INSTITUTO FEDERAL DE TELECOMUNICACIONES

Estudio del servicio de mensajes cortos Aplicación a Persona

Instituto Federal de Telecomunicaciones

Diciembre 2023

Aviso legal

Debido a que el Instituto Federal de Telecomunicaciones es la autoridad de competencia económica, así como el órgano autónomo regulador, con facultades exclusivas, en los sectores de telecomunicaciones y radiodifusión, conforme lo dispuesto en el artículo 28, párrafos décimo cuarto, décimo quinto y décimo sexto, de la Constitución Política de los Estados Unidos Mexicanos; 7 de la Ley Federal de Telecomunicaciones y Radiodifusión; además del 5, párrafo primero, de la Ley Federal de Competencia Económica. Y a que, en México, se ha observado un creciente interés en la industria de telecomunicaciones por prestar el servicio de mensajes cortos en su modalidad Aplicación a Persona. El presente documento aborda la prestación del servicio de mensajes cortos en dicha modalidad, con el fin de identificar y estudiar las condiciones mediante las cuales es ofertado por los prestadores de servicios de telecomunicaciones, los nuevos casos de uso, las conductas no deseadas y/o fraudulentas asociadas a este, así como posibles soluciones a la problemática.

Este estudio se realiza con el objeto de contar con más elementos e insumos para evaluar el diseño de políticas públicas y, en su caso, acciones regulatorias, orientadas a promover la competencia efectiva en el mercado de telecomunicaciones, y favorecer la adopción de nuevos casos de uso del servicio de mensajes cortos en un entorno seguro que eviten el envío de mensajes no solicitados o con contenido fraudulento.

El estudio, no prejuzga otros procedimientos llevados a cabo o que pudiera llevar el Instituto Federal de Telecomunicaciones, en los que se analicen casos particulares, o se cuente con información específica, adicional o proveniente de fuentes distintas a las del presente; y/o sobre el ejercicio de las demás facultades que le corresponden.

Es importante resaltar que el contenido de este documento no refleja la postura institucional, ni es vinculante para el Pleno del Instituto Federal de Telecomunicaciones, así como tampoco para los sectores regulados, sujetos obligados o el usuario.

Contenido

Introducción

Los mensajes cortos aplicación a persona, o A2P (del inglés, "*Application to Person*") son mensajes de texto generados por una aplicación o sistema informático y son generalmente enviados por empresas u organizaciones a un destinatario específico o a un grupo de destinatarios permitiendo prestar diversos servicios, como la autenticación de usuarios, confirmaciones de transacciones financieras, envío de alertas de seguridad, promoción de servicios, entre otros.

A diferencia de los mensajes cortos (SMS) enviados de una persona a otra, los mensajes cortos A2P son enviados de manera masiva y automatizada, y tienen la capacidad de alcanzar a un gran número de destinatarios de manera rápida y eficiente, por lo que han generado un creciente interés para su uso en sectores como el financiero, en comercio electrónico, servicios de logística, entre otros, e interés por parte de los distintos prestadores de servicios de telecomunicaciones.

Sin embargo, uno de los principales desafíos que se han identificado en su prestación, es el envío de mensajes no deseados, como el envío spam[1] y mensajes con contenido fraudulento, los cuales pueden generar un impacto negativo para los usuarios y para los prestadores de servicios, los cuales deben implementar las medidas de seguridad necesarias a fin de reducir potenciales afectaciones en las redes de telecomunicaciones.

Por otro lado, también se han identificado limitantes que impiden que todos los prestadores del servicio de mensajes cortos A2P ofrezcan el servicio en igualdad de condiciones, lo que genera preocupación sobre los escenarios de competencia en la prestación de este servicio.

En este contexto, resulta necesario realizar un análisis que permita inicialmente caracterizar la evolución del servicio de mensajes cortos (SMS), identificando los casos de uso a nivel internacional, las entidades involucradas en la cadena de prestación del servicio de mensajes cortos A2P, las conductas no deseadas y/o fraudulentas, así como las alternativas de solución a éstas; y de manera posterior, discutir los puntos de vista iniciales y principios que debieran adoptarse a nivel industria para promover la competencia efectiva en el sector de telecomunicaciones, en un entorno seguro en el que se garantice la protección de los derechos de los usuarios.

[1] La GSMA (2006) define el spam móvil como aquellas comunicaciones que no han sido solicitadas y que son enviadas vía SMS y MMS, siendo específicamente: aquellos mensajes cortos o multimedia comerciales enviados a los usuarios sin consentimiento (mensajes de marketing); mensajes cortos o multimedia comerciales enviados a los usuarios animándolos directa o indirectamente a llamar o enviar un SMS o cualquier otra comunicación electrónica a un numero de tarifa especial; o mensajes cortos o multimedia enviados a los clientes de forma masiva y fraudulenta.

Glosario

Término	Definición
3GPP	*3rd Generation Partnership Project*
5GS	*5th Generation System*
A2P	*Application to Person*
A-MSISDN	*Addressable Mobile Station Integrated Services Digital Network Number*
API	*Application Programming Interface*
BSC	*Base Station Controller*
BTS	*Base Transceiver Station*
CAAS	*Communication as a Service*
CASL	*Canadian Anti-Spam Legislation*
CEPT	Conferencia Europea de Administraciones Postales y de Telecomunicaciones
CLI	*Calling Line Identification*
CNMC	Comisión Nacional de los Mercados y la Competencia
CPEUM	Constitución Política de los Estados Unidos Mexicanos
CRTC	*Canadian Radio-television and Telecommunications Commission*
CSCA	*Common Short Code Administration*
CST	*Communications and Information Technology Commission*
CTA	*Canadian Telecommunications Association*
CTIA	*Cellular Telecommunications and Internet Association*
DLR	*Delivery Receipt*
DNO	*Do Not Originate List*
EMS	*Enhanced Messaging Service*
EPS	*Evolved Packet System*
ESME	*External Short Message Entity*
ETSI	*European Telecommunications Standards Institute*
FCC	*Federal Communications Commission*
FNE	Fiscalía Nacional Económica
GSM	*Global System for Mobile Communications*
GSMA	*GSM Associtation*
HLR	*Home Location Register*
HPMN	*Home Public Mobile Network*
HTTP	*Hypertext Transfer Protocol*
ICO	*Information Commissioner's Office*
IFT	Instituto Federal de Telecomunicaciones
IMEI	*International Mobile Equipment Identity*

IoT	*Internet of Things*
IW/GW	*Interworking Service Center/Gateway Service Center*
LFTR	Ley Federal de Telecomunicaciones y Radiodifusión
MC	*Message Center*
MEF	*Mobile Ecosystem Forum*
MMS	*Multimedia Messaging Service*
MNO	*Mobile Network Operator*
MO	*Mobile Originated*
MS	*Mobile Station* o Estación Móvil
MSC	*Mobile Switching Center*
MT	*Mobile Terminated*
NANP	*North American Numbering Plan*
NOM	Norma Oficial Mexicana
OCDE	Organización para la Cooperación y el Desarrollo Económico
Ofcom	*Office of Communications*
OTT	*Over The Top*
P2A	*Person to Application*
P2P	*Person to Person*
PDU	*Protocol Data Unit*
PROFECO	Procuraduría Federal del Consumidor
RCS	*Rich Communication Services*
RE	*Routing Entity* o Entidad de Enrutamiento
REPEP	Registro Público Para Evitar Publicidad
RX	Receptor
SC	*Service Center*
SIM	*Subscriber Identity Module*
SIP	*Session Initiation Protocol*
SMPP	*Short Message Peer-to-Peer*
SMS	*Short Messaging Service*
SMSC	Central de Servicio de Mensajes Cortos
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TLS	*Transport Layer Security*
TRX	Transceptor
TX	Transmisor
UIT	Unión Internacional de Telecomunicaciones
UMTS	*Universal Mobile Telecommunications System*
VPN	*Virtual Private Network*

1. El Servicio de Mensajes Cortos (SMS)

El primer mensaje corto fue enviado el 3 de diciembre de 1992 por el ingeniero británico Neil Papworth, quien trabajaba para la compañía de telecomunicaciones Vodafone, y su uso se popularizó a finales de la década de 1990 y principios de la década de 2000 con la expansión de las redes de telecomunicaciones móviles y la popularidad de los teléfonos móviles (Vodafone, 2017).

El servicio de mensajes cortos permite el envío y la recepción de mensajes de texto, limitado a 160 caracteres y puede incluir letras, números y símbolos. Los mensajes cortos son una forma rápida y conveniente de comunicación que se ha vuelto muy popular en todo el mundo, por lo que, a pesar de la popularidad de otras formas de mensajería instantánea en la actualidad, los mensajes de texto siguen siendo una forma común de comunicación a nivel global para fines personales o comerciales.

Si bien, en su inicio, los mensajes cortos eran limitados en cuanto al número y tipo de caracteres que se podían enviar, con el tiempo, este servicio ha sufrido cambios en cuanto a sus capacidades. En este capítulo se describirán los antecedentes del servicio de mensajes cortos y el funcionamiento general del mismo.

1.1 Antecedentes del servicio de mensajes cortos

1.1.1 *Global System for Mobile Communications* (GSM)

Durante el desarrollo de las redes móviles en la década de 1980 se identificó que era posible enviar datos utilizando el canal de señalización. Así, un canal utilizado en las redes de telecomunicaciones fijas digitales para monitorear y verificar la red, ofrecía para las redes móviles una capacidad adicional para la entrega y recepción de datos alfanuméricos.

La Conferencia Europea de Administraciones Postales y de Telecomunicaciones (en adelante, la "CEPT"), creó en 1982 un grupo de trabajo llamado *Groupe Spécial Mobile* (más tarde conocido como *Global System for Mobile Communication*), el cual abordaba el futuro de las comunicaciones de radio móviles celulares digitales (Acker, 2014). En 1989 la CEPT traspasó el control de GSM al *European Telecommunications Standards Institute* (en adelante, la "ETSI"), marcando un cambio importante en la capacidad del organismo de normalización para hacer cumplir un memorando de entendimiento (en adelante, "MoU" por sus siglas en inglés).

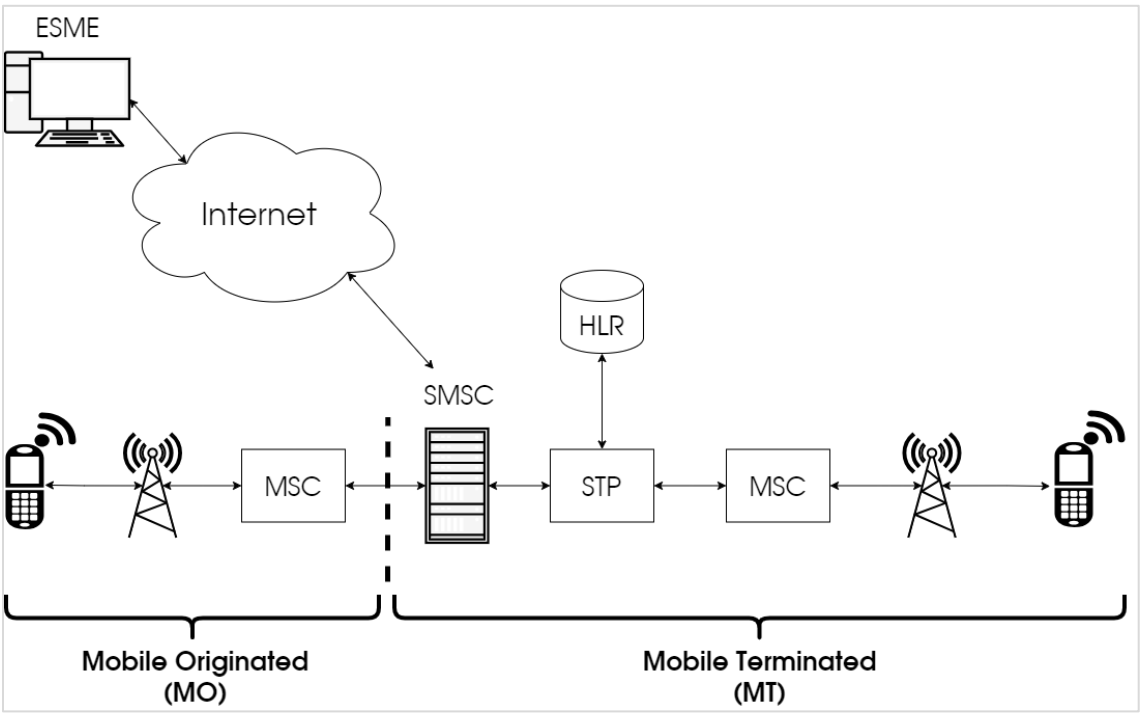
Así, el GSM estableció fases en la introducción de protocolos que requerían que los proveedores de servicios y los fabricantes de equipos homologarán todos sus dispositivos

cumpliendo con estándares técnicos, incluyendo capacidades de SMS (Hillebrand, 2010). Aunque inicialmente el servicio de SMS fue rechazado por otros grupos de trabajo y considerado como un servicio complementario opcional, el GSM decidió que sería obligatorio que los proveedores prestarán el servicio a sus suscriptores y para 1993, todos los suscriptores GSM podían enviar y recibir mensajes de texto con sus dispositivos móviles.

1.1.1.1. Arquitectura y elementos de red

La arquitectura general para la prestación del servicio de SMS se muestra en el diagrama siguiente:

Figura 1. Arquitectura típica del servicio SMS.



Fuente: Elaboración propia con base en (O. Osho, 2014).

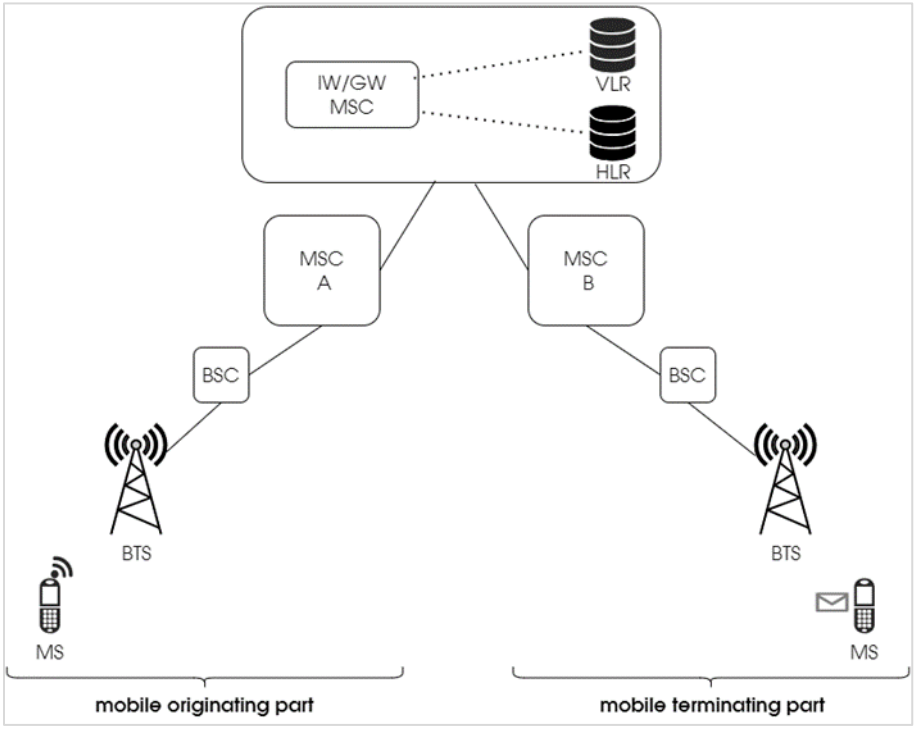
De manera simplificada, el envío de un mensaje corto se inicia desde la terminal del usuario origen el cual envía el mensaje a una Central de SMS ("*SMS Center*" o "SMSC") que en esencia funciona como un almacén de mensajes, y la cual realiza el envío del mensaje a la terminal del usuario receptor.

Para Acker (2014), el servicio de SMS se compone de tres partes interconectadas, esto desde la arquitectura básica de GSM. La primera parte de la que se compone esta red básica es el teléfono móvil o estación móvil (MS) del usuario. La MS es una terminal capaz de realizar y recibir llamadas, enviar y recibir datos dentro de una red móvil. Además,

contiene un módulo de identidad del suscriptor (tarjeta SIM) que permite a los usuarios ser facturados y localizados por sus proveedores de servicios. También tiene un número propio y único, el cual se conoce como *International Mobile Equipment Identity* (IMEI).

Cuando los usuarios envían un SMS, su teléfono transmite el mensaje corto a la segunda parte de la arquitectura de red conocida como subsistema de estación base (BSS). El BSS se compone de una estación base (BS) y un transceptor de estación base (BST). La BS o bien torre celular y un transceptor de estación base entregan el mensaje al Centro de Servicio de Mensajes (MSC) más cercano a la red. Los MSC y las bases de datos que almacenan la información para el enrutamiento y prestación de servicios, conocida como red de conmutación móvil, constituyen la tercera parte de la arquitectura de la red. Los MSC también están conectados a los Centros de Servicio de Mensajes Cortos (SMSC) para la transmisión de mensajes de texto. El SMSC localiza el teléfono del receptor a través de las bases de datos de registros de geolocalización almacenadas en la red y envía el mensaje si el teléfono del receptor está encendido, o lo mantiene en espera hasta que el mensaje pueda entregarse a un teléfono que este encendido y dentro del alcance de la cobertura de la red móvil. (Acker, 2014).

Figura 2. Arquitectura de red de GSM.



Fuente: Elaboración propia con base en Acker (2014).

La arquitectura de red básica de la estructura GSM es jerárquica y el sistema consta de dos áreas de componentes de red: la infraestructura que es fija y admite la recepción y transmisión de datos (como llamadas de voz) y los teléfonos móviles que los usuarios

utilizan mientras se mueven a través de la cobertura de la red. Los servicios de red que los operadores brindan a los usuarios utilizan la interfaz de radio para comunicar información a la infraestructura de la red.

PUNTOS CLAVE DEL CAPÍTULO 1

- El primer mensaje corto fue enviado el 3 de diciembre de 1992 por el ingeniero británico Neil Papworth.
- El Servicio de mensajes cortos se caracteriza por tener un límite de caracteres (160), en el cual se pueden incluir letras, números y símbolos.
- Los principales elementos involucrados en la prestación del servicio de mensajes cortos son: el Equipo Terminal, Subsistema de Estación Base (BSS), Centro de Servicio Mensajes (MSC) y el Centro de Servicio de Mensajes Cortos (SMSC).

2. Evolución del servicio de mensajes cortos

Desde sus inicios, el servicio de mensajes cortos ha representado un gran avance en la manera de comunicarse a distancia debido a su facilidad para expresar ideas en una cantidad limitada de caracteres. Antes de la aparición de los teléfonos inteligentes (*smartphones*), ofrecían una alternativa a soluciones como las llamadas y medios físicos como el correo tradicional, brindando movilidad en la comunicación en comparación con otros servicios de mensajería como el *email*. En este capítulo se presentará un seguimiento de la evolución que ha tenido el servicio de mensajes cortos desde su creación, identificando diferentes modalidades y mejoras del servicio a través de los años, además de un análisis de su uso en la actualidad comparado con el uso de nuevas alternativas a los SMS.

Inicialmente, el servicio de mensajes cortos solo permitía el envío de mensajes de texto entre usuarios de una misma red, lo que rápidamente fue mejorado mediante la interconexión de las redes de telecomunicaciones permitiendo con ello el intercambio de mensajes de texto entre sus usuarios. Además, la evolución tecnológica permitió expandir el uso de los mensajes cortos para dar paso a diferentes modalidades, desde tener únicamente una comunicación entre personas (en adelante, "P2P" de sus siglas en inglés "*Person to Person*"), a comunicación entre aplicaciones y personas en ambos sentidos (en adelante, "A2P" y "P2A" de sus siglas en inglés "*Application to Person*" y "*Person to Application*", respectivamente), modalidades que serán abordadas con mayor detenimiento posteriormente.

El auge de la comunicación mediante mensajes cortos originó que los usuarios requirieran más funcionalidades en este servicio, como la adición de contenido multimedia, y no únicamente texto plano limitado en caracteres. Así fue como en los inicios de la década de los años 2000, surge una evolución del servicio SMS, el EMS (siglas en inglés de "*Enhanced Messaging Service*"), que ha sido definido por el *3rd Generation Partnership Project* (en adelante, "3GPP" por sus siglas en inglés) de la siguiente manera:

> El Servicio de mensajería mejorado (EMS) se basa en el estándar SMS, pero con formato agregado al texto. El formato puede permitir que el mensaje contenga animaciones, imágenes, melodías, texto formateado y vCard y vCalendar. Objetos que pueden mezclarse en un solo mensaje (3GPP, 2022).

Le Bodic (2005) menciona que los mensajes EMS pueden contener elementos como texto con o sin formato (alineación, tamaño y estilo de letra), imágenes de mapas de bits en blanco y negro, animaciones basadas en mapas de bits en blanco y negro o melodías monofónicas; asimismo, destaca como característica de este tipo de mensajes que los elementos gráficos o melodías siempre se ubican en posiciones específicas del

texto, como si fueran un carácter más del mensaje. Además de estas funciones, con el tiempo los mensajes EMS mejoraron permitiendo características adicionales, conociéndose como *Extended EMS*, y que entre sus mejoras se encontraban las animaciones o imágenes de mapas de bits en cuatro escalas de grises o 64 colores, flujos de datos de *vCard* y *vCalendar*, melodías polifónicas y gráficos vectoriales.

Posteriormente, el avance en la tecnología permitió el surgimiento de otro servicio con contenido multimedia, el MMS (siglas en inglés de "*Multimedia Messaging Service*"), habilitado con la aparición de teléfonos con pantallas a color y cámara, así como la introducción de comunicación mediante paquetes en redes móviles, que permite a los usuarios un envío de mensajes que contienen no solo texto, sino también imágenes, video y audio y que, como ventajas adicionales respecto a los SMS, ofrecen confirmación de recepción y lectura, clasificación de mensajes y prioridades de envío, además de permitir el direccionamiento a cuentas de correo o números telefónicos, lo que representa un cambio significativo respecto al servicio de mensajes cortos del que nace la idea, pero que además trajo consigo grandes desafíos para su implementación, operación y gestión (Le Bodic, 2005).

