulado del Proyecto de Norma se encuentra alineado con lo dispuesto en el artículo 44 de la Constitución Política del Perú, el cual establece que son deberes primordiales del Estado, 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, la emisión del Proyecto de Norma guarda coherencia con lo dispuesto en la Única Disposición Preliminar del TUO de la Ley de Telecomunicaciones, el cual declara de necesidad pública el desarrollo de las Telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional.

Del mismo modo, se encuentra acorde con el artículo 2 del TUO de la Ley de Telecomunicaciones, el cual declara de interés nacional la modernización y desarrollo de las telecomunicaciones, dentro del marco de libre competencia, y establece que su fomento, administración y control corresponde al Estado de acuerdo a dicha Ley; así como, con lo dispuesto en su artículo 3, el cual establece el derecho que tiene toda persona de usar y prestar servicios de telecomunicaciones en la forma señalada en las disposiciones que regulan la materia.

Por otro lado, en el Proyecto de Norma se ha dispuesto la modificación Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM.

De esta forma, en la siguiente tabla se muestra el comparativo de la mencionada modificación:

Única Disposición Complementaria Final de la Ley 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor	Propuesta de modificación de la Única Disposición Complementaria Final de la Ley 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor
<i>ÚNICA. Normativa adicional Para la aplicación del párrafo 58.3 del artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor, incorporado por la presente ley, el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración telefónica</i>	<i>ÚNICA. Normativa adicional Para la aplicación del numeral 58.3 del artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor, incorporado por la presente ley, el Poder Ejecutivo establece la normativa adicional que otorgue la numeración telefónica especial a los proveedores,</i>

<p><i>especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas (spam) que reciben, así como los mecanismos de validación de la información transmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de la presente ley.</i></p>	<p><i>los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas y mensajes de texto (spam) que reciben, así como los mecanismos de validación de la información transmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de la presente ley.</i></p> <p><i>Para el cumplimiento de la mencionada normativa adicional, el Ministerio de Transportes y Comunicaciones y el INDECOPI ejercen la facultad fiscalizadora y sancionadora, en el ámbito de sus funciones y competencias.</i></p>
--	---

IX. Análisis de impacto regulatorio ex ante

El 28 de mayo de 2023 se publicó en el diario oficial El Peruano el Decreto Legislativo N° 1565, que aprueba la Ley General de Mejora de la Calidad Regulatoria, cuya única disposición complementaria regulatoria derogó el artículo 2 del Decreto Legislativo N° 1310, que estableció como instrumento para la mejora de la calidad regulatoria el Análisis de Impacto Regulatorio.

Sin perjuicio de lo señalado, la segunda disposición complementaria final del Decreto Legislativo N° 1565, dispuso que en tanto se apruebe su reglamento, continuaba vigente el Reglamento que desarrolla el Marco Institucional que rige el Proceso de Mejora de la Calidad Regulatoria y establece los Lineamientos Generales para la aplicación del Análisis de Impacto Regulatorio Ex Ante, aprobado por Decreto Supremo N° 063-2021-PCM.

Con fecha 25 de febrero de 2025, se publicó el Decreto Supremo N° 023-2025-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria (en adelante, el Reglamento de la Ley General de Mejora de la Calidad Regulatoria).

Al respecto, se tiene que, conforme al literal f) del artículo 15 del Reglamento AIR las entidades del Poder Ejecutivo tienen, entre otras obligaciones, la obligación de determinar si un proyecto normativo requiere la presentación de un expediente AIR Ex Ante o ACR Ex Ante ante la Comisión Multisectorial de Calidad Regulatoria (CMCR), así como el aplicar dichos instrumentos de forma previa a la elaboración de normas de carácter general, cuya responsabilidad es del órgano proponente del proyecto normativo, según corresponda.

