UNIDAD DE POLÍTICA REGULATORIA
INSTITUTO FEDERAL DE TELECOMUNICACIONES
Insurgentes Sur No. 1143
Colonia Noche Buena
Demarcación territorial Benito Juárez
C.P. 03720, Ciudad de México

Ciudad de México, a 20 de septiembre de 2024

**Asunto**: *Comentarios de AT&T a la consulta pública sobre el "Anteproyecto de Lineamientos para garantizar la seguridad de las comunicaciones de voz a través de redes públicas de telecomunicaciones".*

**Antonio Díaz Hernández**, en mi carácter de apoderado legal de **AT&T Comunicaciones Digitales, S. de R.L. de C.V.**, **Grupo AT&T Celullar, S. de R.L. de C.V.** y **AT&T Comercialización Móvil, S. de R.L. de C.V.** (en lo sucesivo, y conjuntamente, "**AT&T México**"), personalidad que acredito con la copia de las escrituras que se encuentran anexas al presente escrito y que previamente se han presentado ante ese Instituto Federal de Telecomunicaciones (en adelante "IFT" o "Instituto"); señalando como domicilio para oír y recibir todo tipo de notificaciones y en relación al presente el ubicado en Río Lerma 232, Piso 20, Colonia Cuauhtémoc, Demarcación territorial Cuauhtémoc, C.P. 06500, Ciudad de México, autorizando para tales efectos a Carlos Edgardo Hirsch Ganievich, Blanca Luévano García, José Manuel Tolentino Medrano, Roberto Carlos Aburto Pavón y Zyanya Norman González, con el debido respeto comparezco a exponer:

## ANTECEDENTE

**ÚNICO**. Con fecha 9 de agosto de 2024, el Instituto Federal de Telecomunicaciones a través de su Unidad de Política Regulatoria publicó para comentarios, opiniones y aportaciones la consulta pública relacionada con el "Anteproyecto de Lineamientos para garantizar la seguridad de las comunicaciones de voz a través de redes públicas de telecomunicaciones" (el "Anteproyecto de seguridad en comunicaciones de voz").

## COMENTARIOS GENERALES

Agradecemos y valoramos la mecánica de consultas públicas que está utilizando el Instituto para enriquecer y mejorar sus resoluciones.

Coincidimos y compartimos el objetivo del IFT de proteger a los usuarios de llamadas no deseadas o incluso fraudulentas. Sin embargo, creemos que el mecanismo propuesto es complicado y podría no cumplir el propósito deseado.

Entendemos que el objetivo del IFT en la consulta es: *se considera necesario definir las reglas operativas sobre el manejo del CLI a efecto de inhibir prácticas no deseadas que pueden afectar tanto a los usuarios como a los operadores de redes públicas de telecomunicaciones al generar afectaciones económicas y de seguridad considerables, erosionar la confianza de los usuarios en el uso de servicios públicos de telecomunicaciones y que pueden generar una degradación en la calidad de los servicios y/o vulnerar su integridad*.

Del mismo documento se puede apreciar que las prácticas relacionadas con el CLI que el IFT considera peligrosas y que desea evitar son:

> Tráfico Sospechoso: Tipo de tráfico que se identifica por un patrón de llamadas de voz que transita por una o más redes de Proveedores de Servicios de Voz y tiene características asociadas con prácticas ilegales o fraudulentas como pueden ser:
>
> - Un alto número de llamadas de corta duración originadas por una Identidad de Línea Llamante o grupo de Líneas Llamantes en particular.
> - El número utilizado en la Identidad de Línea Llamante no es un número que se pueda marcar o no se muestra la Identidad de Línea Llamante.
> - El número utilizado en la Identidad de Línea Llamante pertenece a un bloque de numeración que no ha sido asignado o que no ha sido portado al Proveedor de Servicios de Voz que origino la llamada.
> - El número utilizado en la Identidad de Línea Llamante de una llamada nacional no corresponde a un número del Plan Nacional de Numeración.
> - El número utilizado en la Identidad de Línea Llamante de una llamada internacional entrante corresponde a un número del Plan Nacional de Numeración, no cumple con el estándar UIT-T E.164 o no se proporciona;

Como puede observarse, de la definición anterior el primero punto no está relacionado con el CLI o identificador de llamada y los cuatro puntos restantes pueden resumirse en que el número con el que se "origina" la llamada no pertenece al usuario que la está originando.

Por otro lado, asumimos que este tipo de fenómenos se genera en usuarios que el IFT denomina "Servicios de voz No Residenciales" y que son conocidos como *Call Centers o* como *conmutadores*. Otra posible fuente de este tipo de tráfico son las llamadas internacionales que analizaremos por separado.