De igual manera, la evolución tecnológica permitió el surgimiento de los servicios de comunicación enriquecida (RCS, siglas en inglés de "*Rich Communication Services*"), una plataforma de mensajería basada en estándares abiertos para la comunicación personal y comercial. RCS como aplicación comercial es particularmente interesante, ya que es la única tecnología de mensajería enriquecida que permite mensajes salientes de A2P de empresas a usuarios finales, así como mensajes entrantes de P2A de usuarios finales a empresas, marcas y otras organizaciones (MEF, 2020).

MEF (2020) señala además que los servicios RCS se consideran una evolución del servicio de mensajes cortos y está respaldado por una gran variedad de actores del mercado, que incluyen operadores móviles, empresas como Google y el ecosistema Android, incluyendo a Samsung, además de fabricantes de equipos terminales y proveedores de soluciones de mensajería. No obstante, la implementación de RCS aún enfrenta desafíos porque el enfoque de estándares abiertos que permite la amplia adopción de RCS también requiere un acuerdo sobre la implementación de tecnología fundamental y prácticas comerciales para brindar una interoperabilidad total. Asimismo, entre las mejoras que MEF destaca respecto al estándar de mensajería RCS se encuentran el envío de logo y marca, verificación de remitente, estadísticas de mensaje recibido y mensaje leído, incorporación de imágenes y videos, así como botones de respuestas sugeridas.

De tal manera que el servicio de mensajes cortos ha experimentado diferentes evoluciones, iniciando como un medio de comunicación escrita entre usuarios de una

misma red, con texto plano y limitado a una cantidad máxima de caracteres alfanuméricos, pasando de ser un servicio que permitía la conexión entre usuarios de diferentes redes a través de la interconexión de estas, a ser un servicio utilizado con fines comerciales y que, además ha experimentado la inclusión de atributos como la incorporación de imágenes y sonidos adicionales al texto enviado.

2.1 Desuso del servicio de mensajes cortos P2P y plataformas alternas

Las mejoras en la creación de equipos destinados para la comunicación, desde la invención de los primeros teléfonos y computadoras ha tenido increíbles avances respecto a su tamaño, observando una relación inversa entre el tamaño y el poder de los dispositivos como teléfonos celulares, teniendo terminales cada vez más pequeños que permiten realizar múltiples tareas sin limitarse al envío y recepción de llamadas y mensajes cortos, dando paso a teléfonos inteligentes (*smartphones*).

A grandes rasgos, se puede hablar de una diferenciación entre los teléfonos móviles antiguos y los smartphones, pues los primeros tienen un conjunto fijo de funciones de fábrica limitadas para el usuario, mientras que en los smartphones, el dueño de estos puede añadir distintas funcionalidades en forma de aplicaciones o programas, denominados comúnmente "*apps*", pudiendo ser propias del fabricante del equipo, o desarrolladas por empresas especializadas en ello (Gobierno de Navarra. Dirección General de Política Económica y Empresarial, 2023).

La GSMA (2021) señaló que la adopción de *smartphones* en América Latina se mantuvo firme en 2021, previendo que se alcanzarían 500 millones de conexiones de estos dispositivos a finales de dicho año, traduciéndose en una tasa de adopción del 74%, e indicando que para los próximos 4 años se establecerán cerca de 100 millones de conexiones nuevas de smartphones.

Por otro lado, el Instituto Nacional de Estadística y Geografía (en adelante, "INEGI") a través de la "Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2022" ha señalado que de las personas usuarias de teléfono celular en México, para 2022 se estimó que 94.6% de personas solo utilizaba smartphone, seguido del 5.2% de personas que usaron celular común y un 0.2% de encuestados usaron ambos dispositivos, lo que representó un aumento de 6.7% en las personas que usaron smartphone respecto al año 2019 (INEGI, 2023).

Lo anterior resulta relevante pues el cambio tecnológico en los teléfonos móviles, y la creciente adopción de *smartphones* alrededor del mundo ha impulsado también el uso de aplicaciones que permiten la comunicación entre usuarios como alternativas al uso

de mensajes cortos, lo que resulta en una disminución del tráfico asociado a SMS, y acrecentando la comunicación a través de alternativas que usan la transmisión de paquetes a través de *internet*, como pueden ser las denominadas aplicaciones de mensajería instantánea OTT (siglas en inglés del término "*Over The Top*"), como es el caso de *WhatsApp*, *Messenger* de *Facebook* o *Telegram*, por mencionar algunas.

La disminución del tráfico relacionado con SMS ha sido identificado y reportado por el Instituto Federal de Telecomunicaciones (en adelante, "Instituto" o "IFT") a través del "Análisis de los sectores de telecomunicaciones y radiodifusión en 2020: Valoración de los efectos de la emergencia sanitaria", en el que se realiza un comparativo de la cantidad de mensajes cortos de diciembre de 2019 a diciembre de 2020, pasando de 3,614 millones de SMS a 2,049 millones, lo que representa una disminución de trafico de este servicio del 43.4% y que visto como un promedio de mensajes cortos por línea móvil pasó de 30 SMS a 17 SMS en el mismo periodo, representado una disminución de 43.7% del uso de dicho servicio (IFT, 2021). Además, estimó que, en 2022, el 90.9% de la población usuario de teléfonos inteligentes utilizó aplicaciones de mensajería instantánea (INEGI, 2023).Asimismo INEGI estimó que, en 2022, el 90.9% de la población usuario de teléfonos inteligentes utilizó aplicaciones de mensajería instantánea.

Por otro lado, debe considerarse el incremento en la demanda de conectividad de servicios de banda ancha móvil que, de acuerdo a lo reportado por el Instituto, la expansión de la tecnología 4G ha implicado un crecimiento a nivel exponencial de la cantidad de datos gestionados a través de redes móviles, mismo que para el cuarto trimestre de 2021 contabilizó en 1,670 *Petabytes* (PB, cuya unidad equivale a 1,000,000 GB) en México, que significó un crecimiento del 19.6% respecto al consumo durante el cuarto trimestre del 2020 (1,397 PB), y que durante todo el año 2021, el tráfico total gestionado alcanzó los 6,314 PB, dando un promedio de consumo anual de 58 GB por cada acceso de internet móvil (IFT, 2022a).

Así, con el crecimiento del uso de internet móvil a través de *smartphones*, el uso de aplicaciones para mensajería instantánea ha tenido un crecimiento constante y ha propiciado un cambio en la manera en que los usuarios de servicios de telefonía móvil se comunican entre ellos. Cómo lo ha señalado el propio IFT (2022a), durante 2022 la actividad en línea con mayor frecuencia de uso fue la mensajería instantánea siendo *WhatsApp*, la principal aplicación destinada a la comunicación entre usuarios mediante mensajes escritos, la más utilizada con un 93% de uso durante 2021, presentando un crecimiento respecto al 86% y 92% reportados en 2019 y 2020 respectivamente.

2.2 Nuevos casos de uso

Si bien se ha considerado que, para la comunicación entre usuarios del servicio de telefonía móvil ha disminuido el intercambio de mensajes cortos, con la aparición y popularidad de las alternativas como *WhatsApp* y *Messenger*, el servicio de mensajes cortos ha evolucionado más allá de su uso tradicional respecto a la comunicación entre personas (P2P), y ha encontrado su lugar en nuevos casos de uso, permitiendo su adopción no solo para una interacción entre usuarios tradicionales de los servicios móviles de telecomunicaciones, sino que se ha incorporado en alternativas para la comunicación empresarial a través de sistemas tecnológicos ligados a las redes de telecomunicaciones que, mediante este tipo de mensajes se comunican para el cumplimiento de sus tareas. Entre estos casos de uso se destacan el A2P y P2A.

2.2.1 SMS A2P

La modalidad del servicio de mensajes cortos aplicación a persona (SMS A2P) ha sido reconocida y definida internacionalmente por diversos organismos y entidades relacionadas con la industria de telecomunicaciones y su regulación, cobrando relevancia en el mercado y aportando valor para mantener vigentes los SMS a nivel mundial.

En Estados Unidos de América, la Asociación de Telecomunicaciones Celulares e Internet (en adelante, la "CTIA" por sus siglas en inglés), ha definido SMS A2P como el servicio consistente en el envío de mensajes cortos a múltiples usuarios/consumidores, enviados típicamente por empresas o sus agentes, cuyos remitentes pueden ser proveedores de servicios financieros, escuelas, servicios médicos, entidades de servicio al cliente, organizaciones sin fines de lucro o campañas políticas, por mencionar algunos.

Del mismo modo en Chile, las autoridades en materia de competencia en dicho país, han ampliado la definición del servicio de mensajes cortos en su modalidad de aplicación a persona, indicando que se refiere al servicio de envío de mensajes a un abonado móvil, generalmente desde una aplicación web, como por ejemplo: códigos de verificación de usuarios, notificación de claves dinámicas de un solo uso, promociones y marketing, alertas tempranas de desastres naturales como terremotos, tsunamis, incendios forestales, aluviones y erupciones volcánicas, o cualquier servicio en el que la información deba ser enviada a uno o varios usuarios en forma de mensajes de texto (FNE, 2023).

Por su parte, la Comisión Nacional de los Mercados y la Competencia (en adelante, la "CNMC") (2021) en España, ha señalado que los SMS A2P resultan ser aquellos mensajes que son enviados desde una aplicación a un usuario móvil, y que se tratan fundamentalmente de alertas y notificaciones de los bancos, de tipo comercial o de

publicidad para la comunicación que tienen las empresas con sus clientes, además de que han ganado gran importancia para ser utilizados en procesos de verificación y seguridad, esto último asociado con servicios de telemetría y telecontrol referentes a servicios *IoT* (siglas en inglés de Internet de las Cosas).

La popularidad de esta modalidad del servicio de mensajes cortos ha propiciado la creación de empresas a nivel mundial dedicadas a la prestación del servicio de SMS con un enfoque especial hacia las empresas como los denominados agregadores de SMS, los cuales actúan como intermediario entre los remitentes que envían SMS a gran escala, y los operadores de redes públicas de telecomunicaciones para el envío del mensaje corto.

Por lo anterior, se puede observar que el servicio de mensajes cortos ha evolucionado para contar con modalidades que han sido adaptadas a las necesidades del mercado, proporcionando alternativas de comunicación no solo a los usuarios particulares de servicios de telecomunicaciones móviles, sino también a aquellos usuarios empresariales que requieren la interacción con sus usuarios a través de mensajes cortos, de manera automatizada ocasionando que alrededor del mundo los entes reguladores consideren definir la modalidad de SMS A2P.

2.2.2 SMS P2A

El envío de mensajes cortos en la modalidad A2P no representa por si sola una comunicación bidireccional, entendiendo esto último como la posibilidad de que el destinatario del SMS A2P se convierta en remitente al enviar un mensaje a la aplicación que inició la comunicación, o inclusive que sea la persona quien envié un mensaje por primera vez hacia una aplicación. Lo anterior es posible mediante el uso de mensajes cortos en la modalidad P2A.

El concepto de los mensajes cortos P2A ha sido reconocido por diferentes figuras involucradas en la industria de las telecomunicaciones alrededor del mundo, descritos como aquellos mensajes que son enviados por una persona para la interacción con una interface de aplicación (MEF, 2020), relacionándolo con el servicio de mensajes cortos A2P, al ser presentado como el inverso de este y definirlo como el proceso en que un mensaje de texto es producido desde un usuario móvil y enviado a una aplicación, lo que significa que el usuario del servicio de comunicación móvil es quien inicia la interacción con la aplicación (Autoridad de Telecomunicaciones de Pakistán, 2011).

Los usos de esta forma de comunicación son variados, y permiten a los usuarios de servicios de telecomunicaciones acceder a una comunicación más fluida con empresas en las que tienen interés, ya sea para la provisión de productos o servicios. Los

usuarios pueden utilizar los SMS P2A para realizar votaciones a distancia para una infinidad de propósitos, desde concursos en televisión o radio, o competiciones deportivas, además de ser utilizados para la suscripción a diferentes servicios a través del envío de una solicitud usando SMS en esta modalidad. Un escenario que representa el intercambio de SMS P2A es cuando el usuario recibe una solicitud de confirmación para una cita programada y puede confirmarla a través del envío de un SMS P2A a la aplicación origen del mensaje inicial.

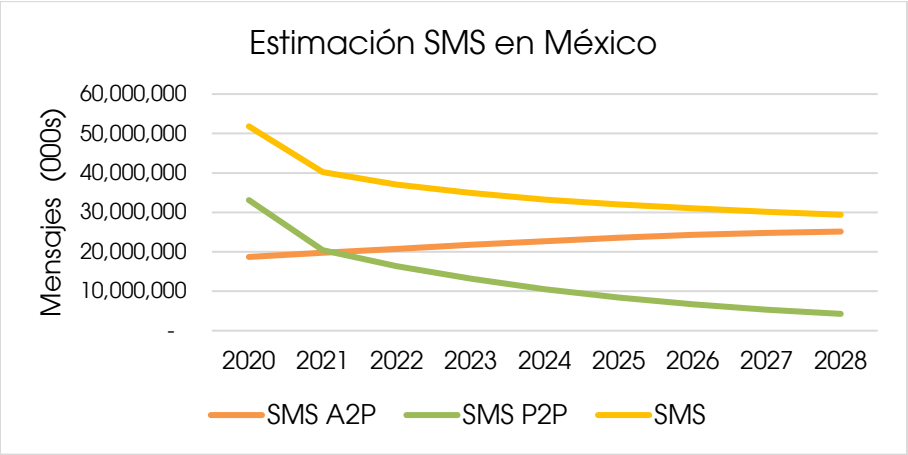
Es así que, a través del uso de SMS P2A, se puede tener una interacción bidireccional entre una aplicación y una persona como extremos de la misma, siendo un complemento a la modalidad de mensajes cortos iniciados por una aplicación, y que comercialmente representa una gran oportunidad para la interacción entre las empresas con sus clientes que son usuarios del servicio de comunicaciones móviles.

La popularidad y uso de estas modalidades para la interacción a través del servicio de mensajes cortos aumenta cada vez más, llegando a presentar crecimientos considerables en la cantidad de tráfico reportado de SMS A2P, incluso al punto de asemejar la cantidad de tráfico de SMS P2P, de acuerdo con las proyecciones.

Lo anterior ha sido reportado así por OMDIA (2023) en su informe de tráfico de mensajería móvil actualizado al año 2023, en el que se documenta la comparativa del volumen de tráfico, reportado en miles de millones de mensajes, de SMS P2P y SMS A2P, así como los ingresos derivados de dichas modalidades del servicio. En dicha comparativa del "Mobile Messaging Traffic and Revenue Forecast Report – 2023" de OMDIA, se observa que en 2020 el tráfico de SMS A2P resultaba ser la mitad respecto a los casi 5 mil millones de mensajes asociados a SMS P2P, mientras que para 2023 el tráfico de este último había disminuido a los 4.5 mil millones y a su vez los mensajes cortos A2P aumentaron a ser casi 3 mil millones, indicando una tendencia de disminución en el tráfico SMS P2P y aumento en SMS A2P que se pronostica con datos similares de tráfico para ambos servicios en el año 2028, donde se tendrán más de 3 mil millones de mensajes enviados para cada modalidad.

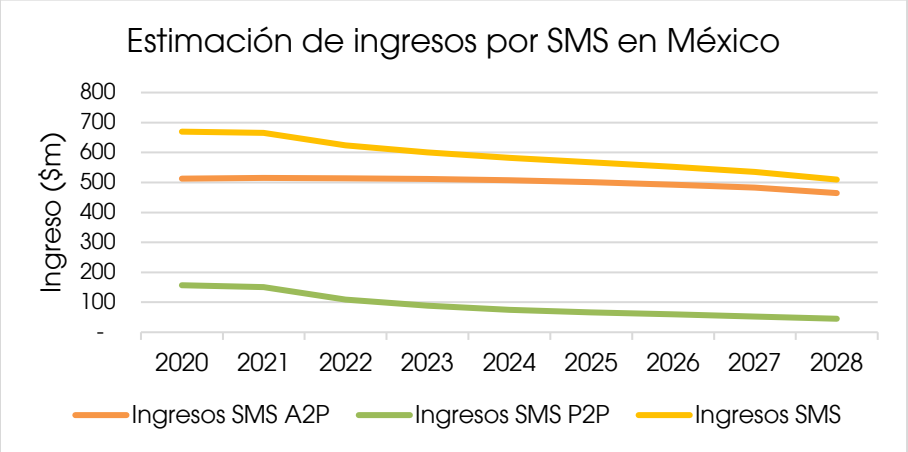
En terminos regionales, particularmente para el caso de México, el informe proporciona estimaciones de la cantidad de mensajes SMS y sus ingresos asociados, donde se puede comparar la evolución de SMS P2P y SMS A2P durante 9 años, pronosticando un descenso considerable en el uso de mensajes perosna a personas, que contrasta con el aumento en la adopción de SMS A2P, mismos que presentan ingresos considerablemente mayores a los que se obtienen con SMS P2P, pero que tienen a disminuir en el futuro. Lo anterior se representa de manera gráfica en las Figuras 3 y 4.

Figura 3. Cantidad de SMS en México. Comparativa entre SMS P2P y SMS A2P.



Fuente: Elaboración propia con datos de OMDIA (2023).

Figura 4. Ingresos por SMS en México. Comparativa entre SMS P2P y SMS A2P.



Fuente: Elaboración propia con datos de OMDIA (2023).

PUNTOS CLAVE DEL CAPÍTULO 2

- En los años 2000 el SMS evolucionó al Enhanced Messaging Service (EMS), permitiendo adicionar multimedia y no únicamente texto plano.

- Los Multimedia Messaging Service (MMS), aunado a los teléfonos con pantallas a color y cámara, permitían el envío de imágenes, videos y audio.

- Surge Rich Communication Services, aplicación comercial que permite servicios A2P y P2A y permite el envío de mensajes de texto enriquecidos mediante contenido multimedia.

- WhatsApp como servicio de mensajería instantánea entre usuarios, fue la más utilizada en 2021 en México, con un crecimiento del 92% respecto 2020.

- Se crean nuevos casos de uso: A2P, P2A.

- El servicio A2P son mensajes de texto enviados desde las empresas a través de una aplicación hacia los usuarios, de una manera automatizada acorde a las necesidades a cubrir.

- El servicio P2A son mensajes de texto enviados de un usuario a una

3. Cadena de Prestación de Servicios SMS A2P

La prestación del servicio de mensajes cortos en su modalidad A2P es posible gracias a la intervención de diferentes actores a lo largo de la trayectoria del mensaje que se pretende comunicar. Estas figuras llevan cabo actividades que permiten que exista una comunicación entre el remitente y el receptor del mensaje. En la cadena de prestación de servicios podemos encontrar elementos como los clientes corporativos encargados de la creación del mensaje corto, agregadores de SMS que fungen como intermediarios frente a múltiples operadores de telefonía móvil que presten el servicio de mensajes cortos, quienes también forman parte de la cadena de prestación del servicio, pudiendo interconectarse entre ellos para poder entregar el mensaje corto al usuario final.

3.1 Remitente (Clientes corporativos/proveedores de contenido)

Los remitentes de mensajes cortos en su modalidad A2P resultan ser clientes corporativos de diversos giros y que pueden pertenecer a diferentes sectores de la industria, como empresas comerciales que buscan con esta alternativa el envío de promociones, ofertas especiales, actualizaciones de sus productos, el recordatorio y confirmación de citas, pedidos, reservas y otros productos y/o servicios; instituciones financieras, como bancos comerciales o de inversión, *brokers* o agentes de inversión, compañías de seguros y fondos de gestión de activos, quienes utilizan los mensajes cortos A2P para enviar notificaciones de transacciones, alertas de seguridad, recordatorios de pagos, códigos de verificación relacionadas con la cuentas de sus clientes; proveedores de servicios públicos, como compañías de electricidad, gas y/o agua que encuentran en los mensajes cortos A2P una gran opción para el envío de facturas, recordatorios de pagos, notificaciones de mantenimiento y emergencias, entre otros; organizaciones gubernamentales que usan los SMS A2P para enviar alertas de emergencia, actualizaciones de seguridad, información sobre programas y/o servicios gubernamentales.

Estos actores dentro de la cadena de prestación del SMS A2P también se pueden clasificar como los proveedores de contenido, mismos que proveen la información, con independencia de su naturaleza, formato o cualidades específicas, a través de SMS. En este escenario, los clientes corporativos son los proveedores de contenido directamente con los operadores de redes públicas de telecomunicaciones, sin requerir intermediarios como los agregadores, mismos que se explican a continuación.

3.2 Agregadores

Entre los actores que pueden formar parte de la cadena de prestación de servicios SMS A2P, podemos señalar a aquellas organizaciones y/o empresas dedicadas a mantener una relación directa con los diferentes operadores de redes públicas de telecomunicaciones para la entrega y procesamiento de mensajes cortos A2P para la difusión del mensaje de clientes corporativos remitentes.

De esta manera, los agregadores de mensajes cortos A2P actúan como intermediarios entre las empresas y/u organizaciones y los operadores de redes facilitando con ello la conectividad al establecer acuerdos con múltiples operadores de redes públicas, gestionando las plataformas para el envío y administración de los mensajes cortos, las listas de destinatarios, la programación de envíos y hasta la personalización de los mensajes. Asimismo, los agregadores de SMS ofrecen niveles de servicio, garantizando la entrega de los mensajes en determinado tiempo. Su integración en la cadena de prestación del servicio SMS A2P puede ser empleando una conexión directa con los operadores de redes públicas de telecomunicaciones, o inclusive existiendo como intermediarios entre los clientes corporativos y otros agregadores conectados directamente con múltiples redes públicas de telecomunicaciones.