Mediante Resolución de Secretaría de Gestión Pública N° 008-2021-PCM-SGP se aprobó el Plan de Implementación del Análisis de Impacto Regulatorio Ex Ante para las entidades públicas del Poder Ejecutivo. Dicho Plan señala el Cronograma de implementación del AIR Ex Ante y la Agenda Temprana en las entidades públicas del Poder Ejecutivo, siendo que resulta de aplicación obligatoria el Análisis de Impacto Regulatorio Ex Ante para el MTC a partir del 02 de enero de 2023.

Ahora bien, el Reglamento de la Ley General de Mejora de la Calidad Regulatoria, señala en el literal g) del artículo 5 que se entiende por “norma de carácter general” a aquella que crea, modifica, regula, declara o extingue derechos u obligaciones de carácter general, de cuyo texto se deriva un mandato genérico, objetivo y obligatorio, vinculando a la Administración Pública y a los administrados, sea para el cumplimiento de una disposición o para la generación de una consecuencia jurídica.

Asimismo, de acuerdo con el numeral 33.2 del artículo 33 del el Reglamento de la Ley General de Mejora de la Calidad Regulatoria estipula que 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 exigencias: 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.

Bajo dicho contexto, se tiene que el Proyecto de Decreto Legislativo amerita la realización de un análisis de impacto regulatorio ya que se subsume en lo regulado en numeral 33.2 del artículo 33 del el Reglamento de la Ley General de Mejora de la Calidad Regulatoria, dado que se establecen reglas, obligaciones, medidas y/o mecanismos a ser cumplidas por las empresas operadoras y agentes vinculados al adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana.

Asimismo, cabe señalar que el Ministerio de Transportes y Comunicaciones ha desarrollado acciones orientadas a la obtención de información y socialización de las medidas de la propuesta normativa, a través de una reunión con las empresas operadoras de fecha 18 de diciembre de 2025, donde se les indico sobre el establecimiento de reglas orientadas a la eliminación de las llamadas anónimas para que las empresas operadoras indiquen porque existe el anonimato en las redes de telecomunicaciones, debido a que ellos tienen el control de sus redes.

De igual manera, se mantuvo una reunión con la Policía Nacional del Perú - PNP y la DGFSC-MTC, donde se recibió los insumos sobre los problemas que experimenta la policía en su accionar contra la delincuencia vinculada a las comunicaciones ilícitas.

En ese sentido, la presente norma cuenta con dictamen favorable de fecha 26 de enero de 2026 de la Comisión Multisectorial de Calidad Regulatoria que valida el expediente AIR Ex Ante correspondiente.

X. Publicación de proyectos normativos

Al respecto, corresponde aplicar la excepción regulada 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 por el Decreto Supremo N° 009-2024-JUS, que prescribe:

“Artículo 19.- Difusión de los proyectos de normas jurídicas de carácter general

(...)

19.2. Se exceptúa de la publicación del proyecto normativo a las siguientes disposiciones:

a) Los decretos de urgencia ordinarios y los decretos legislativos.

(...)".

Por lo que la presente propuesta normativa no requiere ser publicada en las sedes digitales de las entidades de la Administración Pública a cargo de su elaboración ni en otro medio, debido a que consiste en un decreto legislativo.

**DECRETO LEGISLATIVO
N° 1723**

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

Que, mediante Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materia 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 sub numeral 2.1.17 del numeral 2.1 del artículo 2 de la Ley N° 32527, establece que el Poder Ejecutivo está facultado para legislar en materias de Seguridad y lucha contra la criminalidad organizada, entre las cuales se considera: "Establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones";

Que, conforme a los numerales 1, 22 y el segundo párrafo del numeral 4 del artículo 2 de la Constitución Política del Perú, toda persona tiene derecho a la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar; así como, a gozar de un ambiente equilibrado y adecuado al desarrollo de su vida, y a que el Estado promueva el uso de las tecnologías de la información y la comunicación en todo el país;

Que, el artículo 44 de la Constitución Política del Perú, establece que son deberes primordiales del Estado, 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;