COMENTARIOS PARTICULARES

i. En el Anteproyecto de seguridad en comunicaciones de voz se identifican cuatro tipos de obligaciones.

1) Para la red que origina una llamada

La red que origina una llamada es la única que cuenta con la información para determinar si el CLI o número de origen pertenece realmente a ese usuario, puesto que es dicho prestador de servicios de voz quien le asigna la numeración y gestiona sus llamadas. Sin embargo, no es técnicamente posible verificar el CLI en cada llamada en tiempo real.

Lo que sí es posible es realizar esta verificación en un postproceso. En caso de que el prestador de origen detectara en este proceso posterior que se está enviando un número de origen que no corresponde con la numeración asignada a dicho usuario, podría inmediatamente "programar" a esa troncal un número fijo e impedir que el usuario pueda modificarlo.

Este proceso garantizaría la solución del problema en un corto tiempo y sin necesidad de intervención de terceros. El cumplimiento de esta regla podría ser supervisado por el IFT, puesto que es sencillo y además se encuentra dentro de sus facultades.

2) Para la red que recibe la llamada

La red que recibe la llamada no tiene forma de detectar si el CLI recibido es correcto o no es correcto y tampoco el patrón de comportamiento de un usuario; la única forma de saberlo sería por medio de una queja de un usuario. En esta propuesta, pareciera que el IFT le asigna la responsabilidad principal de averiguar el origen de la queja, realizar requerimientos a otras redes (para los que no tienen facultades), darle seguimiento y finalmente reportar los resultados al IFT. Esta parte del proceso carece de legalidad, de incentivos y de sentido práctico. Lo más probable es que lleguen esas llamadas sospechosas a usuarios de diversas redes, tendríamos varios destinos y operadores intentando resolver un problema que no les corresponde. El tema debe resolverse en el origen.

El derecho que supuestamente le otorga del IFT a los operadores de "investigar" llamadas, en realidad se transforma en una obligación de entregar "información" a cualquier operador que la solicite e incluso destinar personal a esta función. Esto es costoso de implementar y no beneficia en nada al proceso que se pretende crear. Como dijimos, este mecanismo propuesto no es el idóneo.

3) Para los "servicios de voz no residenciales o call centers"

En este tema el IFT propone obligar, por medio de los contratos de los operadores que los atienden a ciertos compromisos que se resumen en "portarse bien y no hacer travesuras". En el caso de la experiencia internacional y los países que se mencionan en el documento de consulta existe una legislación que tipifica como delito del orden civil

las prácticas que estamos tratando de corregir. En México no existe esta legislación y, por tanto, el IFT no tiene facultades para supervisar y mucho menos sancionar estos comportamientos. En el mejor de los casos, después de un proceso engorroso, lo único que estaría ocurriendo es que estos *call centers* cambiarían de razón social o de prestador y no se lograría ningún resultado práctico.

4) Tráfico internacional

El tráfico internacional en algunos casos llega a México con números a 10 dígitos que pueden coincidir o simular números mexicanos. En estos casos, lo que se puede exigir es que, al llegar a México, las llamadas que tengan CLI deberán incluir un código de país para que no se confundan con números mexicanos.

## ii. Estudio del Servicio de Mensajes Cortos Aplicación a Persona

En 2023 el IFT preocupado por el spam que se ha generado en el envío de Mensajes Cortos (SMS) A2P que afecta a los usuarios publicó el Estudio del Servicio de Mensajes Cortos Aplicación a Persona, en el que señala que:

- De conformidad con la NOM 184 los proveedores de servicios de telecomunicaciones deben abstenerse de enviar mensajes de texto con fines comerciales, así como publicidad de terceros, a menos que los consumidores hayan manifestado su consentimiento expreso.

- Con la modalidad de SMS A2P han surgido prácticas no deseadas, las cuales pueden generar afectaciones a la privacidad y seguridad de los usuarios, así como un alto consumo de los recursos de 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. Las prácticas no deseadas más relevantes son:

    - Spam: al enviar mensajes cortos con destino a usuarios que no han dado su consentimiento para ser contactados.

    - Flooding: cuando se envía un gran número de mensajes a uno o más destinatarios, ya sean mensajes legítimos o no. La práctica no deseada se constituye cuando la cantidad de mensajes enviados es significativamente mayor que la carga normal y el valor máximo de mensajes esperados.

    - Spoofing: cuando se falsifica la información del origen para parecer legítima.