3.3 Operadores de redes públicas de telecomunicaciones

Los operadores de redes públicas de telecomunicaciones pueden ser identificados como cualquier persona, sea física o moral, que es titular de una concesión única o de red pública de telecomunicaciones, mediante la cual se le confiere el derecho para la prestación de servicios públicos de telecomunicaciones.

Técnicamente, los operadores de redes públicas de telecomunicaciones despliegan y mantienen la infraestructura de red necesaria para el funcionamiento de los servicios públicos de telecomunicaciones que le permiten prestar, tanto a usuarios como a otros concesionarios. La infraestructura desplegada por los operadores de redes públicas de telecomunicaciones pueden ser, sin limitar, equipos de conmutación y sistemas de enrutamiento del tráfico asociado a los servicios prestados, cableado, y obra civil necesaria para el despliegue de la misma, y en su caso, estaciones base y antenas para la comunicación inalámbrica entre sus dispositivos y/o los dispositivos de los usuarios, para lo que es necesario contar con títulos de concesión para el uso de espectro radioeléctrico asociado a la prestación de servicios de telecomunicaciones.

3.4 Usuarios de servicios de telecomunicaciones (Destinatarios)

Para la existencia de cualquier tipo de comunicación se requiere de al menos dos participantes, uno de ellos quien será el encargado de transmitir el mensaje y, por otro lado, se requiere de un receptor de este, quien decodificará e interpretará el mismo

para obtener la información que inicialmente se quería transmitir. Así, como parte de la cadena de prestación del servicio de mensajes cortos A2P, los usuarios de servicios de telecomunicaciones son los destinatarios de los mensajes cortos generados por los remitentes que buscan transmitir un mensaje que pueda resultar relevante para quien lo recibe.

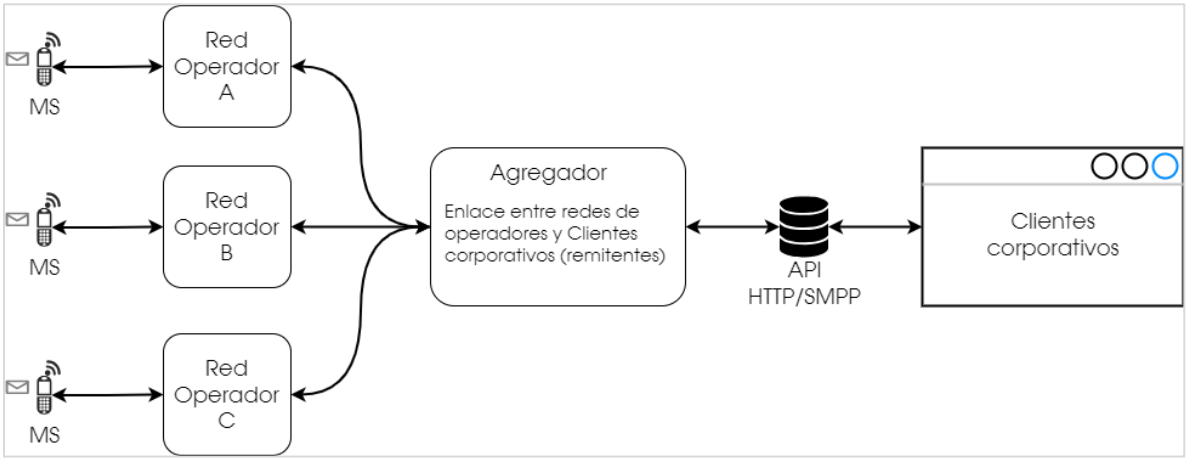
En México, el usuario ha sido definido en la LFTR como toda persona, sea física o moral, que utiliza un servicio de telecomunicaciones como destinatario final, y en la misma se han establecido derechos que ejercerán al usar los diferentes servicios públicos de telecomunicaciones ofrecidos a través de la o las redes públicas de telecomunicaciones de los concesionarios con los que decidan recibirlos.

En términos generales, lo señalado para cada una de figuras que llevan cabo actividades en la cadena de prestación de SMS A2P se sintetiza a continuación:

1. Remitente: Aquel usuario de servicios de telecomunicaciones o entidad que realiza el envío del mensaje corto A2P, siendo este una empresa, una organización o un sistema automatizado.
2. Agregador de SMS: Agente que actúa como intermediario entre el remitente y los operadores de redes públicas de telecomunicaciones para el envío del mensaje corto.
3. Operadores de redes públicas de telecomunicaciones: organizaciones que despliegan y operan redes públicas de telecomunicaciones mediante las cuales se procesa y transporta el tráfico relacionado con el servicio de mensajes cortos A2P a través de la infraestructura que las compone. El tráfico puede transportarse a lo largo de una sola red pública de telecomunicaciones desde el remitente hasta el destinatario, o entre redes públicas de telecomunicaciones en caso de que los usuarios finales no se encuentren en una misma red, lo anterior mediante los acuerdos de interconexión que los operadores tengan firmados para el intercambio del tráfico asociado al servicio.
4. Destinatario: Aquel usuario de servicios de telecomunicaciones que recibe el mensaje corto A2P en un dispositivo con las capacidades técnicas apropiadas para su recepción e interpretación.

Lo anterior se puede ejemplificar mediante las siguientes figuras, donde en la Figura 5 se puede observar el escenario en el que existe un agregador que funge como intermediario entre las redes públicas de telecomunicaciones y los clientes corporativos remitentes, y que además son los proveedores de contenidos para los operadores.

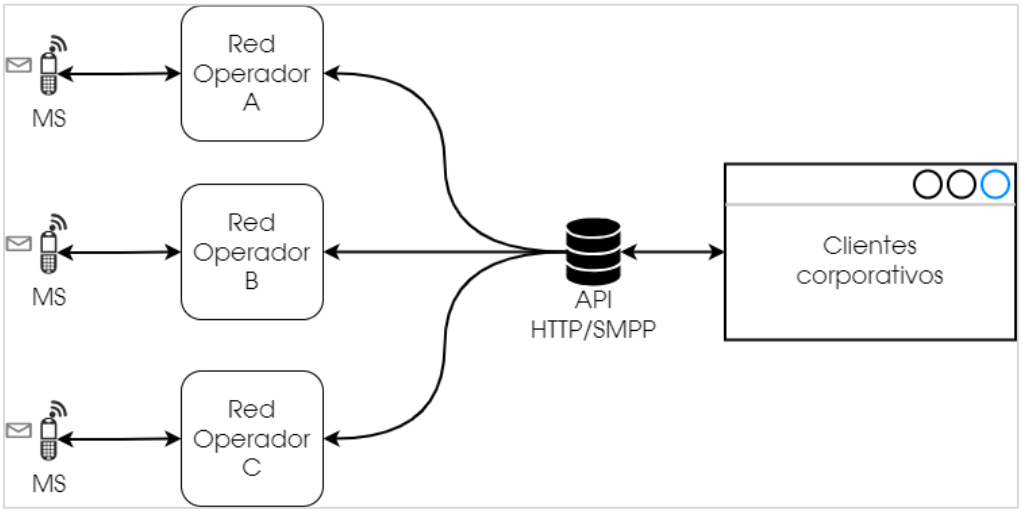
Figura 5. Cadena de prestación de SMS A2P con agregador como intermediario entre los clientes corporativos y los operadores de redes públicas de telecomunicaciones.



Fuente: Elaboración propia

En la Figura 6 se representa el escenario en el que no existe un intermediario, por lo que el cliente corporativo es el proveedor de contenido para los operadores de redes públicas de telecomunicaciones para la generación y envío de SMS A2P.

Figura 6. Cadena de prestación de SMS A2P.



Fuente: Elaboración propia

Cuando el remitente requiere enviar mensajes, el proceso lo puede realizar a través de un agregador de SMS, figura que dentro de la cadena se encarga de facilitar la conexión entre los remitentes y los operadores de redes públicas de telecomunicaciones, simplificando los acuerdos comerciales y técnicos que, de otra manera los primeros tendrían que realizar de manera independiente con cada operador de red pública de telecomunicaciones, facilitando con ello la distribución y envío de los mensajes cortos. De esta manera, los operadores reciben el mensaje corto

y lo transportan a través de la infraestructura que compone sus redes públicas de telecomunicaciones, lo que podría requerir acuerdos de interconexión entre diferentes operadores para el intercambio del tráfico para alcanzar a los destinatarios en caso de que estos se encuentren en una red distinta a la que inició el tráfico del mensaje corto. Así, el destinatario recibe el mensaje corto mediante los dispositivos terminales que sean capaces de su recepción e interpretación.

PUNTOS CLAVE DEL CAPÍTULO 3

- La cadena de prestación de SMS A2P se compone del remitente, agregador, operadores de redes públicas de telecomunicaciones y el destinatario.
- Los remitente A2P en su mayoría resultan ser clientes corporativos; instituciones financieras, proveedores de servicios públicos y organizaciones gubernamentales.
- Los Agregadores actúan como intermediarios entre los remitentes y los operadores de redes facilitando la conectividad y el enrutamiento, gestionando las plataformas para el envío, administración, programación y personalización de los mensajes cortos.
- Los Operadores de Redes Públicas de Telecomunicaciones son las entidades encargadas de operar y dar mantenimiento a las redes de telecomunicaciones (móviles o fijas), a través de las cuales los mensajes cortos son transmitidos.
- Destinatarios son los usuarios de redes de telecomunicaciones quienes requieren de dispositivos técnicamente sean capaces de la recepción, interpretación y presentación del mensaje corto

4. Funcionalidades técnicas del servicio de mensajes cortos A2P

A diferencia del servicio tradicional de mensajes cortos P2P, la modalidad de envío Aplicación a Persona (A2P) requiere de funcionalidades y características adicionales para su prestación efectiva. Dado que los mensajes cortos A2P a menudo implican grandes volúmenes de mensajes, las soluciones técnicas que deben ser implementadas para su prestación deben ser lo suficientemente robustas y escalables, principalmente en la red a cargo de la terminación de los mensajes cortos, a fin de contar con la capacidad de manejar altos volúmenes de tráfico que suelen comportarse de manera atípica respecto al tráfico persona a persona, como es el caso de mensajes cortos para campañas publicitarias o alertas de emergencia, los cuales son enviados de manera masiva y en poco tiempo.

Además, en muchos escenarios, se debe garantizar la entrega oportuna del mensaje corto, por ejemplo, las notificaciones de transacciones bancarias, por lo que la red destino debe priorizar estos mensajes sobre el tráfico de mensajes convencionales los cuales pueden ser encolados para su entrega. En otros casos, es del interés del remitente de los mensajes cortos A2P, contar con la confirmación o estatus de entrega, por lo que la red en la que se encuentre el usuario destino debe generar la información correspondiente.

En tal sentido, para asegurar una prestación exitosa y confiable del servicio A2P, es necesario contar con una serie de funcionalidades técnicas adicionales a las necesarias para su prestación en la modalidad P2P, cuya operación puede ser definida principalmente a través del protocolo de comunicación SMPP (siglas en ingés de *Short Message Peer-to-Peer)* y mediante las funciones de la red en la que se encuentran los usuarios destino.

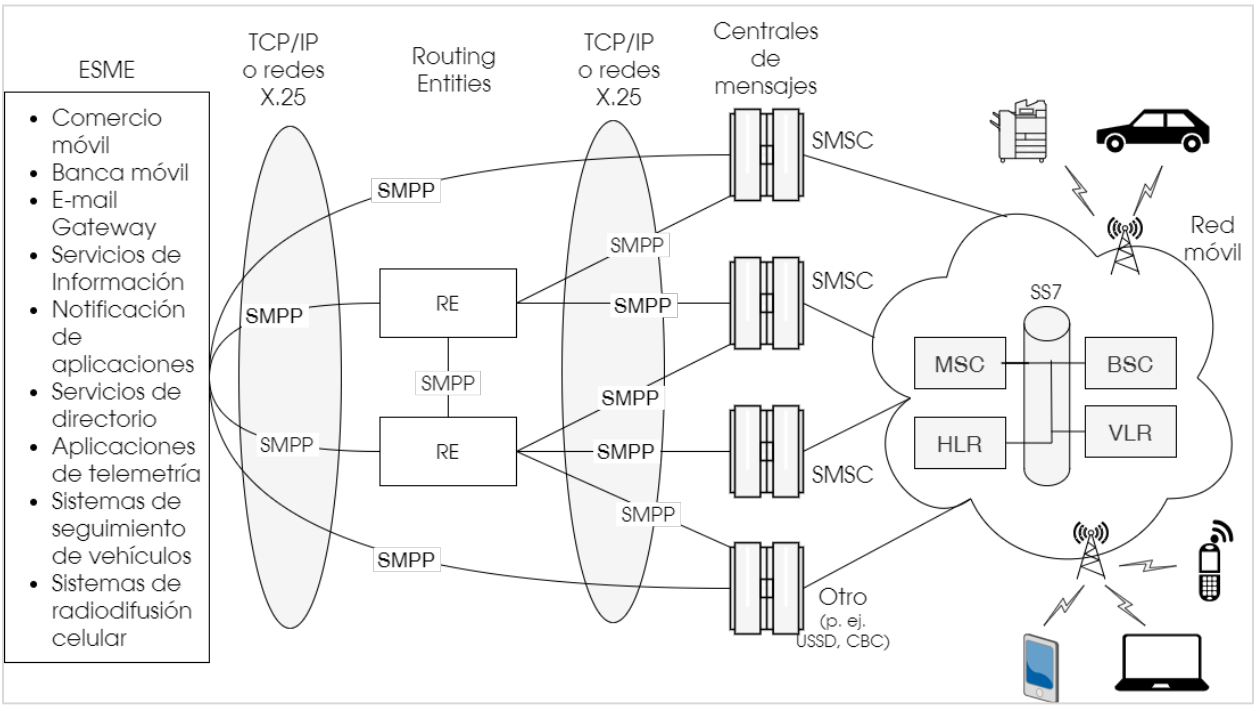
4.1 Prestación del servicio de mensajes cortos A2P en redes móviles y fijas

Si bien el estándar del 3GPP (2022) describe el servicio de mensajes cortos para redes GSM/UMTS/EPS/5GS, en este solo se especifica la parte de las comunicaciones entre las MS y el Centro de servicio (González Gómez, 2002), por lo que para el caso de la comunicación con entidades diferentes a las estaciones móviles se debe considerar un protocolo que permita el intercambio de mensajes de dichas entidades con el centro de servicio. Particularmente se hace mención del protocolo de comunicación SMPP.

El SMPP es un protocolo estándar abierto, diseñado para proporcionar una interfaz de comunicaciones de datos flexible para transferir datos de mensajes cortos entre entidades externas de mensajes cortos (por sus siglas en inglés, ESME), entidades de enrutamiento (por sus siglas en inglés, RE) y central de mensajes (por sus siglas en inglés, MC). Es un medio por el que las aplicaciones pueden enviar y recibir mensajes cortos desde y hacia dispositivos móviles. Las aplicaciones hacen esto mediante una conexión SMPP a un SMSC, *SMS gateway*, *SMPP gateway* o un *hub* (SMPP Developers Forum, 2019).

El protocolo puede ser usado al establecer una sesión SMPP entre la ESME y el Centro de mensajes o la entidad de enrutamiento SMPP. La sesión se basa en una conexión TCP/IP de capa de aplicación entre la ESME y la MC/RE, iniciada generalmente por la ESME. Dicha conexión se realiza a menudo a través de Internet y puede usar SMPP sobre TLS (*Transport Layer Security*) o una VPN (*Virtual Private Network*) para asegurar la conexión.

Figura 7. Diagrama de red SMPP con elementos que la integran.



Fuente: Elaboración propia a partir de SMPP Developers Forum (2003).

Las sesiones iniciadas por ESME pueden ser de tres tipos:

- Transmisor (TX): Autenticándose como transmisor, la ESME puede enviar mensajes cortos a la MC para el envío posterior a las estaciones móviles. La sesión Transmisor también permitirá que la ESME cancele, consulte o reemplace los mensajes enviados anteriormente. Los mensajes enviados de esta manera se denominan mensajes terminados en móviles (MT, siglas en inglés de *Mobile Terminated*).

- Receptor (RX): Una sesión de receptor permite que la ESME reciba mensajes de la MC. Los mensajes de este tipo normalmente se originan en dispositivos móviles y se denominan mensajes originados en móviles (MO, siglas en inglés de *Mobile Originated*).
- Transceptor (TRX): Combinación de TX y RX, de modo que una sola sesión SMPP se puede usar para enviar mensajes MT y recibir mensajes MO.

Para la operación del protocolo SMPP, las operaciones de solicitud y respuesta se definen como PDU (siglas en inglés de *Protocol Data Unit*), utilizados para el intercambio de mensajes cortos entre la ESME y la SMSC, consistiendo en un PDU de solicitud que tiene asociado un PDU de respuesta.

La adopción del protocolo SMPP resulta bastante relevante considerando que es un protocolo abierto, es decir, un estándar de comunicación que se encuentra disponible públicamente, sin restricciones a entidades o empresas en específico, por lo que cualquier desarrollador puede utilizarlo e implementarlo para la comunicación de las aplicaciones que desarrollen con los sistemas y dispositivos asociados al servicio de mensajes cortos, aplicándolo en la modalidad A2P. Su naturaleza permite la interoperabilidad en diferentes redes de telecomunicaciones y sus tecnologías, y provee facilidades para su aplicación en diferentes casos de uso, permitiendo el envío, recepción o intercambio de mensajes entre las entidades externas y los dispositivos móviles de los usuarios a través de elementos que conforman las redes públicas de telecomunicaciones.

A continuación, se describirán algunas funcionalidades asociadas al protocolo SMPP que se han considerado relevantes para la prestación del servicio de mensajes cortos en la modalidad A2P.

4.1.1 BIND

El propósito de la funcionalidad BIND en SMPP es registrar la ESME con el SMSC y solicitar una sesión SMPP a través de esta conexión de red para el envío y entrega de mensajes. De esta forma, la operación BIND puede considerarse como una forma de solicitud de inicio de sesión del SMS para autenticar la ESME que desea establecer una conexión.

La ESME puede establecer un BIND con el SMSC como transmisor (ESME Transmisor), Receptor (ESME Receptor) o transceptor (ESME Transceptor). Hay tres PDU de BIND en SMPP para admitir los diferentes modos de operación, como son, "*bind_transmitter*", "*bind_transceiver*" y "*bind_receiver*". El valor del campo "*command_id*" especifica qué PDU se está utilizando.

La ESME puede realizar BIND como transmisor y receptor utilizando operaciones "*bind_transmitter*" y "*bind_receiver*" por separado (después de haber establecido dos conexiones de red independientes). Alternativamente, la ESME también puede realizar BIND como transceptor después de haber establecido una única conexión de red.

Si un SMSC no admite las operaciones "*bind_transmitter*" y "*bind_receiver*", deberá devolver un mensaje de respuesta con un error "*Invalid Comand ID*" y la ESME deberá intentar realizar BIND utilizando la operación "*bind_transceiver*". Asimismo, si una SMSC no admite el comando "bind_transceiver", deberá devolver un mensaje de respuesta con un error "Invalid Comand ID" y la ESME deberá intentar realizar BIND utilizando las operaciones "*bind_transmitter*" y "*bind_receiver*", o ambas, según corresponda (SMPP Developers Forum, 1999).

De lo anterior se puede observar que la operación BIND resulta imprescindible para la implementación de la modalidad A2P en el servicio de mensajes cortos, mediante el protocolo SMPP, pues dicha operación marca el inicio de las comunicaciones entre los elementos externos (ESME) que interactúan con las centrales de mensajes (SMSC) que forman parte de la arquitectura de las redes públicas de telecomunicaciones.

4.1.2 DLR (*Delivery Receipt*)

Dentro de las operaciones "*submit_sm*" o "*data_sm*" entre la ESME y la SMSC pueden ser transferidos mensajes especiales como el "*SMSC delivery Receipt*", un tipo de mensajes utilizado para llevar un recibo de entrega de la SMSC. La SMSC, al detectar el estado final de un mensaje corto registrado y almacenado, deberá generar un mensaje de recibo dirigido a la ESME remitente del mensaje. El "*SMSC Delivery Receipt*" se lleva como carga de datos de usuario en la operación "deliver_sm" o "data_sm" (SMPP Developers Forum, 1999).

SMPP Developers Forum (1999), en el Apéndice B del estándar SMPP v3.4, presentan el formato correspondiente a un ejemplo típico de un DLR, entre los que podemos encontrar el ID único del mensaje entregado, la cantidad de mensajes enviados, la cantidad de mensajes entregados con éxito al destinatario, fecha de envío y fecha de entrega, estado de entrega del mensaje, código de error en caso de existir estos al momento de la entrega del mensaje, así como texto adicional que puede incluir detalles sobre la entrega.

En este sentido, los DLR son una funcionalidad del protocolo SMPP correspondientes a informes generados por la SMSC una vez que ha procesado y entregado el mensaje corto al destinatario final, permitiendo una retroalimentación para la ESME remitente sobre el estatus que alcanzó el mensaje enviado, incluyendo detalles específicos de

este. De lo anterior, resulta importante destacar que este tipo de mensajes especiales no representan en si un mensaje corto, pues los mismos no tienen como finalidad la comunicación entre los usuarios finales de servicios públicos de telecomunicaciones, sino un informe de entrega generado por elementos de la red (como lo es la SMSC) a la ESME remitente mediante PDU específicos del protocolo SMPP.

4.1.3 Throttling

El protocolo SMPP contine funciones que ayudan a gestionar y regular el flujo de mensajes cortos, evitando así la sobrecarga tanto del ESME como del servidor SMPP. Esta característica se centra en establecer y mantener un equilibrio en la tasa de envío de mensajes para asegurar la estabilidad de la red, a través de la cuál se definen los límites en el número de mensajes que un cliente puede enviar en un período determinado, y son usualmente configurados por el servidor SMPP, durante el proceso de conexión inicial BIND.