Que, los artículos 4 y 5 de la Ley N° 29370, Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones establecen que este Ministerio es competente de manera exclusiva, en materia de infraestructura y servicios de comunicaciones, y tiene, entre otras funciones rectoras, formular, planear, dirigir, coordinar, ejecutar, fiscalizar, supervisar y evaluar la política nacional y sectorial bajo su competencia, aplicable a todos los niveles de gobierno; así como, dictar normas y lineamientos técnicos para la adecuada ejecución, supervisión y evaluación de las políticas, la gestión de los recursos del sector, así como para el otorgamiento y reconocimiento de derechos, la sanción, la fiscalización y ejecución coactiva en materias de su competencia;

Que, la Disposición Preliminar del Texto Único Ordenado de la Ley de Telecomunicaciones aprobado por Decreto Supremo N° 013-93-TCC, declara de necesidad pública el desarrollo de las Telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional;

Que, el artículo 2 del Texto Único Ordenado de la Ley de Telecomunicaciones, declara de interés nacional la modernización y desarrollo de las telecomunicaciones, dentro del marco de libre competencia, y establece que su fomento, administración y control corresponde al Estado de acuerdo a dicha Ley. Asimismo, en su artículo 3 establece el derecho que tiene toda persona de usar y prestar servicios de telecomunicaciones en la forma señalada en las disposiciones que regulan la materia;

Que, los numerales 1, 2, 3 y 13 del artículo 75 del Texto Único Ordenado de la Ley de Telecomunicaciones, establecen que son funciones del Ministerio de Transportes y Comunicaciones, fijar la política de telecomunicaciones a seguir y controlar sus resultados; elaborar y proponer la aprobación de los reglamentos y planes de los distintos servicios contemplados en la Ley y expedir resoluciones relativas a los mismos; otorgar y revocar concesiones, autorizaciones, permisos, licencias y controlar su correcta utilización; y, ejercer las facultades inspectoras y sancionadoras previstas en la Ley;

Que, la comisión de actos ilícitos, tales como fraudes, estafas, extorsiones, amenazas o suplantación de identidad, representa un riesgo creciente para la seguridad ciudadana, al afectar directamente la integridad, el patrimonio y la confianza de la población en el uso de los servicios públicos de telecomunicaciones;

Que, asimismo, la Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley N° 29571, Código de Protección y Defensa del Consumidor a fin de ampliar la prohibición de las comunicaciones SPAM, dispone que el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas (spam) que reciben, así como los mecanismos de validación de la información transmitida, mandato que se encuentra únicamente referido a las llamadas spam, cuando la identificación también debe aplicarse a los mensajes de texto, a fin de estar en concordancia con el numeral 58.3 del artículo 58 de la citada Ley N° 29571; por lo que, resulta necesario precisar en ese sentido la Única Disposición Complementaria Final de la Ley N° 32323;

Que, en ese contexto resulta necesario establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto permitiendo identificar su trazabilidad, así como, determinar responsabilidades con el objetivo de combatir su anonimato y evitar las comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana;

Que, en virtud del numeral 33.2 del artículo 33 del Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, aprobado mediante el Decreto Supremo N° 023-2025-PCM, la presente norma cuenta con dictamen favorable de la Comisión Multisectorial de Calidad Regulatoria que valida el expediente AIR Ex Ante correspondiente;

De conformidad con lo establecido en el artículo 104 de la Constitución Política del Perú; el numeral 1 del artículo 11 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; en ejercicio de la facultad delegada en el sub numeral 2.1.17 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, crecimiento económico responsable y fortalecimiento institucional; la Ley N° 29370, Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones; el Texto Único Ordenado de la Ley de Telecomunicaciones, aprobado mediante Decreto Supremo N° 013-93-TCC; y, el Texto Único Ordenado de su reglamento, aprobado con Decreto Supremo N° 020-2007-MTC;

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 ESTABLECE
REGLAS, MEDIDAS Y/O MECANISMOS PARA
EL ADECUADO USO DE LA NUMERACIÓN
EN LLAMADAS Y MENSAJES DE TEXTO Y SU
TRAZABILIDAD, A FIN DE EVITAR EL ANONIMATO
Y COMUNICACIONES ILÍCITAS EN PERJUICIO DE
LOS USUARIOS DE LOS SERVICIOS PÚBLICOS DE
TELECOMUNICACIONES**

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto

La presente norma tiene por objeto establecer reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y/o mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, en el marco de la lucha contra la inseguridad ciudadana.