    - Rutas grises: cuando se envían mensajes A2P haciéndolos parecer P2P y/o para aprovechar tarifas de interconexión más bajas o nulas.

- La falta de controles de mensaje SMS A2P puede generar problemas a los usuarios y a las redes, por lo que para salvaguardar la experiencia del usuario el IFT propone algunos principios y buenas prácticas:

    - Consentimiento del usuario: se debe aplicar un consentimiento específico para cada campaña de mensajes cortos, evitando consentimientos genéricos para múltiples compañías.

    - Mecanismos Opt-Out: un mecanismo claro y sencillo para que el usuario se dé de baja o retire su consentimiento para recibir mensajes. Se plantea que el usuario pueda enviar una palabra como "CANCELAR", "ALTO", "SALIR".

    - Identidad del remitente: el contenido debe permitir al usuario identificar claramente el remitente.

    - Contenido: prevenir actividades ilícitas o contenido engañoso, fraudulento, no deseado o ilícito.

    - Bloqueo: los prestadores de servicio deben respetar rigurosamente las limitaciones de contacto e implementar medidas para a identificación y bloqueo de cualquier remitente asociado con prácticas de spam.

    - Horario de contacto: los remitentes deben limitar el envío de mensajes con fines mercadotécnicos o publicitarios en horarios laborales.

    - Uso de URL: evitar que los enlaces a sitos web no oculten la identidad del remitente, ni que los remitentes realicen envío de enlaces a sitios web con la intención de causar daño o engañar a los consumidores.

    - Mensajería Snowshoe. Evitar distribuir el envío masivo de mensajes a través de múltiples números de origen o códigos cortos.

    - Auditorías de seguridad: que los actores en la provisión de mensaje implementen procesos para el monitoreo y auditoría periódica de las campañas de mensajes cortos.

Así, es necesario también definir obligaciones de los operadores que generan mensajes A2P para la seguridad de las comunicaciones SMS. Por lo que sugerimos considerar también el spam que se ha incrementado con la autorización del IFT de enviar a través de la interconexión mensajes A2P y que afectan igualmente a los usuarios del servicio móvil.

iii. Conclusiones:

Por lo anteriormente expuesto consideramos que el objetivo de la consulta, en lo referente a evitar que se comentan fraudes por medio de la falsificación del CLI, es válido y puede solucionarse. El método propuesto no es el adecuado, es complicado, lento y no tendría ningún efecto práctico.

Proponemos que se ataque el problema en el origen. Si el prestador de origen (donde se genera la llamada) detecta en postproceso que se están utilizando CLI que no pertenecen al usuario, inmediatamente se aplica un CLI fijo en la central que atiende a dicho usuario y de este modo se elimina el problema sin afectar el tráfico de origen.

Esta solución es simple, rápida, se encuentra dentro de las facultades y control del IFT y es muy probable que disminuya de forma significativa este problema.

En cuanto a otras prácticas fraudulentas que no están relacionadas con el CLI, consideramos que deben atenderse por medio de la autoridad judicial y legal correspondiente.

Finalmente, este Instituto, preocupado por el envío de SMS no deseados, debería generar obligaciones hacia los operadores que envían tráfico A2P por interconexión para garantizar la seguridad de las comunicaciones SMS.

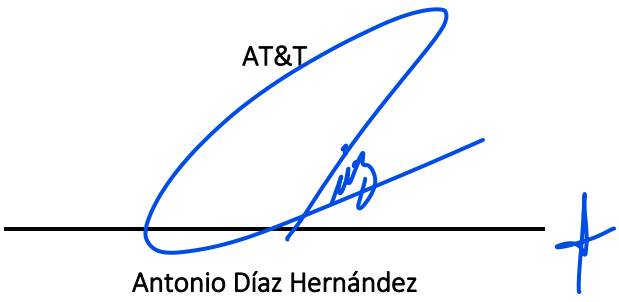
Por lo expuesto solicitamos al Instituto Federal de Telecomunicaciones:

**PRIMERO.-** Tenerme por presentado en los términos del presente escrito, en representación de AT&T y por autorizadas a las personas y domicilio que se señala en el proemio para oír y recibir notificaciones.

**SEGUNDO.-** Se tengan por presentados en tiempo y forma, los comentarios y opiniones de AT&T respecto de la *consulta pública sobre el "Anteproyecto de Lineamientos para garantizar la seguridad de las comunicaciones de voz a través de redes públicas de telecomunicaciones".*

Atentamente,

AT&T



Antonio Díaz Hernández

Apoderado legal