Durante la comunicación, si un cliente excede la tasa permitida de mensajes, el servidor responde con un error específico de *throttling,* como el código de error "*esme_rthrottled*".

La implementación de prácticas de *throttling* depende tanto de la capacidad del servidor SMPP para manejar y aplicar las restricciones de envío, el dimensionamiendo de la red que recibe los mensajes cortos, y el acuerdo establecido con la red que envía los mensajes, para garantizar que estos sean procesados de manera eficiente.

4.1.4 Priorización de mensajes

El protocolo SMPP permite asignar diferentes niveles de prioridad a los mensajes cortos durante su envío, asegurando que aquellos considerados como más urgentes o importantes sean procesados y entregados primero. Esto se realiza a través de la función "*priority_flag*" en el comando "*submit_sm*", permitiendo establecer un rango de prioridad, generalmente desde 0 (baja) hasta 3 (alta).

Esta función es especialmente útil para escenarios donde el tiempo de entrega de un mensaje puede tener un impacto significativo, como en alertas de emergencia o transacciones financieras críticas, sin embargo, es importante tener en cuenta que la implementación real y aplicación de las prioridades de los mensajes también dependen en gran medida de las políticas y capacidades del operador de la red móvil. No todas las redes soportan la diferenciación de prioridades de la misma manera, y algunas pueden tener sus propias reglas para manejar mensajes de diferentes niveles de prioridad. Por lo tanto, el uso efectivo de la priorización de mensajes en SMPP requiere

de un un entendimiento claro de las capacidades y limitaciones entre el remitente y la red destino.

PUNTOS CLAVE DEL CAPÍTULO 4

- En el servicio de mensajes cortos, es factible que una de las partes en la comunicación no sea una estación móvil, siempre que se disponga de las capacidades técnicas necesarias para permitir la interacción entre los remitentes y destinatarios de los mensajes.

- El protocolo SMPP es crucial por su naturaleza abierta y pública, lo que posibilita su empleo por cualquier desarrollador para aplicaciones de mensajes cortos, fomentando la interoperabilidad en múltiples redes y tecnologías. Esto facilita su utilización en diversas situaciones y permite la comunicación entre entidades externas y dispositivos móviles a través de redes públicas de telecomunicaciones.

- La operación BIND es esencial para habilitar la modalidad A2P en el servicio de mensajes cortos utilizando el protocolo SMPP. Esta operación inicia las comunicaciones entre los elementos que interactúan con las SMCS en la arquitectura de las redes públicas de telecomunicaciones, permitiendo así el acceso al usuario final a través de sus dispositivos móviles.

- Los DLR en SMPP son informes de entrega de mensajes generados por el SMSC para notificar el estado de un mensaje al remitente. Ofrecen detalles sobre la entrega al destinatario final. Es importante tener en cuenta que los DLR no constituyen mensajes independientes.

- Las funciones de *throttling* ayudan a gestionar y regular el flujo de mensajes cortos, evitando así la sobrecarga tanto del ESME como del servidor SMPP. Son usualmente configurados por el servidor SMPP, durante el proceso de conexión inicial BIND.

- El protocolo SMPP permite asignar diferentes niveles de prioridad a los mensajes cortos durante su envío, asegurando que aquellos considerados como más urgentes o importantes sean procesados y entregados primero. La aplicación de las prioridades de los mensajes también depende en gran medida de las políticas y capacidades del operador de la red móvil destino.

5. Prácticas no deseadas asociadas al servicio de mensajes cortos A2P

El servicio de mensajes A2P resulta una herramienta valiosa para empresas y usuarios al facilitar una comunicación rápida y eficiente a través de mensajes de texto. Esta modalidad ha representado grandes beneficios comerciales al permitir a las empresas de cualquier mercado la promoción de sus productos de manera directa y personalizada a los usuarios, además de posibilitar el envío de notificaciones importantes y el establecimiento de una comunicación directa con sus clientes, como medio de confirmación de transacciones o trámites, así como la solicitud y aceptación de servicios ofrecidos por las empresas.

Si bien la modalidad de SMS A2P cuenta con grandes beneficios, es cierto también que han surgido prácticas no deseadas asociadas al servicio de mensajes cortos A2P. Entre los usos no deseados podemos incluir, como ejemplo, el envío de mensajes cortos que no han sido autorizados y/o solicitados, cuya práctica es conocida como *spam*.

Entre los perjuicios que pueden asociarse al envío *spam* a través de mensajes cortos A2P, además de la afectación a la privacidad de los usuarios, los mensajes enviados sin autorización pueden contener enlaces maliciosos que podrían comprometer la integridad de los dispositivos o que buscan obtener información personal y/o confidencial; además de que la recepción de mensajes promocionales que no han sido autorizados pueden resultar irrelevantes para los usuarios, generando molestia por la recepción constante de estos, y ocasionando con ello una mala percepción del servicio proporcionado por los concesionarios y operadores de redes públicas de telecomunicaciones que les ofrecen el servicio, así como desconfianza en los remitentes de dichos mensajes.

Por otro lado, las prácticas no deseadas mediante SMS A2P pueden generar un alto consumo de los recursos que las redes de telecomunicaciones destinadas para la provisión del servicio, generando afectaciones técnicas y operativas, que derivan en un aumento en costos y trabajos de mantenimiento para las redes afectadas.

En este capítulo se dará un contexto general de algunas de las prácticas no deseadas que se han considerado más relevantes en la prestación del servicio de mensajes cortos en su modalidad A2P, considerando la manera en que se aplican dichas prácticas y las afectaciones que pueden generar en el entorno del servicio.

5.1 Spam

Una de las prácticas más presentes a nivel mundial, y que es fácilmente asociada por las personas es el *spam,* pues no está limitado al servicio de mensajes cortos, sino que también es común asociar dicha práctica a los correos electrónicos, como un antecedente a su aplicación mediante SMS.

El término "*spam*" ha sido ampliamente definido alrededor del mundo, pudiendo encontrar una gran cantidad de documentación asociada a la problemática, y que puede ser abordada en términos generales o particulares dependiendo del servicio en el que se aplique. Por su parte, la GSMA (2006) define el spam móvil como aquellas comunicaciones que no han sido solicitadas y que son enviadas vía SMS y MMS, siendo específicamente: aquellos mensajes cortos o multimedia comerciales enviados a los usuarios sin consentimiento (mensajes de *marketing*); mensajes cortos o multimedia comerciales enviados a los usuarios animándolos directa o indirectamente a llamar o enviar un SMS o cualquier otra comunicación electrónica a un numero de tarifa especial; o mensajes cortos o multimedia enviados a los clientes de forma masiva y fraudulenta.

Por otro lado, MEF (2020a) lo define en términos amplios como un mensaje no solicitado o no deseado por el destinatario, sin importar que dicho mensaje haya sido enviado con buenas o malas intenciones.

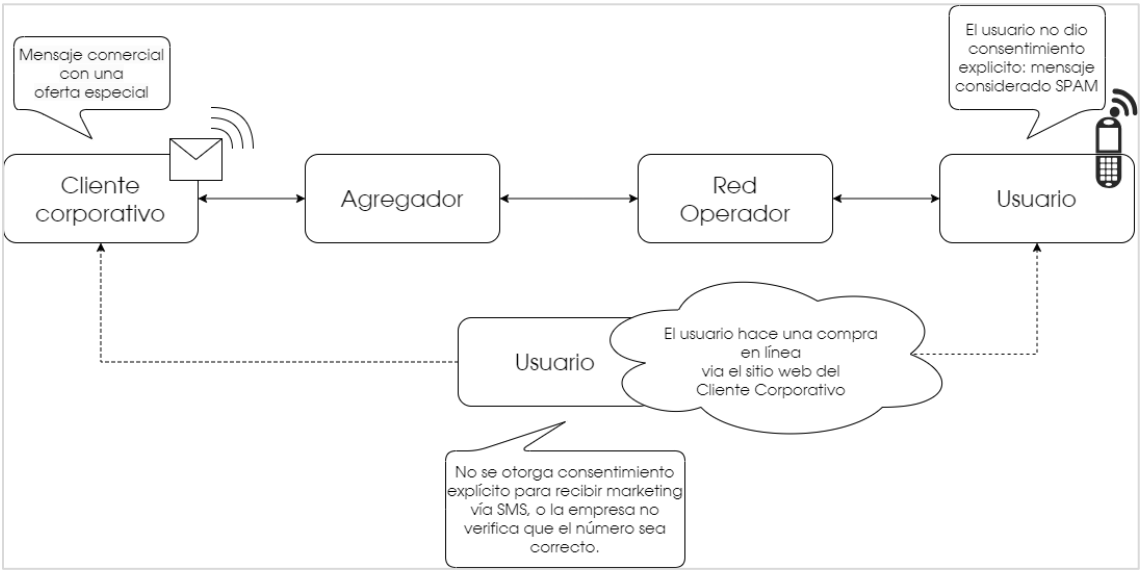
Existen diferentes formas para optar o dar permiso para recibir mensajes comerciales, como aceptar mediante un registro en línea o de forma física y debe tenerse en cuenta además que los mensajes transaccionales son solicitados por el usuario para una transacción específica y se entrega una sola vez (MEF, 2021a).

Asimismo, desde una perspectiva de redes de telecomunicaciones por las que se transporta el tráfico asociado al servicio de mensajes cortos, siendo el *spam* un acto de envío masivo de mensajes a una gran cantidad de usuarios en periodos cortos de tiempo, a modo de ráfagas, esto genera afectaciones como saturación en los equipos encargados del transporte y procesamiento del tráfico, comprometiendo todos los servicios que conviven en la redes al ser estas multiservicios, traduciendo lo anterior en molestia a los usuarios, y en costos adicionales para los operadores de red, al destinar recursos económicos, materiales y humanos para el mantenimiento correctivo de la red.

Lo anterior resulta crítico y altamente relevante, sobre todo si se considera la velocidad con la que esta actividad crece cada año, pues de acuerdo con estudios realizados por Truecaller (2022), en Estados Unidos de América el promedio de *spam* de mensajes cortos fue de 19.5 mensajes cortos mensuales por usuario durante 2022, representando un incremento significativo año con año, pues se observaron promedios de 16.9, 14.7, 10.6 y 8.5 mensajes cortos en los años 2021, 2020, 2019 y 2018 respectivamente.

En la Figura 8 se ejemplifica el caso de envío de spam, en el cual, el usuario destino es identificable al haber proporcionado su número telefónico con un propósito distinto a ser contactado con fines comerciales, no obstante, el envío de *spam* no está limitado a este escenario, pues sin los controles adecuados, remitentes malintencionados pueden realizar el envío aleatorio a números que formen parte del plan de numeración nacional.

Figura 8. Spam en SMS.



Fuente: Elaboración propia a partir de diagramas de MEF (2021a).

5.2 Flooding

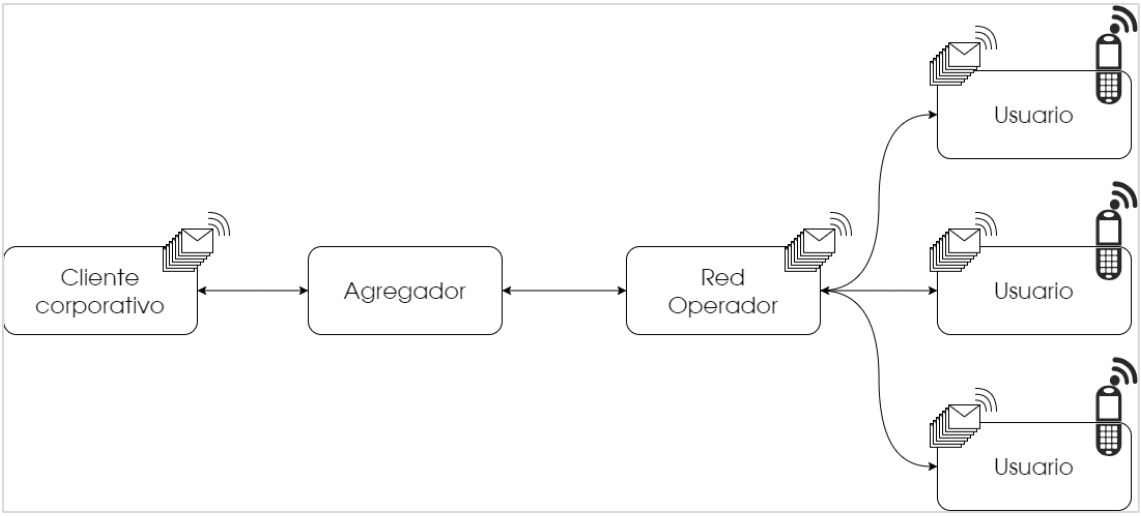
Otra práctica no deseada en la prestación del servicio de mensajes cortos en redes de telecomunicaciones y con afectaciones similares a las provocadas por el spam en SMS es el *flooding*. Esta práctica ha sido reconocida por la GSMA (2013) dentro de los problemas en el servicio de mensajes cortos que enfrentan los operadores móviles.

El *flooding* en SMS se presenta cuando un gran número de mensajes es enviado a uno o más destinatarios, pudiendo ser mensajes validos o no, y la práctica no deseada se configura cuando la cantidad de mensajes enviados es un número extraordinario en comparación con el promedio de carga normal y el valor máximo esperado de mensajes. Así, cuando el parámetro es inusualmente alto y sin otra explicación, se puede considerar que se está cometiendo *flooding* (GSMA, 2013).

El significado del término *flooding* se refiere a la situación en la que un área determinada es cubierta con agua, y literalmente se traduce como "inundación", por lo que la práctica no deseada asociada al servicio de mensajes cortos toma este nombre como

una metáfora al concepto comúnmente asociado a cuestiones climáticas, ya que la inundación es representada como una saturación en la capacidad de procesamiento de los elementos de red y dispositivos que intervienen el servicio de mensajes cortos.

Figura 9. Flooding en SMS.



Fuente: Elaboración propia.

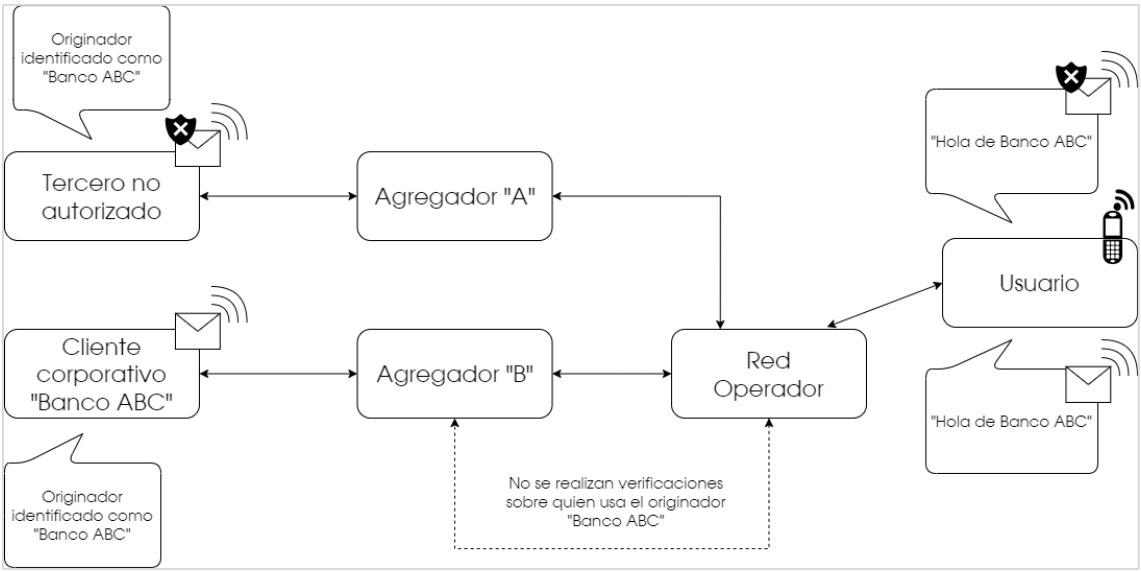
5.3 Spoofing

El *spoofing* representa otro uso no deseado para las comunicaciones electrónicas como llamadas o mensajes cortos a través de redes públicas de telecomunicaciones. En el caso del servicio de mensajes cortos, con el *spoofing* se manipula el número del remitente del mensaje corto para que parezca que proviene de una fuente legitima y confiable, con el fin de engañar a los destinatarios para que el tercero no autorizado realice acciones ilícitas que pueden generarles una afectación, como proporcionar información como datos personales sensibles o aquellos asociados a cuentas bancarias, además de persuadir a los destinatarios de hacer clic en enlaces maliciosos.

En términos de seguridad, el *spoofing* en el servicio de mensajes cortos está relacionado con el uso ilegal del SMSC de la red móvil pública local (HPMN SMSC, por sus siglas en inglés) por parte de un tercero (entidad externa), para lo cual, se manipula el Número de Directorio Internacional de Suscriptor Móvil (A-MSISDN, siglas en inglés de *Addressable Mobile Station Integrated Services Digital Network Number*) que origina el mensaje corto para poder hacer uso del SMSC de la red móvil pública local (GSMA, 2020).

En este sentido, el *spoofing* aprovecha la identificación de un suscriptor real de la red origen, pero el mensaje corto no es generado por dicho suscriptor, sino por una entidad externa que obtiene acceso a la red haciéndose pasar por el usuario real y aprovechar esto para el envío de mensajes cortos, tal como se muestra en la Figura 10.

Figura 10. Spoofing en SMS.



Fuente: Elaboración propia a partir de diagramas de MEF (2021a).

5.4 Rutas grises

MEF (2020) define a las rutas grises como aquellas por las que se envían mensajes cortos A2P desde otro país, disfrazados como mensajes P2P, con el objetivo de aprovechar las tarifas de interconexión más bajas (o nulas) entre las redes.

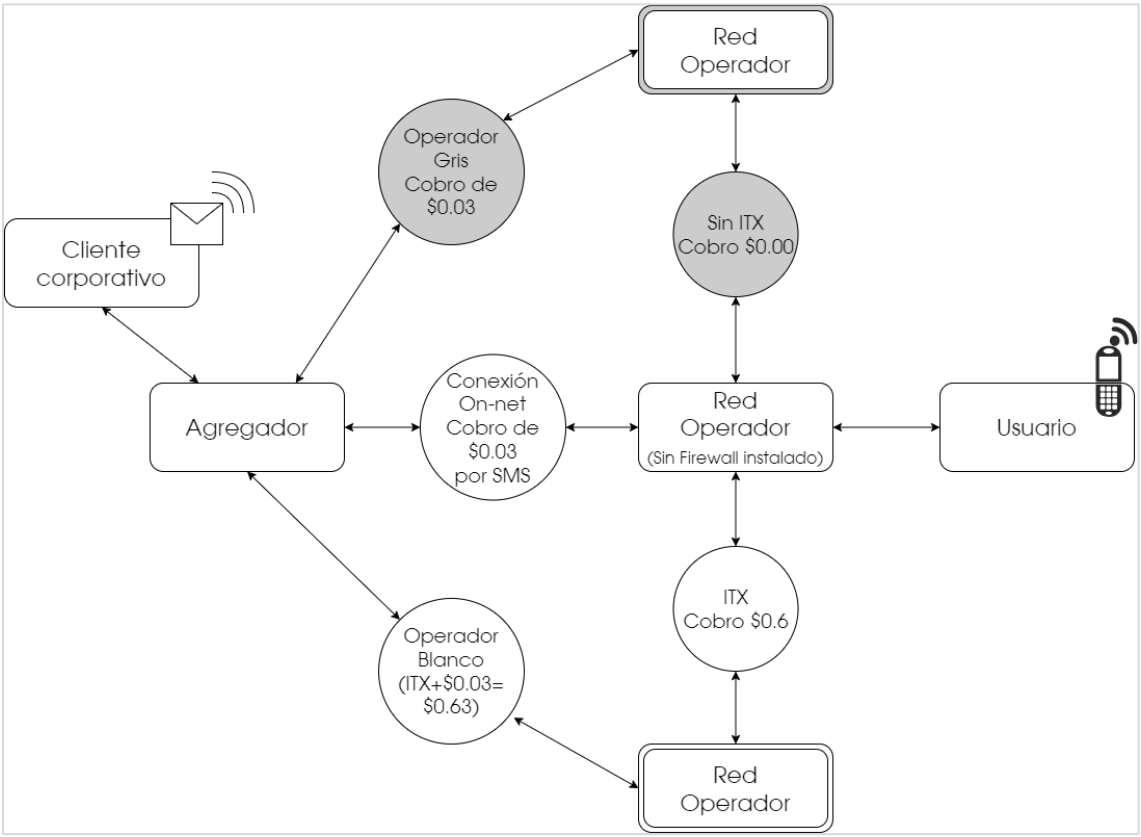
Esta práctica presenta un gran impacto y prolifera facilmente, pues las rutas grises se utilizan para aprovechar el pago de tarifas menores o para no pagar por ninguna tarifa por la terminación de mensajes.

Las rutas grises se pueden utilizar para: a) enviar mensajes desde un enlace destinado a mensajes P2P o a través de un enlace de señalización de *roaming*, que no están autorizados por un operador para el transporte de tráfico del tipo A2P; b) terminación de tráfico internacional a través de rutas nacionales designadas solo para entregar tráfico nacional, con una tarifa de interconexión más baja que la de las rutas internacionales designadas; o c) enviar tráfico del tipo A2P entre operadores de redes de telecomunicaciones cuando no existe acuerdo para monetizar el tráfico.

Las causas para que se cometan este tipo de prácticas no deseadas pueden ser buscar reducir los costos del envío de mensajes para aumentar el margen en el tráfico del servicio a prestar, además de atraer más tráfico al ofrecer una ventaja competitiva; debido a que no se cuentan con controles suficientes por parte de los operadores para

rastrear, monitorear y bloquear el tráfico que proviene de rutas no autorizadas o no monetizadas, entre otras (MEF, 2021a).

Figura 11. Rutas grises en SMS.



Fuente: Elaboración propia a partir de diagramas de MEF (2021a).