Artículo 2.- Finalidad

El presente Decreto Legislativo permite la identificación y/o veracidad del número de origen de la comunicación, y evita o mitiga las prácticas de enmascaramiento o manipulación del recurso numérico que conllevan al progreso de llamadas y/o mensajes de texto ilícitos y los efectos negativos que generan en la sociedad.

Artículo 3.- Ámbito de aplicación

3.1 La presente norma es aplicable a las empresas operadoras de los servicios públicos de telecomunicaciones y los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto.

3.2 Para efectos del presente Decreto Legislativo, se considera como agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto a toda persona natural o persona jurídica que interviene en el enrutamiento o encaminamiento de las comunicaciones y/o cuenta con información de la trazabilidad de las mismas.

CAPÍTULO II**OBLIGACIONES DE LAS EMPRESAS OPERADORAS DE SERVICIOS PÚBLICOS DE TELECOMUNICACIONES PARA IDENTIFICAR LA TRAZABILIDAD DE LAS COMUNICACIONES Y EVITAR SU PROGRESO CON FINES ILÍCITOS****Artículo 4.- Obligaciones de las empresas operadoras de servicios públicos de telecomunicaciones**

4.1 Las empresas operadoras adoptan medidas y/o mecanismos técnicos y/u operativos para evitar el progreso de llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos; así como, para permitir a los abonados y usuarios advertir sobre dichas comunicaciones.

4.2 Las empresas operadoras implementan medidas tecnológicas para impedir que se concreten comunicaciones con fines ilícitos.

Las empresas operadoras pueden implementar medidas adicionales a lo dispuesto en el párrafo anterior, sin contravenir lo dispuesto en el presente marco normativo.

4.3 Las empresas operadoras adoptan medidas que coadyuven a determinar el origen de las llamadas y/o mensajes de texto con uso inadecuado de la numeración para fines ilícitos.

4.4 Las medidas, mecanismos y/o disposiciones mencionadas en los numerales 4.1, 4.2 y 4.3 de la presente norma, son desarrolladas y determinadas en el Reglamento de la misma.

Artículo 5.- Gestión y administración de las redes de las empresas operadoras

Las empresas operadoras proporcionan y otorgan las facilidades al Ministerio de Transportes y Comunicaciones, para el acceso y monitoreo constante de sus redes, para verificar el cumplimiento de las obligaciones establecidas en el artículo 4, según corresponda, para la correcta prestación de los servicios públicos de telecomunicaciones, con la finalidad de salvaguardar la seguridad ciudadana en los mismos, en beneficio y protección de los usuarios, resguardando la inviolabilidad y el secreto de las telecomunicaciones.

CAPÍTULO III**OBLIGACIONES DE LOS AGENTES VINCULADOS EN LA TRAZABILIDAD DE LAS LLAMADAS Y/O MENSAJES DE TEXTO****Artículo 6.- Obligaciones de los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto**

6.1 Los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto coadyuvan y/o participan en la identificación y trazabilidad de las referidas comunicaciones

para evitar su progreso con fines ilícitos, para la correcta prestación de los servicios públicos de telecomunicaciones y/o en aras de salvaguardar la seguridad ciudadana en los mismos, en beneficio y protección de los usuarios. Para tal efecto, cumplen las disposiciones establecidas en el Reglamento de la presente norma.

6.2 El Ministerio de Transportes y Comunicaciones está facultado para establecer, a través del Reglamento del presente Decreto Legislativo, las condiciones y/o requisitos aplicables a los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto, así como, para establecer las obligaciones aplicables a estos.

Artículo 7.- Gestión y administración de los sistemas de los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto

Los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto otorgan las facilidades al Ministerio de Transportes y Comunicaciones, para el acceso y monitoreo constante de sus sistemas de gestión, para verificar el cumplimiento de las obligaciones establecidas en el artículo 6, según corresponda, resguardando la inviolabilidad y el secreto de las telecomunicaciones.