5.5 Phishing

MEF (2021a) señala que el *phishing* es una actividad criminal que combina el spam, spoofing y tecnicas de ingenieria social para pretender ser una entidad confiable, para así obtener acceso a sistemas en línea, cuentas o datos de tarjetas de crédito, información bancaria o contraseñas.

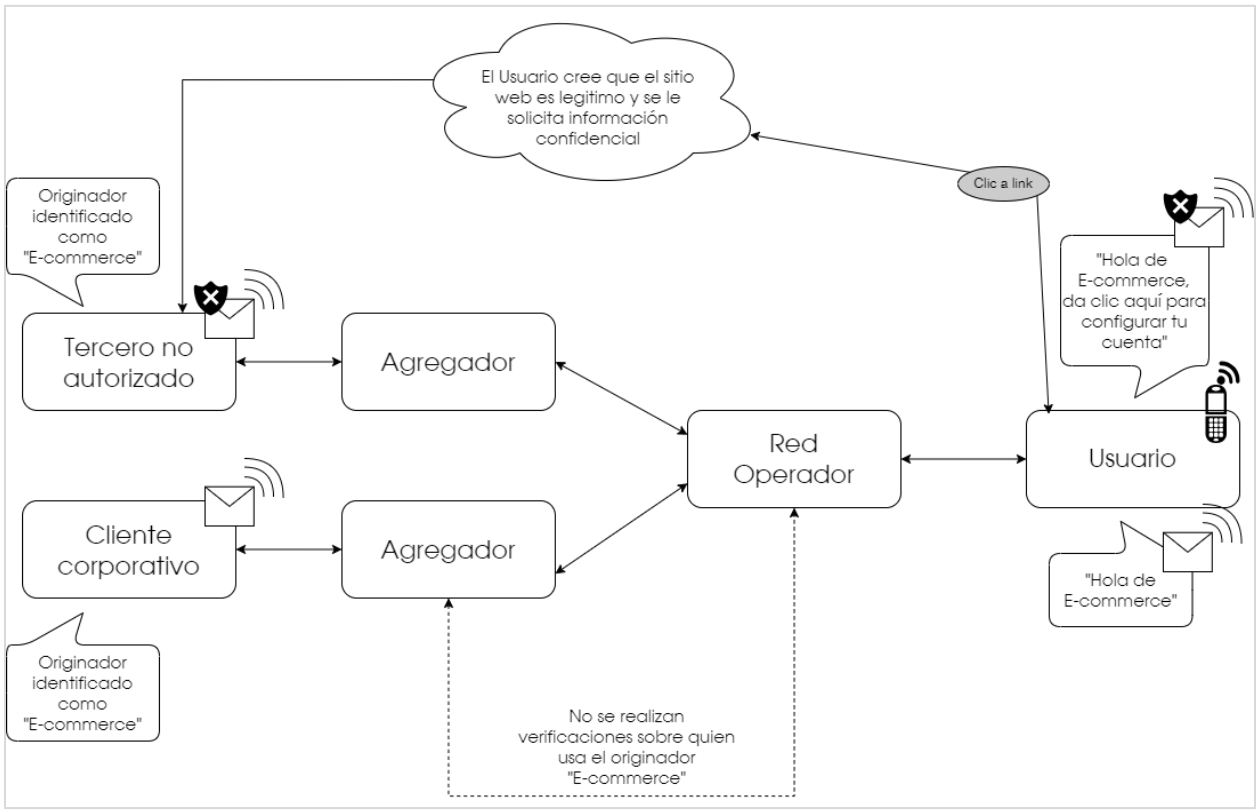
Dentro de las causas que se pueden mencionar para cometer este tipo de prácticas no deseadas podemos encontrar:

- La facilidad con que los usuarios pueden ser engañados mediante el uso de tecnicas básicas de ingeniería social para generar confianza.
- Los reminentes pueden usar un enfoque basado en probabildiades y, por lo tanto, no necesitan saber si un consumidor tiene o no una relación con la empresa que

pretenden ser, aunque tener esa información aumentará sus posibilidades de éxito.

- Reglas de operación deficientes por parte de los proveedores de soluciones de mensajería empresarial.

Figura 12. Phishing en SMS.



Fuente: Elaboración propia a partir de diagramas de MEF (2021a).

5.6 Malware

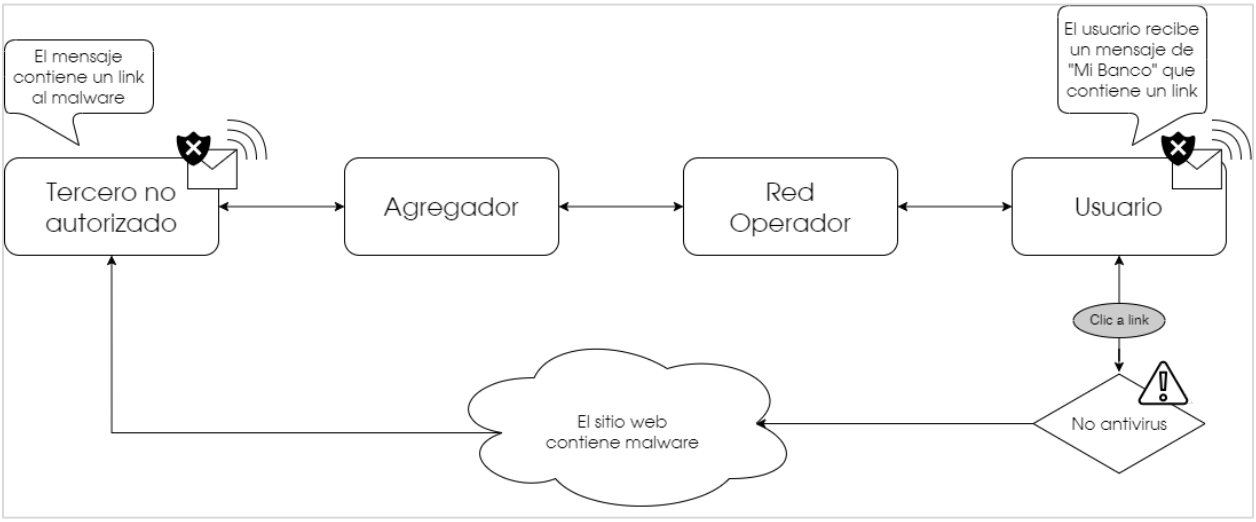
De acuerdo con MEF (2021a), el malware es una actividad delictiva que combina spam, spoofing y tecnicas de explotación como el hackeo para obtener acceso al sismera operartivo del usuario y la información y datos dentro de él, incluyendo datos de cuentas o detalles de tarjetas de credito, información bancaria o contraseñas.

El *malware* es utilizado para dirigir el navegador del dispositivo terminal del usuario a una URL maliciosa que inicia la descarga e instalación de un software en el dispositivo sin el consentimiento del usuario, o que se disfraza de una aplicación confiable que actúa en segundo plano comprometiendo datos sensibles o explotando la conectividad del equipo, incluyendo:

- Reconfiguración a los ajustes del teléfono, aplicaciones y datos.

- Envío de mensajes o realización de llamadas a números de tarificación especial.
- Acceso a la bandeja de entrada de mensajes para localizar alertas de saldo bancarios o códigos PIN, contraseñas, etc.
- Acceso a la lista de contactos y otra información personal.
- Utilización de la lista de contactos para propagar *malware*.

Figura 13. Malware en SMS.



Fuente: Elaboración propia a partir de diagramas de MEF (2021a).

PUNTOS CLAVE DEL CAPÍTULO 5

- Sin los controles adecuados, los mensajes cortos A2P pueden generar afectaciones a la privacidad y seguridad de los usuarios, al recibir mensajes no autorizados los cuales pueden contener enlaces maliciosos que ponen en riesgo la integridad de los dispositivos o buscan obtener información confidencial.

- Las prácticas no deseadas pueden generar un alto consumo de los recursos de las redes de telecomunicaciones, causando problemas técnicos y operativos. Esto resulta en mayores costos y necesidad de mantenimiento para las redes afectadas.

- El *spam* se configura al enviar mensajes cortos con destino a usuarios que no han dado su consentimiento para ser contactados.

- El *flooding* ocurre cuando se envía un gran número de mensajes a uno o más destinatarios, ya sean mensajes legítimos o no. Se considera una práctica no deseada cuando la cantidad de mensajes enviados es significativamente mayor que la carga normal y el valor máximo esperado de mensajes.

- El spoofing implica falsificar la información del origen para parecer legítima. En términos de seguridad, para el caso de mensajes cortos, implica el uso ilegal del SMSC de la red móvil por parte de un tercero que se hace pasar por un usuario real.

- Las rutas grises son usadas para enviar mensajes A2P haciéndolos parecer P2P y/o para aprovechar tarifas de interconexión más bajas o nulas.

6. Marco legal y regulatorio

6.1 Interconexión para el servicio de mensajes cortos.

A través de la reforma de 2013 a la Constitución Política de los Estados Unidos Mexicanos (en adelante y de manera indistinta, la "Constitución" o "CPEUM"), se determinó a las telecomunicaciones como servicios públicos de interés general, propiciando así que el Estado garantice su prestación en condiciones de competencia, calidad, interconexión y acceso libre, entre otras, con fundamento legal en el artículo 6o. Asimismo, mediante las modificaciones realizadas al artículo 28, se estableció el Instituto como el órgano autónomo con personalidad jurídica y patrimonio propio encargado de la regulación, promoción y supervisión del uso, aprovechamiento y explotación de las redes y la prestación de servicios de telecomunicaciones.

Asimismo, con la entrada en vigor de la LFTR, se determinaron los servicios de interconexión que son de prestación obligatoria entre los concesionarios de redes públicas de telecomunicaciones, entre los que se encuentra el servicio de mensajes cortos, con lo que se garantiza que el servicio de mensajes cortos sea utilizado no solo entre usuarios de la misma red, sino que exista un canal de comunicación entre usuarios de distintas redes.

Es así que, el artículo 127 de la LFTR establece lo siguiente:

> *"Artículo 127. Para efectos de la presente Ley se considerarán servicios de interconexión, entre otros, los siguientes:*
>
> *Conducción de tráfico, que incluye su originación y terminación, así como llamadas y servicios de mensajes cortos;*
>
> *(…)"*
>
> (Énfasis añadido)

De lo anterior, se observa que los servicios de mensajes cortos considerados como servicios de interconexión no distinguen ni excluyen las modalidades bajo las cuales puede llevarse a cabo la prestación de dichos servicios, por lo tanto, la prestación de los servicios de mensajes cortos en cualquier modalidad constituye un servicio de interconexión, el cual debe prestarse de manera obligatoria entre los concesionarios de redes públicas de telecomunicaciones.

Así, se puede observar que, desde la máxima norma mexicana como lo es la Constitución, se han determinado los servicios de telecomunicaciones como una

garantía para los ciudadanos, proveyéndolos en condiciones de calidad, competencia y libertad, siendo supervisados y protegidos por el Instituto como órgano especializado en la materia y que vigila la prestación de estos servicios, como es el caso de los de servicios de interconexión, dentro de los cuales particularmente se encuentra el servicio de mensajes cortos, mismos que representan una obligación a ser prestados por todos aquellos concesionarios de redes públicas de telecomunicaciones.

6.2 Derechos de los usuarios

La LFTR establece a través de su artículo 191, los derechos que los usuarios de los servicios de telecomunicaciones gozarán, además de los previstos en la Ley Federal de Protección al Consumidor (en adelante, la "LFPC"). Dicho artículo establece que el Instituto y la PROFECO realizar las acciones, en el ámbito de sus atribuciones, para la protección y restitución de los derechos de los usuarios, o en su caso, la imposición de sanciones por parte del Instituto por el incumplimiento de las obligaciones a los concesionarios.

Con relación a la publicidad no deseada, la LFPC señala lo siguiente:

> *"ARTÍCULO 17.- En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.*
>
> *El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.*
>
> *ARTÍCULO 18.- La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.*
>
> *ARTÍCULO 18 BIS. - Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros."*

Asimismo, la Norma Oficial Mexicana *NOM-184-SCFI-2018, Elementos normativos y obligaciones específicas que deben observar los proveedores para la comercialización y/o prestación de los servicios de telecomunicaciones cuando utilicen una red pública de telecomunicaciones,* establece que los proveedores de servicios de telecomunicaciones deben abstenerse de realizar llamadas o enviar mensajes de texto con fines comerciales a los consumidores a los que provean servicios de telecomunicaciones, así como publicidad de terceros, a menos que los consumidores hayan manifestado su consentimiento expreso, mismo que puede ser revocado por el consumidor en cualquier momento a través de los mecanismos establecidos para tal fin.

De lo anterior, se desprende que los consumidores tienen derechos específicos relacionados con la mercadotecnia y la publicidad, como el derecho de exigir no ser molestados en su domicilio, lugar de trabajo, dirección electrónica, o cualquier otro medio con ofertas de bienes, productos o servicios, y también a rechazar el envío de publicidad. Además, pueden exigir que su información personal no sea compartida o transmitida a terceros, salvo por orden judicial, y tienen acceso a un registro público para aquellos consumidores que no desean que su información se use con fines publicitarios o de mercadotecnia.

Por otro lado, los proveedores y empresas tienen la obligación de abstenerse de enviar publicidad a los consumidores que hayan indicado su deseo de no recibirla, o que estén inscritos en el registro al que se refiere el artículo 18 de la LFPC. En tal sentido, la PROFECO tiene la atribución de mantener un registro público de consumidores que optan por no permitir que su información sea usada para fines mercadotécnicos o publicitarios, denominado Registro Público Para Evitar Publicidad (en adelante, el "REPEP").

El REPEP permite a los consumidores registrar su número telefónico, con independencia de si es fijo o móvil, indicando la clave y el número telefónico asociado a su línea, e indicar los sectores comerciales de los cuales no quieren recibir publicidad, como puede ser el sector de telecomunicaciones y/o turístico, entre otros. (PROFECO, 2023a).

Esta herramienta resulta un medio de empoderamiento para los usuarios de telecomunicaciones móviles, con el que se evitan prácticas como el envío de mensajes de texto no deseado que pueden causar molestia, representando una herramienta adicional para la prevención y control de prácticas no deseadas en la prestación del servicio de mensajes cortos.

PUNTOS CLAVE DEL CAPÍTULO 6

- Conforme a la LFTR, el servicio de mensajes cortos se considera un servicio de interconexión y debe ser prestado por los concesionarios de redes públicas de telecomunicaciones.

- La NOM-184-SCFI-2018 establece que los proveedores de servicios de telecomunicaciones deben abstenerse de enviar mensajes de texto a los consumidores que utilizan sus servicios, incluyendo publicidad de terceros, a menos que cuenten con el consentimiento expreso de los consumidores.

- El REPEP permite a los consumidores que no desean ser contactados con fines mercadotécnicos o publicitarios, registrar su número de teléfono fijo o móvil. También les permite especificar los sectores comerciales de los cuales no desean recibir publicidad en específico.

7. Experiencia internacional referente al control del envío de mensajes no deseados.

Parte importante de este análisis es mostrar un panorama general de cómo se ha enfrentado la problemática referente al uso del servicio de mensajes cortos A2P para la comisión de prácticas no deseadas, las cuales generan afectaciones y molestia a los usuarios, las redes y demás involucrados en dichas comunicaciones. En tal sentido, en este capítulo se describirán los enfoques empleados por los organismos reguladores de diversos países, además de presentar las iniciativas de diferentes organizaciones encargados de fomentar la adopción de medidas, códigos de conducta, y buenas prácticas para hacer frente a prácticas no deseadas, como es el envío de *spam*.

La experiencia internacional referente al control del envío de mensajes no deseados identificada en el presente capitulo se condensa en una tabla comparativa que permite identificar los países en estudio, sus órganos reguladores especializados en la materia y/o asociaciones encargadas de la creación de documentación relacionada con la problemática en comento, los instrumentos normativos y/o reglas emitidas o propuestas y algunos datos relevantes relativos a cada documento considerado. Dicha tabla comparativa se presenta como Anexo I del presente estudio.

7.1 Estados Unidos de América

En el caso de Estados Unidos, la Comisión Federal de Comunicaciones (en adelante, la "FCC" por sus siglas en inglés), a través de la Declaratoria FCC 18-178, determinó que los servicios de mensajes cortos, SMS y MMS, servicios son "servicios de información" y no "servicios de telecomunicaciones". La implicación principal de esta decisión es que estos servicios de mensajería no están sujetos a la regulación común de los operadores de telecomunicaciones bajo la *Communications Act* de los Estados Unidos, lo cual limitaría la capacidad de los proveedores de servicios inalámbricos para combatir eficazmente el *spam* y los mensajes de texto fraudulentos (FCC, 2018).

Además, la Ley de Protección al Consumidor por Teléfono (en adelante, "TCPA" por sus siglas en inglés), prohíbe el envío de mensajes de texto sin el consentimiento previo y explícito del destinatario, por lo que la FCC ha tomado varias medidas para combatir el *spam* en el servicio de mensajes de texto, vigilando la aplicación de las obligaciones establecidas en la TCPA y mediante la coordinación con operadores de telecomunicaciones para bloquear y filtrar mensajes no deseados.

Por otra parte, como una iniciativa de la industria de las comunicaciones inalámbricas de los Estados Unidos, en 2017, la CTIA publicó los Principios y Mejores Prácticas de

Mensajería (CTIA's *Messaging Principles and Best Practices*), un documento que, como su nombre lo indica, presenta las mejores prácticas que deberán considerarse para la prestación del servicio de mensajería, en el cual se establece la obligación de obtener el consentimiento del consumidor antes de enviarle mensajes de texto, así como facilitar y respetar la decisión del consumidor de optar por no recibir más mensajes de texto.

Asimismo, se establece que, al recopilar el consentimiento de los consumidores, los remitentes de mensajes deben mostrar información clara y visible sobre el tipo y el propósito del mensaje que el consumidor puede esperar recibir, además de que el remitente debe obtener un consentimiento por cada campaña que este quiera hacer llegar a los consumidores.

Otras prácticas recomendadas por CTIA (2019), son las siguientes:

1. Números de Teléfono compartidos y códigos cortos: en los casos donde se apruebe el uso de números compartidos, todos los remitentes de mensajes que operen con un mismo número compartido deben estar documentados y disponibles.

2. Mensajería *Snowshoe*: los remitentes no deben emplear técnicas de envío de mensajería de tipo *Snowshoe*. Estas técnicas tienen como objetivo evitar la detección por parte de los filtros antispam y las listas negras, ya que el volumen de mensajes de cada fuente individual es lo suficientemente bajo como para pasar desapercibido.

3. Rutas Grises: los remitentes no deben enviar mensajes a través de rutas grises.

4. Códigos cortos: el uso de números cortos debe realizarse mediante su registro a través de la Administración de Códigos Cortos Comunes (CSCA, por sus siglas en inglés)

Asimismo, en septiembre de 2022, la FCC (2022) lanzó una iniciativa con el propósito de combatir los mensajes de texto de estafa y *spam* al ampliar ciertas protecciones contra llamadas ilegales a los mensajes de texto. Durante este proceso, la agencia permitió al público dar su opinión sobre la aplicación de estándares de autenticación de la identificación del llamante en los mensajes de texto, así como sobre la obligación de los proveedores de identificar y bloquear de manera activa los mensajes ilegales antes de que lleguen a los consumidores. Además, se solicitó la retroalimentación de la comunidad acerca de otras posibles medidas que la FCC podría implementar para abordar los mensajes de texto ilegales, incluyendo el fortalecimiento de la educación del consumidor.

Además, en marzo de 2023 la FCC realizó una propuesta de regulación para la eliminación de mensajes no deseados, en la que se toman medidas para exigir a proveedores de servicios inalámbricos móviles que bloqueen ciertos mensajes de texto automáticos que tienen muchas probabilidades de ser ilegales. Asimismo, se les exige a

los proveedores de servicios inalámbricos móviles que bloqueen a nivel de red, los mensajes de texto originados en números no válidos, no asignados o no utilizados conforme al Plan de numeración de América del Norte, así como los números que a petición del suscriptor ha solicitado que se bloqueen.

7.2 Arabia Saudita

Dentro de las regulaciones emitidas por la Comisión de Comunicación, Espacio y Tecnología (en adelante, la "CST" por sus siglas en inglés) para combatir los mensajes de spam, se encuentra el "*Regulations for Curbing SPAM Messages & Calls*", a través del cual se regula el uso de mensajes y llamadas, contribuyendo a reducir los mensajes y llamadas fraudulentas y *spam*. El documento se basa en el principio de protección de los usuarios y sus intereses, así como en proporcionar comunicaciones con la apropiada calidad, protección contra contenido dañino y manteniendo la confidencialidad de las comunicaciones.

La CST (2022) clasifica los mensajes de texto en cinco tipos, los cuales ha definido de la siguiente manera:

1. Mensajes promocionales: mensajes electrónicos de carácter comercial o fines de mercadotecnia para la promoción de productos o servicios o para el cobro o recordatorio de donaciones.
2. Mensajes de servicio: mensajes electrónicos con contenido de servicios, enviados a un determinado usuario con el objeto de prestarle un servicio contratado, o para informarle de operaciones realizadas sobre dicho servicio, sus características y opciones.
3. Mensajes de orientación: mensajes electrónicos con contenido de concientización u orientación enviados a todos los usuarios por parte de entidades de naturaleza jurídica tales como agencias gubernamentales, bancos, hospitales y otros.
4. Mensajes de alarma: mensajes electrónicos de alta prioridad con un contenido de advertencia enviados a todos los usuarios en todas o algunas partes de Arabia Saudita o por agencias gubernamentales competentes para advertir sobre un evento inminente u ocurrido, siempre que estos mensajes sean para personas en la zona de peligro únicamente.
5. Mensajes personales: mensajes cortos de un número de usuario especificado a otro número de usuario especificado para fines personales.

Además, la CST ordenó la creación de un sistema electrónico de mensajes cortos masivos (en adelante, "Bulk SMS e-System") el cual estará interconectado con los prestadores de servicios, y de esa manera, administrar el envío de mensajes cortos A2P conforme a las reglas especificadas por el CST.

Entre los servicios o funciones a cargo del Bulk SMS e-System se encuentran:

- Recepción y procesamiento de solicitudes para registrar remitentes;

- Permitir que el usuario final bloquee o reciba mensajes cortos masivos, guarde sus preferencias y pueda visualizarlas a través de la interfaz del sistema de envío de mensajes cortos masivos;
- Permitir al usuario reportar mensajes de fraude recibidos;
- Filtrar y prevenir el envío de cualquier mensaje corto masivo que no tenga el nombre de un remitente aprobado o un formulario de mensaje aprobado;
- Asegurarse que más de un remitente no tenga el mismo nombre de remitente.

Para poder ayudar al desarrollador y prevenir el envío de mensajes cortos masivos no deseados, la CST puede crear un listado con los nombres de los remitentes prohibidos o bloqueados y debe compartirla con el administrador del *Bulk SMS e-System*. Así como, es una obligación impuesta por la CST que todos los remitentes clasificados como anuncios deberán añadir a su nombre de remitente el subfijo "(-AD)".

Asimismo, en la regulación emitida por la CST se establecen obligaciones para los diferentes actores que forman parte de la cadena de prestación de mensajes cortos A2P, destacando las siguientes:

1. Creación de una base de datos unificada entre los operadores, en la que se compartan los datos necesarios para frenar los fraudes y las estafas.
2. Aplicación de las soluciones técnicas necesarias para monitorear e impedir el uso de sus redes para el envío de mensajes spam, scam y spoof, y tomar las medidas preventivas necesarias para frenar los mismos antes de que lleguen al usuario final.
3. Filtrar todos los mensajes cortos de remitentes no autorizados, o enviados desde un proveedor de mensajes cortos que no tiene relación con el nombre del remitente autorizado, así como los mensajes cortos enviados a usuarios que han solicitado el bloqueado según sus preferencias.
4. Los operadores de servicios deben incluir una cláusula en el contrato de servicios celebrado con el usuario final en la que se confirme que el número de móvil no se utilizará con fines promocionales.
5. En el caso de que el remitente desee enviar algún mensaje promocional al usuario final, deberá dar al usuario final la posibilidad de aceptar expresamente recibir o no mensajes promocionales, siendo obligación del remitente aportar la prueba de consentimiento.

Además, los usuarios pueden solicitar dejar de recibir mensajes promocionales en cualquier momento, ya sea que dicha solicitud se presente a través de canales tradicionales y/o electrónicos. Una vez realizada la solicitud por parte del usuario, solicitando la suspensión del envío de mensajes promocionales deberá detenerse su entrega en un plazo no superior a veinticuatro (24) horas desde la recepción de la solicitud. De igual manera, deberá ser enviada una notificación confirmando la activación o suspensión, según sea el caso, del envío de mensajes promocionales tras recibir una solicitud para ello.

7.3 Canadá

En Canadá, la Comisión Canadiense de Radiodifusión y Telecomunicaciones (la "CRTC", por sus siglas en inglés) se encarga de vigilar el cumplimiento de la "*Anti-Spam Legislation"* de Canadá (CRTC, 2023).

La Ley Canadiense *Anti-Spam* o *Canadian Anti-Spam Legislation* (en adelante, "CASL"), es una legislación promulgada en Canadá para abordar el problema del spam electrónico y las prácticas de *marketing* no deseadas. El objetivo principal de la ley es proteger a los usuarios canadienses de los mensajes electrónicos no solicitados y garantizar una práctica justa y ética en el uso del correo electrónico y otras formas de comunicación electrónica.

Como parte de la legislación, se define un "mensaje electrónico" como un mensaje enviado por cualquier medio de telecomunicaciones, incluyendo un mensaje de texto, sonido, voz o imagen. De igual manera, se define un "mensaje electrónico comercial" como un mensaje electrónico donde se debe tener en cuenta aquellos que invitan a participar en una actividad comercial.

Para el consentimiento, la CASL requiere que los remitentes obtengan de manera previa el consentimiento expreso o implícito de los destinatarios y queda prohibido el envío de mensajes electrónicos que contengan solicitudes de consentimiento, ya que se consideran un mensaje electrónico comercial.

Los mensajes electrónicos comerciales deben contener información clara y precisa donde se identifique el remitente y proporcione un mecanismo de contacto. Asimismo, todos los mensajes electrónicos comerciales deben incluir un mecanismo de cancelación (dirección electrónica o enlace a una página en internet a la que se pueda acceder a través de un navegador web) de suscripción que permita a los destinatarios retirarse fácilmente de futuras comunicaciones, el cual debe ser sin costo alguno y podrá ser enviado por el mismo medio electrónico por el que se recibió el mensaje o cualquier otro medio electrónico que permita a la persona manifestar su deseo.

Asimismo, la Asociación Canadiense de Telecomunicaciones ("CTA", por sus siglas en inglés), la cual es una organización representante de la industria de telecomunicaciones en Canadá, publicó en agosto de 2023, el documento *Best Practices for Canadian Application-to-Person (A2P) Messaging Programs* con el objetivo de:

- Proporcionar orientación y recomendaciones a proveedores de contenido, marcas, agregadores y proveedores de servicios de aplicaciones sobre la gestión eficaz de A2P en Canadá.
- Abogar por la protección de los usuarios finales mediante la reducción de *spam* y otros mensajes maliciosos.

- Facilitar el crecimiento continuo y la adopción de la mensajería A2P en Canadá garantizando que los usuarios finales sigan considerándolo un canal de comunicaciones confiable.

Este documento exhorta a todas aquellas organizaciones involucradas en la operación de programas de mensajería A2P en Canadá, a cumplir con todas las leyes, reglas y regulaciones aplicables a este tipo de mensajes, incluyendo la CASL (CTA, 2023). Asimismo, como su nombre lo indica, establece las mejores prácticas y estándares recomendados a considerar por los involucrados en el envío de mensajes A2P, entre los que se destacan:

- Todas las campañas de envío de mensajes cortos deben basarse en el consentimiento del destinatario. Se debe evitar estrictamente el envío de mensajes no solicitados o *spam*.
- Todas las campañas de envío de mensajes cortos deben proporcionar un mecanismo de exclusión voluntaria mediante el uso de palabras clave estandarizadas (por ejemplo, CANCELAR, DETENER, SALIR y FINALIZAR).
- Las campañas de envío de mensajes no deben utilizar promoción/publicidad engañosa para obtener participación.
- Todos los mensajes enviados a un usuario final deben identificar con precisión el número A2P y la marca/organización desde la que se envió el mensaje.
- Todas las campañas de envío de mensajes cortos deben generar respuestas a palabras clave (por ejemplo, AYUDA, INFORMACIÓN, DETENER)
- En su caso, se debe informar a los usuarios finales sobre el costo de participar en un programa A2P.
- Las campañas que incluyan contenido restringido por edad deben verificar que cada usuario sea mayor de edad de manera previa.
- Los programas no deben enviar contenido relacionado con discursos de odio, malas palabras, representaciones y respaldo de la violencia, ni ningún contenido ilegal.

Asimismo, el documento de la CTA limita los horarios para el envío de mensajes A2P con fines comerciales y recomienda que los prestadores de servicios y agregadores implementen de manera regular pruebas y auditorías a los programas de envío de mensajes A2P, a fin de garantizar la experiencia de los usuarios y el cumplimiento a la regulación y normas aplicables.

Respecto a las prácticas relacionadas con el envío de mensajes A2P que la CTA identifica como negativas dado que afectan a los usuarios finales y pueden resultar en la suspensión indefinida del servicio de mensajería A2P por parte de los proveedores de servicios inalámbricos y agregadores, se encuentra el envío de mensajes a través de rutas grises, la utilización de numeración compartida, mensajería *Snowshoe*, inflación de tráfico artificial, *spoofing*, *spam*, *phishing* y mensajes maliciosos.

7.4 Asociación Global para las Comunicaciones Móviles (GSMA)

En 2006, la GSMA (del inglés, Global System for Mobile Communications, originally Groupe Special Mobile) creó una iniciativa de la mano de sus operadores miembros, titulada "Código de Prácticas para spam móvil" (en adelante, el "Código de prácticas"), la cual fue planteada para facilitar que los operadores pudieran ofrecer servicios en un entorno seguro y confiable, garantizando que los usuarios reciban la menor cantidad posible de *spam* a través de SMS y/o MMS. Si bien, es documento de carácter voluntario y no forma parte de una legislación formal, este código complementa el actuar de la regulación y autoridades nacionales correspondientes.

El Código de Prácticas abarca las comunicaciones no deseadas transmitidas mediante SMS y MMS, abarcando: mensajes de índole comercial enviados a clientes sin su consentimiento, mensajes de carácter comercial que incentivan directa o indirectamente a los clientes a llamar o enviar mensajes a números con tarifas adicionales, y mensajes masivos fraudulentos dirigidos a los clientes (como mensajes falsos, suplantación de identidad o estafas).

Los Operadores de telefonía móvil que hayan firmado el Código de Prácticas presentado por la GSMA (2006) se comprometen a:

1. Incluir cláusulas contra el *spam* en todos los nuevos contratos con proveedores externos.

   Dentro de estas cláusulas se recomienda el compromiso de:
   - Abstenerse de enviar o participar en *spam* móvil.
   - Cumplir con los requisitos de consentimiento establecidos por la legislación nacional correspondiente.
   - Ofrecer a los clientes medios claros, efectivos y fácilmente identificables para optar por no recibir más comunicaciones de *marketing* a través de SMS o MMS.
   - En lo posible, establecer sanciones en caso de incumplimiento de los compromisos contra el *spam*, que pueden incluir la suspensión y/o terminación de contratos.

2. Establecer un mecanismo que garantice el consentimiento adecuado de los clientes y les otorgue un control efectivo sobre las comunicaciones comerciales de los operadores móviles.

Los métodos para obtener el consentimiento deberán involucrar la implementación de mecanismos de consentimiento "*opt-in*"[2] y/o mecanismos "*opt-out*"[3] para los clientes.

Asimismo, los operadores se comprometen a asegurar que los procesos utilizados para obtener el consentimiento sean transparentes y claros, y a mantener registros del tipo de consentimiento obtenido de los clientes, incluyendo detalles sobre cómo y cuándo se obtuvo dicho consentimiento.

3. Colaborar con otros operadores de telefonía móvil para abordar los problemas relacionados con el *spam*.

4. Proporcionar a los clientes información y recursos que les ayuden a reducir los niveles y el impacto del spam en sus dispositivos móviles, entre la que se recomienda incluir lo siguiente:

    - Suministro de información sobre las políticas *antispam* de los operadores, la legislación relevante y los códigos de práctica locales.
    - Ofrecer consejos sobre cómo abordar incidentes de presunto *spam* a través de los canales de atención al cliente, medios de comunicación y/o sitios web.
    - Facilitar la notificación de *spam* móvil, ya sea a través de los canales de atención al cliente, el sitio web de los operadores o mediante un "código corto" al cual los clientes puedan reenviar el *spam* móvil sospechoso.

5. Llevar a cabo otras actividades contra el *spam* con el fin de minimizar su incidencia y efectos en los usuarios móviles, entre las que se consideran:

    - Garantizar la implementación de una política antispam que prohíba el uso de la red móvil para enviar o iniciar *spam* móvil.
    - Revisar los contratos de los clientes, términos y condiciones generales, así como las políticas de uso aceptable, para asegurar que se incluyan condiciones actualizadas y relevantes en contra del *spam*. Estas condiciones pueden especificar que las quejas serán investigadas (incluida la colaboración con las autoridades competentes, cuando corresponda) y que el operador puede dar de baja el servicio a un cliente que sea responsable de enviar *spam* móvil.

[2] Los mecanismos "opt-in" se refieren al proceso en el que un usuario da su consentimiento explicito para recibir mensajes, al suscribirse activamente a un servicio.
[3] Los mecanismos "opt-out" se refieren al proceso que le permite al usuario retirar su consentimiento y dejar de recibir mensajes a los que se haya suscrito explícitamente.

- Priorizar e investigar las denuncias de los clientes relacionados con el *spam* móvil, tomar las medidas necesarias y reportar los casos a las autoridades competentes, cuando sea necesario.
- Monitorear las redes en busca de señales de *spam* móvil y tomar acciones proactivas para eliminarlos, respetando los requisitos de la legislación nacional.
- Compartir información sobre las mejores prácticas y colaborar con otros operadores móviles a nivel nacional e internacional para reducir el *spam* móvil transmitido a través de las redes. Esto puede incluir la adopción de las técnicas recomendadas por la GSMA para detectar y abordar la transmisión internacional de *spam* móvil fraudulento, así como SMS y MMS no solicitados que promuevan cargos adicionales. También se deben tomar medidas para garantizar que los operadores que originan los SMS y MMS estén adecuadamente identificados, evitando la suplantación de la identificación del remitente.

6. Fomentar el apoyo de los gobiernos y reguladores hacia la industria en esta materia, por lo que se recomienda:

    - Respaldar los mecanismos de autorregulación de la industria.
    - Apoyar el desarrollo de prácticas responsables de *marketing* móvil y de industrias de tarificación adicional. Esto implica respaldar códigos de conducta que promuevan principios de consentimiento efectivo, transparencia y claridad en los precios.
    - Apoyar la investigación de fraudes y abusos relacionados con el *spam* móvil. Por ejemplo, abordar cualquier problema relacionado con la protección de datos, privacidad o pagos de tarifas especiales que menos puedan obstaculizar la capacidad de los operadores de telefonía móvil para investigar los abusos de *spam* móvil.
    - Apoyar a los operadores de telefonía móvil en sus esfuerzos para combatir el *spam* móvil a nivel de red. Esto puede incluir permitir el uso de filtros a nivel de red para identificar y evitar que el *spam* móvil llegue a los clientes.
    - Establecer o respaldar un entorno que sancione a aquellos que envíen mensajes SMS o MMS no solicitados que inciten a responder con tarifas más altas. Por ejemplo, permitir a los operadores de telefonía móvil retener los pagos a los presuntos destinatarios de *spam* móvil mientras las autoridades competentes investigan sus actividades de *spam*.

7.5 Foro del Ecosistema Móvil (MEF)

En 2020, MEF (del inglés, *Mobile Ecosystem Forum*), publicó un código de autorregulación consistente en un código de conducta para el envío de mensajes cortos empresariales titulado "*Business SMS Code of Conduct*", mismo que establece un estándar de comportamientos, procedimientos y acciones para todos los actores que operan dentro del mercado de SMS A2P (también denominado empresarial, masivo o mayorista e incluye el tráfico de P2A). Su objetivo es proteger a los consumidores, demostrar responsabilidad ética y comercial, así como para maximizar el valor para todas las empresas involucradas en el ecosistema de mensajería, y se señala como relevante para todas las empresas involucradas con el servicio SMS A2P entre los que se encuentran:

- Operador de redes móviles (MNO) y Operadores de redes móviles Virtuales (MVNO)
- Agregadores de SMS A2P o Proveedores de plataforma de comunicaciones como servicio (CAAS)
- Marcas y cualquier empresa que interactúe con sus clientes a través de SMS.

Entre los principios que establece el Código de Conducta del MEF se destacan:

- No crear, transportar ni entregar mensajes SMS A2P no solicitados. Para lo anterior, los generadores de mensajes deben asegurar que los consumidores estén informados de sus derechos y tengan la oportunidad de elegir y controlar los mensajes que deseen recibir.
- Se debe aceptar que los usuarios podrán cambiar o revocar su consentimiento para ser contactados. Para ello, se debe incluir una guía de opción de exclusión dentro del proceso de inclusión voluntaria.
- Los generadores de mensajes deben respetar las preferencias legales de los usuarios con respecto al tiempo y frecuencia de la interacción de SMS A2P. Cuando no existe una ley respecto al momento y frecuencia de los mensajes enviados se debe observar el mejor juicio (de 8 a.m. a 8 p.m. en semana laboral, evitando días festivos, etc.)
- Se debe proteger y manejar adecuadamente los datos personales de los consumidores.
- No se modificará el contenido de los mensajes o sus metadatos a menos que se requiera legítimamente para la entrega del mensaje.
- Se deben implementar procedimientos y herramientas efectivos para evitar el fraude al consumidor o fraude comercial. En este sentido, se destaca que se deben proteger las redes de telecomunicaciones parta bloquear, entre otros, los siguientes casos:
    - Granjas de SIM que aprovechan tarjetas SIM de consumidores.
    - Rutas grises.

- Otras redes que utilizan la falsificación o manipulación para eludir conscientemente los *firewalls*.

- No se ocultará la identidad ni se utilizará la de otra persona.
- Se promoverá y educará activamente a todas las partes de la industria para garantizar que cada servicio ofrecido sea seguro, confiable y cumpla con todos los requisitos operativos y legales relevantes.
- Los interesados deberán ayudar de manera proactiva a los reguladores, a agencias de aplicación de la ley u otras partes del ecosistema para limitar el alcance y la recurrencia de incidentes fraudulentos e identificar actores malintencionados.

Asimismo, el Código presenta un apartado relacionado con la gestión de incidentes de fraude, entre los que se destaca que, una vez detectado que se envían mensajes no deseados, y que esto no ha cesado, se debe bloquear el tráfico fraudulento; se deben proporcionar pruebas del consentimiento de aceptación o el cese del tráfico sospechoso dentro de un tiempo estipulado bajo contrato.

7.6 Comisión Europea

En el 2002, se crea por parte de la Comisión Europea la Directiva sobre privacidad y comunicaciones electrónicas, también conocida como Directiva 2002/58/CE o ePrivacy Directive, la cual tiene como objetivo principal el garantizar la privacidad y la protección de datos en las comunicaciones electrónicas en los países miembros de la Unión Europea y la cual introdujo en el principio del marketing basado en el consentimiento (opt-in) para el correo electrónico y para los mensajes SMS o MMS.

7.7 Organización para la Cooperación y el Desarrollo Económico (OCDE)

Como parte de las iniciativas de la OCDE para combatir el *spam* y la posibilidad de nuevos problemas como consecuencia de la convergencia de tecnologías de la comunicación, se crea un grupo llamado "OECD *Task Force on Spam*" (en adelante, Grupo Operativo) el cual tiene como objetivo la creación de un marco para hacer frente al *spam* utilizando una amplia gama multidisciplinar de soluciones.

El Grupo Operativo desarrolló en 2004 el "Anti-*Spam Toolkit*" (en adelante, Toolkit), el cual es un conjunto de políticas y medidas recomendadas, para orientar a los miembros de la OCDE sobre la política global y un marco coherente en la lucha contra el spam

en el correo electrónico y en otras comunicaciones electrónicas que pueden verse amenazados.

Para la OCDE (2006), el *Toolkit* se compone ocho elementos interrelacionados, los cuales abordan:

1. **Enfoques normativos:** El desarrollo de una legislación antispam clara es fundamental para establecer directrices sobre lo permitido y lo no permitido.

2. **Preocupación por la aplicación de la ley:** La ejecución y aplicación rápida de la ley es fundamental, al igual que las medidas y sanciones son cruciales si se quiere frenar eficazmente al *spam*. De igual manera, debemos prestar atención a la coordinación nacional, las sanciones, la capacitación y la cooperación transfronteriza ya que serán sumamente importantes.

3. **Iniciativas impulsadas por la industria:** Las leyes antispam deben ir acompañadas de acciones del sector privado, para frenar de manera eficaz el *spam.*

4. **Soluciones técnicas:** Se requiere la aplicación sensata de herramientas y métodos tecnológicos antispam en varios niveles para reducir el *spam*. Haciendo el uso de una o varias tecnologías/métodos, se puede pueden reducir drásticamente el nivel de *spam* que afecta un sistema.

5. **Educación y concienciación:** Es esencial capacitar a los usuarios finales sobre cómo enfrentar el spam y otras amenazas en línea. Las actividades de educación y sensibilización son necesarias empresas, para los usuarios residenciales y en los centros de enseñanza. Su objetivo debe ser crear una cultura de la seguridad y fomentar un uso responsable del ciberespacio.

6. **Asociaciones cooperativas contra el *spam*:** La cooperación público-privada es necesaria para la sensibilización, intercambio de información y buenas prácticas. De esta manera se busca preservar la disponibilidad y fiabilidad de las herramientas de comunicación para fomentar el desarrollo de la economía digital. Así mismo, las asociaciones son una herramienta fundamental para mejorar la comunicación y comprender mejor las necesidades, expectativas y problemas recíprocos y, por tanto, potenciar la cooperación y la implicación mutua.

7. **Métricas del *spam*:** La evaluación de la evolución del *spam* y la efectividad de las soluciones antispam y los esfuerzos educativos se basa en la medición. Las métricas permiten analizar las estrategias nacionales y su implementación, además de identificar los cambios requeridos en los aspectos políticos, normativos y técnicos.

8. **Cooperación mundial (*Outreach*):** La cooperación entre gobiernos, sector privado, sociedad civil y otras partes interesadas es fundamental para promover marcos nacionales adecuados y garantizar la aplicación efectiva de medidas técnicas y normativas. Ya que el *spam*, no conoce fronteras y viaja desde y hacia las economías desarrolladas y en desarrollo

Mediante los enfoques normativos presentados por la OCDE (2006), se busca fomentar el desarrollo de una legislación antispam y la cual debe garantizar los beneficios de las comunicaciones electrónicas al fomentar la confianza de los usuarios en Internet y en los medios de mensajería electrónica, además de mejorar la disponibilidad, confiabilidad y eficacia de los servicios, así como el rendimiento de las redes de comunicación a nivel global.

Como parte de la propuesta se examinaron las mejores prácticas en materia de legislación y, en la medida de lo posible la OCDE (2006) recomienda incluir las mencionadas en la siguiente tabla, donde se deberá tener en cuenta el marco institucional y jurídico de cada país.