CAPÍTULO IV**POTESTAD FISCALIZADORA Y SANCIONADORA****Artículo 8.- Potestad fiscalizadora, sancionadora y de imposición de medidas correctivas y cautelares del Ministerio de Transportes y Comunicaciones**

8.1 El Ministerio de Transportes y Comunicaciones, de acuerdo a sus competencias y normas reglamentarias, tiene potestad para fiscalizar y sancionar a las empresas operadoras y a los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto por el incumplimiento de las obligaciones derivadas del presente Decreto Legislativo. El tipo de sanción a imponer es amonestación escrita o multa.

8.2 Las infracciones por el incumplimiento de las obligaciones derivadas del presente Decreto Legislativo se clasifican en leves, graves y muy graves, y se tipifican en su Reglamento.

8.3 Las infracciones son sancionadas, de acuerdo a las escalas de multas establecidas en la Ley N° 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL o norma que sustituya dicha escala de multas. En el caso de infracciones leves, el Ministerio de Transportes y Comunicaciones puede aplicar la sanción de amonestación escrita o multa, y para las infracciones graves y muy graves aplica la sanción de multa.

8.4 El Ministerio de Transportes y Comunicaciones puede aplicar medidas preventivas, cautelares y/o medidas correctivas, según correspondan.

8.5 En el ejercicio de la actividad de fiscalización, el Ministerio de Transportes y Comunicaciones se encuentra facultado para monitorear de manera constante las redes de las empresas operadoras y los sistemas de gestión de los agentes vinculados en la trazabilidad de las llamadas y/o mensajes de texto, para verificar el cumplimiento de las obligaciones establecidas en los artículos 4, 5, 6 y 7, según corresponda, para la correcta prestación de los servicios públicos de telecomunicaciones, salvaguardar la seguridad ciudadana en los mismos y/o en otras situaciones análogas, en beneficio y protección de los usuarios, resguardando la inviolabilidad y el secreto de las telecomunicaciones e información protegida por ley.

Artículo 9.- Financiamiento

La implementación del presente Decreto Legislativo se financia con el presupuesto institucional del Ministerio de Transportes y Comunicaciones sin demandar recursos adicionales al Tesoro Público, conforme a lo establecido en las leyes anuales de presupuesto del sector público.

Artículo 10.- Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros y el Ministro de Transportes y Comunicaciones.

DISPOSICIONES COMPLEMENTARIAS FINALES**PRIMERA.- Vigencia**

El presente Decreto Legislativo entra en vigencia a partir del día siguiente de la publicación del Reglamento de la presente norma en el diario oficial El Peruano.

SEGUNDA.- Reglamentación

El Ministerio de Transportes y Comunicaciones en un plazo no mayor a noventa (90) días calendario contado desde la publicación de la presente norma, mediante Decreto Supremo, aprueba el Reglamento correspondiente.

DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA

ÚNICA.- Modificación de Disposiciones Complementarias Finales de la Ley N° 32323, Ley que modifica la Ley N° 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM

Se modifica la Única Disposición Complementaria Final de la Ley N° 32323, Ley que modifica la Ley N° 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM, en los siguientes términos:

“ÚNICA.- Normativa adicional

Para la aplicación del numeral 58.3 del artículo 58 de la Ley N° 29571, Código de Protección y Defensa del Consumidor, incorporado por la presente ley, el Poder Ejecutivo establece la normativa adicional que otorgue la numeración telefónica especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas y mensajes de texto (spam) que reciben, así como los mecanismos de validación de la información transmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de la presente ley.

Para el cumplimiento de la mencionada normativa adicional, el Ministerio de Transportes y Comunicaciones y el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI ejercen la facultad fiscalizadora y sancionadora, en el ámbito de sus funciones y competencias”.