Cuestiones	Enfoque	
ALCANCE	Servicios Afectados	El formato de mensajería se fusionará o evolucionará, y pueden surgir medios de mensajería imprevistos. Se pueden adoptar dos posibles legislativos: "Tecnología específica". Dirigirse a tecnologías de mensajería específicas, normalmente las que plantean un problema actual de *spam*. "Tecnología neutral" El instrumento regulador abarca las tecnologías de la comunicación en general, y es lo suficientemente flexible como para abarcar futuros cambios en la tecnología de la mensajería sin necesidad de modificación. Los servicios de voz a voz en tiempo real podrían regularse por separado.
	Finalidad Comercial	Considere si la legislación debe abordar únicamente los mensajes comerciales y transaccionales, o si también debe abordar contenidos específicos no comerciales, como mensajes políticos o religiosos. Determinadas categorías de mensajes pueden excluirse expresamente del ámbito de aplicación de la ley (por ejemplo, los mensajes de instituciones académicas a sus antiguos alumnos).

CONSENTIMIENTO	Consentimiento	El grado de consentimiento o permiso que los legisladores o reguladores desean exigir puede variar en función del enfoque de la regulación del spam. Existen tres enfoques principales del consentimiento, que a menudo se mezclan en la legislación: Expreso: forma de consentimiento en la que un individuo u organización ha dado su permiso de forma activa para una acción o actividad concreta (*opt-in*). Inferido/implícito: consentimiento que generalmente pueden inferirse de la conducta y/u otras relaciones comerciales del destinatario. Consentimiento presunto: existe una presunción de consentimiento hasta que el destinatario lo retira, por ejemplo, "dándose de baja" (*opt-out*).
REQUISITOS PARA UN MENSAJE PUBLICITATARIO LEGITIMO	Dirección para darse de baja	Los mensajes deben incluir siempre una opción de exclusión funcional, que permita al destinatario darse de baja indicando su deseo de no recibir en el futuro más comunicaciones de la parte remitente. Esto implica que deben incluirse una dirección de remitente válida en el correo electrónico, para que el destinatario pueda darse de baja fácilmente. También podría exigirse una dirección postal. La falta de un dispositivo de exclusión voluntaria, la ausencia de una dirección de remitente válida y de una dirección postal válida, o el hecho de no cesar la transmisión de los mensajes en el plazo establecido por la ley deben ser sancionados.
	Información sobre el origen de los mensajes	Un reto clave en la regulación del *spamming* y la aplicación de las leyes sobre *spam* es responder a la capacidad de los *spammers* para ofuscar el origen del *spam* que se envía: -La legislación debe prohibir el envío de correos electrónicos que falsifiquen el origen u oculten información de cabecera/ID. -La legislación también debería exigir que se identifique claramente al vendedor que apoya al remitente del correo electrónico.
	No *Bulk*	La legislación puede prever que el correo electrónico se clasifique como *spam* sólo si se ha enviado un determinado número de mensajes en un periodo de tiempo determinado (normalmente más de 50-100 en 24 horas).

		Por supuesto, este elemento debe tener en cuenta el hecho de que existe correo electrónico masivo legítimo (por ejemplo, boletines informativos, etc.)
	Etiquetado	La legislación puede incluir una disposición que exija el uso de una etiqueta específica para los correos electrónicos que contenga publicidad, material pornográfico, etc.
ELEMENTOS AUXILIARES	Personas que autoriza el envío del spam o ayuda/facilita/asiste al *spammer*	La ley no debe sancionar únicamente a la persona que envía físicamente el mensaje, sino también a la persona que encargó o autorizó el envío de los mensajes o que ha obtenido beneficios económicos con las actividades de *spamming*. Este enfoque podría facilitar la aplicación de la normativa, ya que a menudo es difícil determinar quien envió realmente el *spam*, mientras que puede ser más fácil determinar quién se beneficia de la actividad de *spam*.
	Software de recolección y listas de direcciones recolectadas Ataques de diccionario	La legislación puede incluir disposiciones específicas para imponer sanciones adicionales si dichas herramientas se utilizan para ayudar al envío de *spam* contraviniendo la legislación sobre *spam* de la jurisdicción: el acto de vender, adquirir o utilizar *software* de recolección o listas de direcciones recolectadas, o la generación automática de direcciones de destinatarios puede ser sancionado.
CIBERDELICUENCIA Y CUESTIONES RELACIONADAS CON LOS CONTENIDOS	Acceso ilegal	La legislación debe prohibir el uso no autorizado de recursos informáticos protegidos. Debe sancionarse a todo aquel que ponga en peligro los ordenadores con el fin de utilizarlos para enviar mensajes.
	Contenido engañosos o fraudulentos	Centrarse en el contenido del mensaje. Esto deja de lado muchas de las preocupaciones sistémicas relativas a los mensajes *spam*. Las estafas de *spam* y el *phishing* podrían constituir delitos informáticos, es decir, delitos comunes que se cometen frecuentemente mediante el uso de un sistema informático. -La legislación antispam podría incluir, además, disposiciones sobre la prohibición de encabezamientos de asunto engañosos o que induzcan a error. -La legislación sobre *spam* puede abarcar el contenido de los mensajes, en particular si las leyes antifraude, de protección del consumidor, etc. No están claramente definidas.
	Amenazas a la seguridad	Los aspectos del *spam* relacionados con el *malware* suelen estar tipificados en la legislación o pueden penalizarse utilizando el marco del Convenio sobre ciberdelincuencia del Consejo de Europa.

ELEMENTO INTERNACIONAL	Jurisdicción fronteriza	La regulación debería: - Especificar que los mensajes enviados a/o desde la jurisdicción están cubiertos, así como los mensajes encargados desde dentro de la jurisdicción y los beneficios financieros vinculados al spam. - Los *spammers* que operan desde la jurisdicción nacional, aunque envíen *spam* a otros países, deben ser sancionados por la legislación nacional. - Las autoridades nacionales encargadas de hacer cumplir la ley deben estar facultadas para emprender la cooperación internacional y los acuerdos transfronterizos de ejecución son importantes.

PUNTOS CLAVE DEL CAPÍTULO 7

- De la experiencia a nivel internacional resalta que el requisito principal para prevenir el envío de *spam* es asegurar que los remitentes obtengan el consentimiento explícito del usuario antes de realizar el envío de mensajes cortos con fines comerciales.

- En distintos países existen iniciativas de autorregulación por parte de la industria de telecomunicaciones, a través de las cuales se han creado guías de mejores prácticas enfocadas en el desarrollo del servicio de mensajes cortos A2P para su prestación de manera segura, fiable y respetuosa de los derechos de los usuarios.

- La implementación de mecanismos *opt-out* que sean claros y fáciles de utilizar para los usuarios que desean dejar de recibir mensajes cortos con fines comerciales, forman parte de las buenas prácticas empleadas a nivel internacional en la prestación de servicios A2P.

- Otro mecanismo extendido a nivel internacional para detener el spam, son las listas de números a los que no se puede llamar o enviar mensajes de texto.

8. Opciones y propuestas para el desarrollo del servicio de mensajes cortos A2P.

El servicio de mensajes cortos en su modalidad A2P es un medio de comunicación particularmente efectivo en situaciones que exigen atención inmediata o información crucial, como es el caso de los servicios de autenticación de dos factores y las notificaciones de transacciones bancarias, además de su efectividad en la comunicación entre empresas y clientes.

Una de sus ventajas más destacadas es su capacidad de alcanzar a un público amplio con facilidad, dado que no necesita de una conexión a Internet y puede ser recibido por casi cualquier Equipo Terminal Móvil, por lo que, a pesar de la popularidad de las aplicaciones de mensajería instantánea basadas en el uso del protocolo IP, los mensajes cortos siguen siendo una herramienta confiable y muy demandada en el sector empresarial.

No obstante, la falta de controles en la prestación de servicios de mensajes cortos A2P puede abrir la puerta a una serie de problemas significativos para los usuarios, siendo el más evidente el envío de *spam*, resultando no solo molesto para los usuarios, sino una vía para prácticas fraudulentas, como el phishing, que amenazan la seguridad personal y financiera de los usuarios, así como su privacidad.

Por otra parte, la calidad de los servicios de telecomunicaciones también puede ser afectados negativamente. Una red sobrecargada por *spam* puede sufrir retrasos y fallas en la entrega de mensajes cortos de servicios de interés para los usuarios, impactando no solo a los destinatarios del *spam*, sino a todos los usuarios de la red.

Ante este panorama, resulta necesario la implementación de medidas para salvaguardar la experiencia y derechos del usuario evitando el envío de mensajes no solicitados o fraudulentos. A nivel internacional, además de la existencia de ordenamientos jurídicos específicos para la protección de la privacidad de los usuarios y para regular el envío de publicidad, se identifican diversas iniciativas originadas por la industria, las cuales, a través de la adopción voluntaria por parte de los prestadores de servicios, han implementado medidas adicionales de protección para los usuarios, buscando, al mismo tiempo, un desarrollo sano de los actores involucrados en la prestación de servicios de mensajería A2P.

En tal sentido, se proponen principios y buenas prácticas para el envío de mensajes cortos A2P, buscando equilibrar la eficiencia y efectividad del servicio con la protección y respeto a los derechos y la seguridad de los usuarios.

8.1 Principios para el envío de mensajes cortos A2P

Consentimiento del usuario. Para cualquier comunicación con fines mercadotécnicos o publicitarios, los remitentes de mensajes cortos deben contar y mantener el registro del consentimiento del usuario. Se debe aplicar un consentimiento específico para cada campaña de mensajes cortos, evitando el uso de un consentimiento genérico para múltiples campañas ni la transferencia de consentimientos entre remitentes.

Mecanismos *Opt-Out*. Los remitentes de mensajes cortos deben proporcionar un mecanismo claro, sencillo y gratuito para que los usuarios se den de baja o retiren su consentimiento con la finalidad de dejar de recibir mensajes. Esto puede implementarse a través del uso de palabras clave que el usuario puede enviar, como "CANCELAR"," "ALTO", "SALIR", entre otras, o mediante la habilitación de un número de contacto o correo electrónico para tal propósito.

Identidad del remitente: El contenido del mensaje debe permitir al usuario identificar plenamente la identidad del remitente. Los agregadores o redes en los cuales se origina el mensaje corto deben establecer medidas para autenticar y validar la identidad de los remitentes a los que prestan servicios.

Contenido. Se deben prevenir actividades ilícitas o contenido engañoso, fraudulento, no deseado o ilícito. Además, se deben tomar medidas para asegurar que el contenido con fines mercadotécnicos o publicitarios no sea engañoso.

Bloqueo. Los prestadores de servicios y agregadores deben respetar rigurosamente las limitaciones de contacto establecidas para los usuarios inscritos en listas de "No Originar" (DNO), e implementar medidas para la identificación y bloqueo de cualquier remitente asociado con prácticas de *spam* o el envío de mensajes cortos maliciosos.

Horarios de contacto: Se recomienda que los remitentes de mensajes con fines mercadotécnicos o publicitarios limiten su envío en horarios laborales. Los mensajes de servicios, alertas o transaccionales pueden enviarse cuando sea necesario.

Uso de URLs. Los enlaces a sitios web dentro de los mensajes cortos no deben ocultar ni oscurecer la identidad del remitente. Los agregadores o redes en los cuales se originan mensajes cortos A2P deben establecer medidas para prevenir que los remitentes a los que prestan servicios no realicen el envío de enlaces a sitios web con la intención de causar daño o engañar a los consumidores.

Mensajería *Snowshoe.* Debe evitare el uso de esta técnica, que implica distribuir el envío masivo de mensajes a través de múltiples números de origen o códigos cortos.

Auditorías de seguridad. Es recomendable que los prestadores de servicios, agregadores y remitentes de mensajes cortos A2P, implementen de manera conjunta procesos para el monitoreo y auditoría periódica de las campañas de mensajes cortos, a fin de evitar afectaciones a la privacidad de los usuarios.

9. Bibliografía

3GPP. (2022). Technical realization of the Short Message Service (SMS) (3GPP TS 23.040 version 17.2.0 Release 17). Recuperado el 28 de Febrero de 2023, de https://www.etsi.org/deliver/etsi_ts/123000_123099/123040/17.02.00_60/ts_123040v170200p.pdf

3GPP. (2022a). *Alphabets and language-specific information (3GPP TS 23.038 version 17.0.0 Release 17).* Obtenido de https://www.etsi.org/deliver/etsi_ts/123000_123099/123038/17.00.00_60/ts_123038v170000p.pdf

Acker, A. (2014). *The Short Message Service: Standards, infrastructure and innovation.* Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S073658531400015X

Altira. (23 de Octubre de 2019). *¿Qué es SMS A2P? Ventajas y ejemplos de uso*. Obtenido de https://www.altiria.com/4040/que-es-sms-a2p-ventajas-y-ejemplos-de-uso/

Altiria. (Abril de 2022). *Sobre Nosotros*. Obtenido de https://www.altiria.com/nosotros/

Álvarez, C. L. (2018). *Telecomunicaciones y Radiodifusión en México.* Obtenido de http://derecho.posgrado.unam.mx/site_cpd/public/publis_cpd/telecomyradiodifenMX.pdf

ATIS. (2022). *Signature-based Handling of Asserted information using toKENS (SHAKEN).* Obtenido de https://access.atis.org/apps/group_public/download.php/67436/ATIS-1000074.v003.pdf

Autoridad de Telecomunicaciones de Pakistán. (22 de diciembre de 2011). *SMS Report 2011. SMS Traffic in Pakistan during Y2010.* Obtenido de https://www.pta.gov.pk/media/sms_report_2011.pdf

CNMC. (18 de febrero de 2021). *Resolución por la que se aprueba la homogeneización y simplicación de los sistemas de contabilidad de costes de los operadores móviles.* Obtenido de VECO/DTSA/010/20/HOMOGENEIZACIÓN SCC MÓVILES: https://www.cnmc.es/sites/default/files/3388326_4.pdf

ComReg. (2023). *Nuisance Communications*. Obtenido de https://www.comreg.ie/industry/electronic-communications/nuisance-communications/

Congreso General de los Estados Unidos Mexicanos. (01 de julio de 2020). *Ley de Infraestructura de la Calidad.* Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LICal_010720.pdf

CRTC. (2010). *Canadian Anti-Spam Act.* Obtenido de https://laws-lois.justice.gc.ca/eng/acts/E-1.6/FullText.html

CRTC. (2023). *Our Mandate, Mission and What We Do*. Obtenido de https://crtc.gc.ca/eng/acrtc/acrtc.htm

CST. (2022). *Regulations for Curbing SPAM Messages & Calls.* Obtenido de https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_469/c49da5de-60ba-4113-9fed-259ec3437187_Regulations%20for%20Curbing%20SPAM%20Messages%20&%20Calls.pdf

CTA. (03 de Noviembre de 2020). *Canadian Common Short Code Application Guidelines Version 3.8.* Obtenido de https://www.txt.ca/wp-content/uploads/2020/11/Canadian-Common-Short-Code-Application-Guidelines-Version-3-8-Final.pdf

CTA. (2023). *Best Practices for Canadian Application-to-Person (A2P) Messaging Programs.* Canadá. Obtenido de https://www.txt.ca/wp-content/uploads/2023/08/Canadian-A2P-Messaging-Best-Practices-v1.0-August-2023.pdf

CTIA. (2019). *Messaging Principles & Best Practices.* Obtenido de https://api.ctia.org/wp-content/uploads/2019/07/190719-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf

Easterlin, R. P. (1962). Telex in the U.S.A. doi:10.1109/TCE.1962.6373131

Europea, U. (2023). *European Union Website*. Obtenido de https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission_es

FCC. (2018). *FCC 18-178.* Washington, D.C. Obtenido de https://docs.fcc.gov/public/attachments/FCC-18-178A1.pdf

FCC. (2022). *NOTICE OF PROPOSED RULEMAKING.* Obtenido de https://docs.fcc.gov/public/attachments/FCC-22-72A1.pdf

FCC. (2023). *FCC Adopts Its First Rules Focused on Scam Texting.* Obtenido de https://docs.fcc.gov/public/attachments/FCC-23-21A1.pdf

FNE. (30 de enero de 2023). *Informe con recomendación.* Obtenido de Denuncia en contra de WOM en el mercado de los SMS. Rol N°2699-22 FNE: https://www.fne.gob.cl/wp-content/uploads/2023/01/Informe-Rol-2699-22-WOM.pdf

Gobierno de Navarra. Dirección General de Política Económica y Empresarial. (2023). *Acércate a las TIC.* Obtenido de Uso de dispositivos móviles (teléfonos móviles,"smartphones", "ebooks", GPS y "tables"): https://www.navarra.es/NR/rdonlyres/48F9746B-080C-4DEA-BD95-A5B6E01797E1/315641/7Usodedispositivosmoviles.pdf

González Gómez, J. (2002). *El servicio SMS: Un enfoque práctico.* Obtenido de http://www.iearobotics.com/personal/juan/doctorado/sms/sms.pdf

GSMA. (febrero de 2006). *Code of Practice. Mobile Spam 1.0.* Obtenido de https://www.gsma.com/publicpolicy/wp-content/uploads/2012/04/codeofpractice.pdf

GSMA. (25 de julio de 2013). *SMS SS7 Fraud. Versión 4.0.* Recuperado el junio de 2023, de https://www.gsma.com/newsroom/wp-content/uploads/IR.70-v4.0.pdf

GSMA. (2020). *SMS Evolution Versión 2.0.* Obtenido de https://www.gsma.com/newsroom/wp-content/uploads/NG.111-v2.0.pdf

GSMA. (2021). *La Economía Móvil en América Latina 2021.* Obtenido de https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/11/GSMA_ME_LATAM_2021_SPA.pdf

Hillebrand, F. (2010). *Short Message Service (SM) The Creation of Personal Global Text Messaging.* WILEY. Obtenido de https://books.google.com.mx/books?hl=es&lr=&id=YPgfNaoYHUsC&oi=fnd&pg=PR5&ots=y64_UAcnDN&sig=-fRu3IahpUtQmPEDeLeex2h-zaA&redir_esc=y#v=onepage&q&f=false

ICO. (2018). *Spam texts.* Obtenido de https://ico.org.uk/for-the-public/texts/

IFT. (24 de Noviembre de 2016). Resolución mediante la cual el Pleno del Instituto Federal de Telecomunicaciones modifica y autoriza al Agente Económico Preponderante los términos y condiciones del Convenio Marco de Interconexión presentado por Radiomóvil Dipsa, S.A. de C.V. Obtenido de https://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/piftext24111642.pdf

IFT. (12 de octubre de 2021). *Análisis de los sectores de telecomunicaciones y radiodifusión en 2020:.* Obtenido de Valoración de los efectos de la emergencia

sanitaria: https://www.ift.org.mx/estadisticas/analisis-de-los-sectores-de-telecomunicaciones-y-radiodifusion-en-2020

IFT. (2022). *Resolución mediante la cual el Pleno del Instituto Federal de Telecomunicaciones prorroga la vigencia de dos títulos de concesión para usar, aprovechar y explotar bandas de frecuencias del espectro radioeléctrico para uso determinado en los Estados Unidos.* Obtenido de https://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/pift26012221_0.pdf

IFT. (29 de diciembre de 2022a). *Comportamiento de los Indicadores de Mercados y la Economía Digital 2022.* Obtenido de https://www.ift.org.mx/transparencia/indicadores-de-los-mercados-regulados

IFT. (2023). *Convenio Marco de Interconexión entre las redes de Radiomóvil Dipsa, S.A. de C.V. (en lo sucesivo "Telcel") y de (nombre del concesionario) (en lo sucesivo el "concesionario").* Recuperado el Abril de 2023, de https://www.ift.org.mx/sites/default/files/contenidogeneral/politica-regulatoria/cmitelcel2023.pdf

INEGI. (2023). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2022.* Obtenido de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22.pdf

Infobip. (2022). *What is Flash SMS?* Obtenido de https://www.infobip.com/glossary/flash-sms

Le Bodic, G. (2005). *Mobile messaging technologies and services SMS, EMS and MMS* (Segunda ed.). John Wiley & Sons, Ltd. Obtenido de https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/Mobile%20Messaging%20Technologies%20and%20Services.pdf

Marvin, C. (1988). *When Old Technologies Were New: Thinking About Communication in the Late.* Obtenido de https://repository.upenn.edu/cgi/viewcontent.cgi?article=1628&context=asc_papers

MEF. (2020). *RCS Business messaging best practices 2.0. Implementation guides for the effective launch of A2P & P2A communication services via RCS.* Obtenido de https://mobileecosystemforum.com/programmes/future-of-messaging/market-development/rich-business-messaging-best-practices/

MEF. (12 de diciembre de 2020a). *Business SMS. Code of Conduct.* Obtenido de https://mobileecosystemforum.com/programmes/future-of-messaging/fraud-management/trust-in-enterprise-messaging/a2p-code-of-conduct/#:~:text=0%20of%20MEF's%20Business%20SMS,practices%20and%20poor%20procurement%20processes.

MEF. (2021a). *Business SMS Fraud Framework. Version 3.0.* Obtenido de https://mobileecosystemforum.com/enterprise-mobile-messaging-fraud-framework/

O. Osho, O. Y. (2014). Frameworks for Mitigating Identity Theft and Spamming through Bulk Messaging. *Proceedings of the IEEE 6th International Conference on Adaptive Science and Technology,* (págs. 1-6). Ota, Nigeria. doi:10.1109/ICASTECH.2014.7068119

OCDE. (2006). *Report of the OECD Task force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures.* doi:DSTI/CP/ICCP/SPAM(2005)3/FINAL

OECD. (2023). *Acerca de*. Obtenido de https://www.oecd.org/acerca/

Ofcom. (2022). *Improving the accuracy of Calling Line Identification (CLI) data.* Obtenido de https://www.ofcom.org.uk/__data/assets/pdf_file/0031/247486/statement-improving-accuracy-CLI-data.pdf

Ofcom. (2022). *Tackling scam calls and texts.* Obtenido de https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-scam-calls-and-texts

Ofcom. (2022). *Tackling scam calls and texts: Ofcom's role and approach.* Obtenido de https://www.ofcom.org.uk/__data/assets/pdf_file/0018/232074/statement-tackling-scam-calls-and-texts.pdf

Ofcom. (2023). *About Ofcom*. Obtenido de https://www.ofcom.org.uk/about-ofcom

Ofcom. (2023). *Tackling nuisance calls and messages.* Obtenido de https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-nuisance-calls-messages

OMDIA. (2021). *Market Landscape: Developments in Wholesale Telecom Security & Anti-Fraud.* Obtenido de https://omdia.tech.informa.com/OM017047/Market-Landscape-Developments-in-Wholesale-Telecom-Security--AntiFraud

OMDIA. (2023). *Mobile Messaging Traffic and Revenue Forecast Report – 2023*. Obtenido de https://omdia.tech.informa.com/OM031727/Mobile-Messaging-Traffic-and-Revenue-Forecast-Report--2023

Parlamento Europeo, Consejo de la Unión Europea. (2002). *EUR-Lex - 32002L0058 - EN - EUR-Lex.* Obtenido de DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02002L0058-20091219

PROFECO. (2023). *¿Qué hacemos?* Obtenido de https://www.gob.mx/profeco/que-hacemos

PROFECO. (2023). *Informes de actividades.* Obtenido de https://www.gob.mx/profeco/documentos/informes-de-actividades-29444?state=published

PROFECO. (2023a). *Registro Público para Evitar Publicidad (REPEP)*. Obtenido de https://repep.profeco.gob.mx/

Secretaría de Economía. (08 de enero de 2016). *La Normalización en México: cuáles son sus funciones y beneficios para el consumidor*. Obtenido de https://www.gob.mx/se/articulos/la-normalizacion-en-mexico-cuales-son-sus-funciones-y-beneficios-para-el-consumidor#:~:text=La%20normalizaci%C3%B3n%20regula%20las%20actividades,%2C%20directrices%2C%20especificaciones%2C%20atributos%2C

Secretaría de Economía. (08 de marzo de 2019). *NORMA Oficial Mexicana NOM-184-SCFI-2018.* Obtenido de Elementos normativos y obligaciones específicas que deben observar los proveedores para la comercialización y/o prestación de los servicios de telecomunicaciones cuando utilicen una red pública de telecomunicaciones (cancela a la NOM-184-SCFI-2012).: https://www.dof.gob.mx/nota_detalle.php?codigo=5552286&fecha=08/03/2019#gsc.tab=0

SMPP Developers Forum. (1999). *Short Message Peer to Peer Protocol Specification v3.4 Issue 1.2.* Obtenido de https://smpp.org/SMPP_v3_4_Issue1_2.pdf

SMPP Developers Forum. (2003). *Short Message Peer-to-Peer Protocol Specification Version 5.0.* Obtenido de https://smpp.org/SMPP_v5.pdf

SMPP Developers Forum. (2019). *SMPP Protocol: API to enable SMS messaging between applications and mobiles.* Obtenido de https://smpp.org/

Taylor, A. &. (2005). *An SMS history.* Obtenido de https://www.researchgate.net/publication/226340906_An_SMS_history

The CIU. (5 de Octubre de 2021). *Mercado de Smartphones en México: Evolución, Relevancia y Reconfiguración.* Obtenido de https://www.theciu.com/documentos-de-analisis/2021/10/5/mercado-de-smartphones-en-mxico-evolucin-relevancia-y-reconfiguracin

Truecaller. (2022). *Truecaller Insights 2022 U.S. Spam & Scam Report*. Recuperado el 2023, de https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report

UIT. (2021). *ITU-T TR.spoofing Countering spoofing.* Obtenido de https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-TRUST-2021-PDF-E.pdf

Unión Internacional de Telecomunicaciones. (1988). SERIE U: CONMUTACIÓN TELEGRÁFICA. Obtenido de https://www.itu.int/rec/T-REC-U.80-198811-S

Vodafone. (04 de December de 2017). *25 years since the world's first text message*. Obtenido de https://www.vodafone.com/news/technology/25-anniversary-text-message

Anexo I

Cuadro comparativo

Experiencia internacional referente al control del envío de mensajes no deseados

PAÍS	REGULADOR / ASOCIACIÓN	INSTRUMENTO NORMATIVO	REGLAS ESPECÍFICAS SOBRE ENVÍO DE MENSAJES	DATOS RELEVANTES
Estados Unidos de América	FCC *(Federal Communications Commission*) CTIA (*Cellular Telecommunications and Internet Association*)	*Messaging Principles and Best Practices*, es un conjunto de mejores prácticas voluntarias desarrolladas por los miembros de CTIA.	Se establecen las mejores prácticas de la "mensajería para no consumidores" (asociada a SMS A2P), entre las que podemos encontrar: - Consentimiento del consumidor (implícito, expreso, escrito) - Privacidad y seguridad - Contenido (prevenir *Spam*, *spoofing*) - Numeración validada para remitentes de mensajes - Números compartidos y códigos cortos para remitentes - Evitar "*Snowshoe Messaging*" - Evitar rutas grises para enviar mensajes - Evitar códigos cortos comunes fuera del plan de numeración de E.U.A.	*Messaging Principles and Best Practices* ha sido utilizado por operadores como T-Moblie y AT&T para la creación de sus propios códigos de conducta. *Messaging Principles and Best Practices* se crea de conformidad con las leyes y regulaciones aplicables en E.U.A. como el *Telephone Consumer Protection Act (TCPA)* y el *Controlling the Assault of NonSolicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)*
		Controlling the Assault of NonSolicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)	El término "*commercial electronic mail*" puede ser aplicable a SMS, y se establece claramente que se prohíbe la transmisión de información falsa o engañosa, con encabezados engañosos o que no identifique al remitente. Asimismo, indica que no pueden enviarse mensajes después de que el receptor solicita no recibir mensajes comerciales.	*CAN-SPAM Act* define el mensaje de correo electrónico comercial como aquel mensaje cuyo objetivo principal es la publicidad comercial o promoción de un producto o servicio, y no incluye mensajes transaccionales. El término puede ser atribuido al servicio de mensajes cortos,

				pues *Messaging Principles and Best Practices* hace alusión al *CAN-SPAM Act* para su emisión.
Canadá	CRTC (*Canadian Radio-television and Telecommunications Commission*) CTA (*Canadian Telecommunications Association*)	*Best Practices for Canadian Application-to-Person (A2P) Messaging Programs* es una guía creada por CTA a petición de sus miembros.	Se define la mensajería Aplicación a Persona (A2P) y se detallan los canales y protocolos A2P (códigos cortos comunes, números gratuitos, números a 10 dígitos, mensajería empresaria enriquecida RBM), los tipos de mensajes A2P, así como las mejores prácticas para su prestación, entre las que se encuentran: - Consentimiento bajo la *Canada's Anti-Spam Legislation (CASL)* - Estándares de gestión de programas para envío de SMS A2P - Promoción y publicidad clara de programas A2P respecto a términos y condiciones de este - Auditorias y pruebas al programa A2P - Reducir el envío de spam y mensajes maliciosos, para cumplir con los requerimientos de la CASL - Evitar prácticas desaconsejables (rutas grises, numeración compartida, ciclo de numero/URL, "*Snowshoe Messaging*", fraude de inflación de tráfico artificial, *spoofing*, *spam*, *phishing*, mensajes maliciosos)	Además de establecer las mejores prácticas para la prestación del servicio SMS A2P, *Best Practices for Canadian Application-to-Person (A2P) Messaging Programs* presenta términos, definiciones y protocolos relacionados con el servicio, así como los casos de uso comunes en A2P y recursos regulatorios asociados a las mejores prácticas.
		Canada's Anti-Spam Legislation (CASL)	Prohíbe el envío, creación o permitir que se envíen mensajes comerciales sin el consentimiento del receptor y que no se ajuste a las siguientes características: - Identificación clara del remitente - Contacto claro del remitente - Mecanismo de cancelación	*Canada's Anti-Spam Legislation* (CASL) entiende el mensaje como cualquiera por medio de telecomunicaciones (texto, sonido, voz, imagen) y se considera comercial cuando fomenta la participación en una actividad

				comercial (ofertas de compra/venta, ofertas de negocio, publicidad, promoción de personas con fines comerciales)
Arabia Saudita	CST (*Communications, Space & Technology Commission*)	Regulations for Curbing SPAM Messages & Calls	Se establece una clasificación de SMS, siendo estas: - Mensajes promocionales - Mensajes de servicio - Mensajes de concientización - Mensajes de advertencia - Mensajes personales Asimismo, se establecen las obligaciones mínimas que deberán considerar los diferentes actores dentro del servicio, como pueden ser: - Para operadores: o Base de datos de fraudes y estafas o Soluciones técnicas para impedir *spam, scam, spoof* o Sistemas técnicos de estudio y análisis de usuarios o Filtros a SMS masivos - Para proveedores SMS: o Suspensión de mensajes idénticos enviados a más de 50 números en 1 minuto o Correcta clasificación de remitentes o No enviar mensajes de campañas promocionales - Para remitentes: o No comprar/vender mensajes masivos no autorizados o Clasificación correcta de SMS masivos	El documento *Regulations for Curbing SPAM Messages & Calls* se crea con fundamento en la Telecommunication and Information Technology Act, particularmente atendiendo el artículo 2.5 que establece protección de los usuarios y sus intereses, así como en proporcionar comunicaciones con la apropiada calidad, protección contra contenido dañino y manteniendo la confidencialidad de las comunicaciones.

			○ No enviar campañas promocionales desde sus sistemas hacia sistemas de otros proveedores de SMS.	
Australia	ACMA (*Australian Communications and Media Authority*)	Spam Act 2003	Se regula de manera general el envío de mensajes electrónicos comerciales, en los que se puede considerar el servicio de mensajes cortos en su modalidad A2P, Se establecen normas sobre el *software* de recopilación de direcciones y listas de direcciones recogidas, además de señalar las sanciones y establecer la obtención de consentimientos para el envío de los mensajes. Entre los principales objetivos del *Spam Act* 2003 se encuentran: - Prohibición a enviar mensajes no solicitados - Incluir información precisa del remitente - Los mensajes deben contener una manera funcional de dar de baja su recepción - No se deben suministrar, adquirir ni utilizar software de recopilación de direcciones, ni listas de direcciones recopiladas	El *Spam Act* 2003 considera sanciones civiles y/o económicas a quien no atienda las disposiciones, además de compensaciones a los afectados por el envío de mensajes electrónicos comerciales, siempre que haya sufrido daños o pérdidas a causa de estos. El consentimiento para el envío de mensajes electrónicos comerciales debe ser expreso.
Francia	ARCEP (*Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse*)	Code des postes et des communications électroniques	Define las comunicaciones electrónicas como cualquier emisión, transmisión o recepción de signos, señales, escrituras, imágenes o sonidos, por cable, por radio, por medios ópticos o por otros medios electromagnéticos, por lo que dentro de dicha definición se puede considerar el servicio de mensajes cortos, con independencia de su modalidad.	El código presenta una sección específica para las disposiciones aplicables a las comunicaciones electrónicas.
		Décision n° 2022-1583 du 1er septembre 2022 modifiant la décision établissant le	Establece las condiciones específicas de los números de uso general utilizables para intercambios con una plataforma técnica, misma que puede entenderse como una aplicación con la que se puede tener una comunicación con usuarios de comunicaciones electrónicas, haciendo	Las condiciones específicas, en el apartado 2.3.9 indican la manera en que se asignan los números a utilizar, su estructura geográfica, las condiciones de uso, condiciones de

		plan national de numérotation et ses règles de gestion	referencia a los mensajes cortos en su modalidad A2P.	elegibilidad de los operadores de comunicaciones que los soliciten, el tiempo de uso de los números, así como un apartado de protección contra llamadas realizadas por sistemas automatizados
Irlanda	ComReg (*Commission for Communications Regulation*)	Combatting scam calls and texts Consultation on network based interventions to reduce the harm from Nuisance Communications	Propuesta del regulador irlandés de telecomunicaciones para combatir estafas mediante llamadas y mensajes de texto fraudulentos, a través de medidas como las siguientes: - Bloqueo de Identificador de línea llamante (CLI por sus siglas en inglés) fijo - Bloqueo de CLI móvil - Una lista de número protegidos, que no estén en funcionamiento para que no sean empleados por estafadores - Lista No Originar, para registrar remitentes y bloquear a aquellos que no lo estén	Resulta importante destacar que el documento *Combatting scam calls and texts Consultation on network based interventions to reduce the harm from Nuisance Communications* se sometió a consulta pública por el regulador irlandés para la obtención de comentarios respecto al proyecto por parte de los interesados, y aún no es aplicable en irlanda.
Reino Unido	Ofcom (Office of Communications)	Improving the accuracy of Calling Line Identification (CLI) data	Requiere a los proveedores que, cuando sea técnicamente posible, detecten y bloqueen las llamadas que contengan datos de la CLI (Identificación de la línea llamante) que no sean válidos, no identifiquen de manera única al llamante o no incluyan un número que pueda marcarse. Especifican lo siguiente: - CLI debe ser un número de 10 u 11 dígitos - Se usan datos de asignación de numeración proporcionados por Ofcom y lista de "No Originar" (DNO) para identificar números inapropiados	A través del documento *Improving the accuracy of Calling Line Identification (CLI) data* en Reino Unido se exige a los proveedores de servicios de telecomunicaciones roporcionar información sobre el remitente de la llamada para ayudar al receptor a comprender quién lo está llamando y decidir si desean responder, y se propusieron medidas para que los proveedores comprendan mejor cómo esperamos que

			- Se detectan y bloquean llamadas sin CLI válida proveniente del extranjero - Se detectan y bloquean llamadas del extranjero que suplantan CLI del Reino Unido - Se prohíbe el uso de números no geográficos que comienzan con 09 como CLI	utilicen los datos asociados con las llamadas.
		The Do Not Originate (DNO) list	Tiene el propósito de registrar los números empleados para recibir llamadas, pero no para realizarlas (bancos, instituciones gubernamentales). Permite a los proveedores verificar las llamadas entrantes en función de los números registrados en la lista DNO, y en caso necesario, bloquear la llamada.	Lista creada en asociación de Ofcom con la UK Finance. Existe una guía para las organizaciones, para saber cómo integrar números a la lista DNO.
	ICO (Information Commissioner's Office)	Memorandum of Understanding Nuisance and Scam Calls (Technical Measures)	Establece medidas técnicas para reducir el impacto de las llamadas ilegales molestas y fraudulentas en los consumidores. Asegura el desarrollo de la confianza al: - Establecer el origen de las llamadas cuando sea técnicamente factible - Dotar a los usuarios herramientas para gestionar mejor sus llamadas entrantes - Facilitar la toma de medidas contra llamantes que generen comunicaciones electrónicas ilegales	En este contexto, las responsabilidades de ICO se centran en mantener la lista de números de teléfono de personas y empresas que desean excluirse de recibir llamadas de marketing en vivo no solicitadas o faxes de marketing no solicitados, así como de tomar medidas de cumplimiento para asegurarse de que no se realicen llamadas de marketing directo a números de teléfono incluidos en el registro del servicio telefónico sin consentimiento previo.
Nueva Zelanda	Ministry of Business, Innovation, and Employment	The Unsolicited Electronic	Aplicable para mensajes electrónicos no solicitados, esta ley busca prohibir el envío de mensajes de carácter comercial que no hayan sido previamente	La ley, en su definición de mensaje electrónico, abarca diferentes tipos de mensajes,

		Messages Act 2007	solicitados por los receptores, además de exigir que dichos mensajes comerciales incluyan información precisa sobre el remitente y mecanismos de cancelación para dejar de recibir dichos mensajes.	entre los que se puede considerar el SMS, sin embargo, define ciertas características por las que algunos mensajes no podrán aplicar en esta ley, entre los que se encuentran: - Respuestas a solicitud de cotización - Mensajes de confirmación de transacción comercial - Información de garantía, retiros de productos, y seguridad de bienes - Entrega de bienes
Internacional	GSMA (*Global System for Mobile communications Association*)	Code of Practice Mobile Spam 1.0	Diseñado por GSMA para que los clientes de operadores móviles reciben la menor cantidad posible de *spam* a través de SMS/MMS. Abarca SMS/MMS de índole comercial enviados a clientes sin su consentimiento, o que incentivan el envío de mensajes a números con tarifas adicionales, así como mensajes masivos fraudulentos (mensajes falsos, suplantación de identidad, estafas). Entre sus compromisos se encuentran: - Incluir clausulas contra *spam* en contratos con proveedores externos - Establecer mecanismos de consentimiento del cliente - Colaboración entre operadores móviles para problemáticas de *spam*	Documento de carácter voluntario y sin fuerza legal, que requiere el compromiso de los operadores para adaptarlo en sus prácticas.

			- Informar a los clientes para reducir el impacto de *spam* - Realizar actividades contra *spam*, como revisión de contratos, investigación de denuncias, monitorear redes - Fomentar el apoyo de los gobiernos y reguladores respaldando mecanismos de autorregulación de la industria, apoyar prácticas responsables e investigación de fraudes y abusos	
	Comisión Europea	DIRECTIVA 2002/58/CE	Directiva creada con el objetivo de garantizar la privacidad y la protección de datos en las comunicaciones electrónicas en los países miembros de la UE. El artículo 13, relacionado con las comunicaciones no solicitadas establece: - El uso de comunicación sin intervención humana con fines de venta directa solo podrá autorizarse cuando los usuarios hayan dado su consentimiento previo - No se permitirá el envío de mensajes electrónicos con fines de venta en los que se disimule o se oculte la identidad del remitente	Directiva emitida por la Comisión Europea en un sentido general, en el que no se hace mención explícita de su aplicación única en el servicio de mensajes cortos en su modalidad A2P.
	OCDE (Organización para la Cooperación y el Desarrollo Económico)	Anti-Spam Toolkit	Entre las mejores prácticas, la OCDE recomienda incluir las relacionadas con: - Servicios afectados - Finalidad comercial - Consentimiento - Dirección para darse de baja - Información sobre el origen de los mensajes	Compuesto por 8 elementos interrelacionados que abordan: - Enfoques normativos: desarrollo de legislación antispam

			- No *bulk* - Etiquetado - Sanción a la persona que autoriza el envío de *spam* ayuda/asiste/facilita al *spammer* - Sanción a *software* de recolección de listas de direcciones - Acceso ilegal - Contenidos engañosos o fraudulentos - Amenazas de seguridad - Jurisdicción fronteriza	- Preocupación por la aplicación de la ley: ejecución y aplicación de la ley para frenar el spam - Iniciativas impulsadas por la industria: las leyes deben acompañarse de acciones del sector privado - Soluciones técnicas: aplicación de herramientas y métodos tecnológicos antispam - Educación y orientación: capacitación a usuarios finales sobre cómo enfrentar el spam - Asociaciones cooperativas contra el spam: cooperación público-privada, con intercambio de información y buenas prácticas - Métricas del spam: evaluación de la evolución del spam Cooperación mundial: cooperación entre gobiernos, sector privado, sociedad civil y otros interesados

				El *Anti-Spam Toolkit* busca fomentar el desarrollo de una legislación antispam para garantizar los beneficios de las comunicaciones electrónicas. Basado en 4 principios generales: - Orientación política - Simplicidad normativa - Eficacia de aplicación - Vínculos internacionales
	MEF (*Mobile Ecosystem Forum*)	Business SMS Code of Conduct	Entre los principios que establece el Código de Conducta del MEF se destacan: - No se crearán, transportarán ni entregarán mensajes SMS A2P no solicitados - Se debe aceptar que los consumidores podrán cambiar o revocar su consentimiento para ser contactados - Los generadores de mensajes deben respetar las preferencias legales de los consumidores con respecto al tiempo y frecuencia de la interacción de SMS A2P - Se debe proteger y manejar adecuadamente los datos personales de los consumidores - No se modificará el contenido de los mensajes o sus metadatos a menos que se requiera legítimamente para la entrega del mensaje	El *Business SMS Code of Conduct* se presenta por MEF como un documento que podrá ser firmado por los interesados en aplicar los principios que establece. Código presenta un apartado relacionado con la gestión de incidentes de fraude, entre los que se destaca que, una vez detectado que se envían mensajes no deseados, y que esto no ha cesado, se debe bloquear el tráfico fraudulento; se deben proporcionar pruebas del consentimiento de aceptación o el cese del tráfico sospechoso dentro de un tiempo estipulado bajo contrato.

			- Se deben implementar procedimientos y herramientas efectivos para evitar el fraude al consumidor o fraude comercial - No se podrá acceder ni utilizar la infraestructura de otra empresa para ningún propósito para el que no tengan una autorización explicita - No se ocultará la identidad ni se utilizará la de otra persona - Se promoverá y educará activamente a todas las partes de la industria para garantizar que cada servicio ofrecido sea seguro, confiable y cumpla con todos los requisitos operativos y legales relevantes - Los interesados deberán ayudar de manera proactiva a los reguladores, a agencias de aplicación de la ley o otras partes del ecosistema para limitar el alcance y la recurrencia de incidentes fraudulentos e identificar actores fraudulentos	

COLABORADORES QUE PARTICIPARON EN LA ELABORACIÓN DE ESTE ESTUDIO.

Vanegas Soriano José Pablo

Dirección General de Regulación de Interconexión y Reventa de Servicios Mayoristas

Huichán Muñoz Gabriel

Dirección de Regulación Técnica de Servicios Mayoristas

Ramírez Pedraza Mario Izael

Subdirección de Regulación Técnica de Interconexión

Andrade Zarco Carlos David

Jefatura de Departamento de Regulación Técnica de Interconexión

Pérez Villarreal Glorismel Del Carmen

Profesional de Intercambio

INSTITUTO FEDERAL DE TELECOMUNICACIONES

Insurgentes Sur 1143, Col. Nochebuena,

Demarcación Territorial Benito Juárez, C.P. 03720

Ciudad de México, Tel: 55 5015 4000 / 800 2000 120

www.ift.org.mx