POR TANTO:

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

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

JOSÉ ENRIQUE JERÍ ORÉ
Presidente de la República

ERNESTO JULIO ÁLVAREZ MIRANDA
Presidente del Consejo de Ministros

ALDO MARTÍN PRIETO BARRERA
Ministro de Transportes y Comunicaciones

2484948-6

**DECRETO LEGISLATIVO
N° 1724**

Decreto Legislativo que modifica el Decreto Legislativo N° 822, Ley sobre el Derecho de Autor, a fin de incorporar disposiciones en materia de eximentes de responsabilidad de proveedores de acceso a Internet y proveedores de servicios en el entorno digital

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, el Congreso de la República, mediante la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana, lucha contra la criminalidad organizada, crecimiento

económico responsable y fortalecimiento institucional, ha otorgado facultades al Poder Ejecutivo para legislar, entre otros aspectos, en materia de crecimiento económico responsable, por el plazo de sesenta días calendario;

Que, el numeral 2.2.12 del párrafo 2.2 del artículo 2 de la Ley N° 32527, faculta al Poder Ejecutivo a legislar en materia de crecimiento económico responsable, para incorporar en el Decreto Legislativo N° 822, Ley sobre el Derecho de Autor, disposiciones en materia de limitación de responsabilidad de proveedores del servicio de Internet a fin de fortalecer la observancia de los derechos de propiedad intelectual, en concordancia con los compromisos comerciales internacionales asumidos por el Perú;

Que, de conformidad con el párrafo 29 del Artículo 16.11 del Capítulo Dieciséis sobre Derechos de Propiedad Intelectual del Acuerdo de Promoción Comercial (APC) entre la República del Perú y los Estados Unidos de América, el Perú se comprometió a establecer incentivos legales para que los proveedores de servicios colaboren con los titulares de derechos de autor en disuadir el almacenaje y transmisión no autorizados de materiales protegidos por el derecho de autor; así como, establecer eximentes de responsabilidad para dichos proveedores, en casos de infracción al derecho de autor y derechos conexos en el entorno digital;

Que, los proveedores del servicio de Internet pueden estar sujetos a responsabilidad solidaria por infracciones al derecho de autor y derechos conexos, conforme a las normas vigentes en la materia, entre ellas el artículo 54 de la Decisión 351 de la Comunidad Andina que establece el Régimen Común sobre Derecho de Autor y Derechos Conexos, y el artículo 39 del Decreto Legislativo N° 822, Ley sobre el Derecho de Autor; sin embargo, dichas normas no contienen disposiciones específicas que regulen circunstancias eximentes de la responsabilidad en casos de infracciones al derecho de autor y los derechos conexos por parte de los usuarios de sus sistemas o redes;

Que, el fortalecimiento de la observancia de los derechos de propiedad intelectual es de vital importancia para promover el aprovechamiento de los activos de propiedad intelectual por parte de los titulares de estos derechos, promoviendo el comercio formal en el marco digital, contribuyendo al crecimiento económico responsable;

Que, en virtud a lo dispuesto en el literal r) 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 por el Decreto Supremo N° 023-2025-PCM, la presente norma se considera exceptuada del alcance del Análisis de Impacto Regulatorio - AIR Ex Ante, conforme lo ha señalado la Comisión Multisectorial de Calidad Regulatoria (CMCR) de la Presidencia del Consejo de Ministros;

De conformidad con lo establecido en el artículo 104 de la Constitución Política del Perú, y en el ejercicio de las facultades delegadas en el numeral 2.2.12 del párrafo 2.2 del artículo 2 de la Ley N° 32527, Ley que delega en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana, 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 EL
DECRETO LEGISLATIVO N° 822, LEY SOBRE EL
DERECHO DE AUTOR, A FIN DE INCORPORAR
DISPOSICIONES EN MATERIA DE EXIMENTES
DE RESPONSABILIDAD DE PROVEEDORES DE
ACCESO A INTERNET Y DE PROVEEDORES DE
SERVICIOS EN EL ENTORNO DIGITAL**

Artículo 1.- Objeto

La presente norma tiene por objeto modificar el Decreto Legislativo N° 822, Ley sobre el Derecho de Autor, a fin de incorporar disposiciones sobre circunstancias