Zanya Pineda
ABOGADA

Bogotá D.C. 22 de diciembre de 2025

Doctora
CLAUDIA XIMENA BUSTAMANTE
Directora Ejecutiva
Comisión de Regulación de Comunicaciones
Correo: medidasantifraude@crcom.gov.co.
Ciudad

Asunto: Comentarios a la alternativa regulatoria de Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles

Respetada Doctora Bustamante:

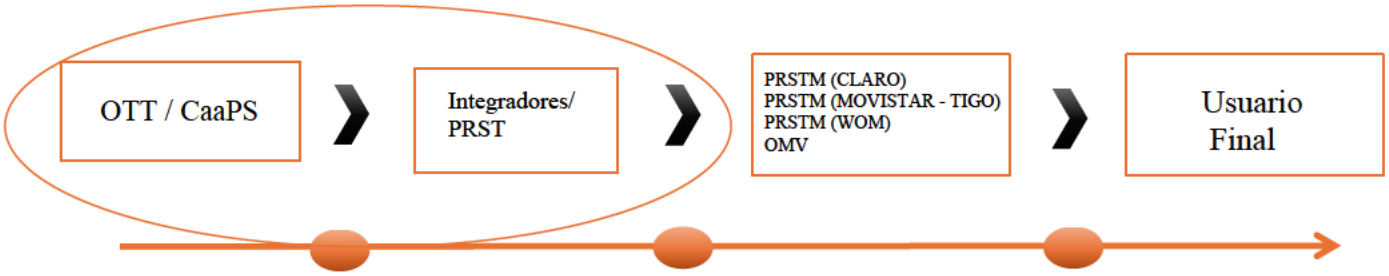
Me permito remitir comentarios Comentarios a la alternativa regulatoria de Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles, en los siguientes términos:

El fenómeno del fraude en llamadas de voz en redes móviles constituye uno de los principales desafíos actuales para el sector de las telecomunicaciones en Colombia. No obstante, su análisis y abordaje regulatorio exige partir de una comprensión integral del ecosistema, evitando soluciones parciales que, aunque técnicamente viables, pueden generar efectos adversos sobre la competencia, la innovación y los derechos de los usuarios. En particular, las propuestas orientadas a concentrar el control del tráfico de voz en los operadores móviles, especialmente respecto de llamadas internacionales que ingresan por rutas de larga distancia, deben evaluarse con especial cautela, en la medida en que no atacan la causa estructural del problema y pueden derivar en una exclusión injustificada de actores legítimos del mercado.

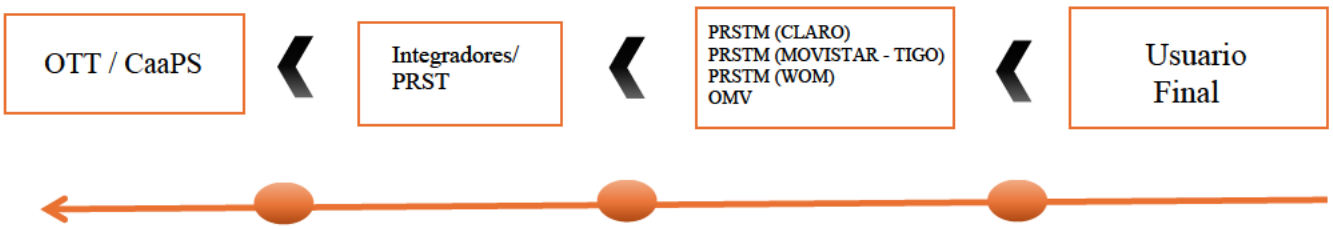
El fraude en servicios de voz no es un fenómeno aislado ni atribuible a un único segmento de la cadena de valor. Su origen se encuentra en fallas históricas en la administración y control de la numeración móvil, derivadas de la comercialización masiva de SIM Cards sin esquemas robustos de identificación y trazabilidad del titular real. Esta situación permitió que la numeración móvil, recurso escaso administrado por el Estado, fuera utilizada de manera indebida por estructuras criminales, generando un problema que necesariamente se materializa en la terminación de llamadas en redes móviles. En este contexto, las respuestas regulatorias deben orientarse a soluciones integrales, proporcionales y técnicamente neutrales, que partan del usuario final, preserven la diversidad de actores del ecosistema y fortalezcan la confianza en el servicio de voz.

En el servicio de llamadas de voz, los operadores pueden gestionar tanto tráfico originado por acuerdos directos con clientes nacionales (por ejemplo, bancos, comercios, entidades de salud, aerolíneas), como tráfico internacional que llega a través de cadenas de intermediarios, donde el originador de la llamada no siempre es certificado o plenamente identificable. ¿Qué diferencias, riesgos y oportunidades observa entre estos dos tipos de tráfico en relación con la prevención y mitigación del fraude? ¿Qué criterios, mecanismos o medidas considera relevantes para gestionar de manera diferenciada el tráfico directo y el tráfico en cadena, especialmente en lo relacionado con la trazabilidad, autenticación, control de llamadas sospechosas y judicialización?

En el servicio de llamadas de voz, el tráfico originado mediante acuerdos directos con clientes nacionales presenta condiciones estructuralmente distintas frente al tráfico internacional que ingresa a través de cadenas de intermediarios. En el primer caso, existe una relación contractual directa entre el originador de la llamada y el proveedor del servicio, lo que permite niveles significativamente más altos de trazabilidad, identificación del responsable, verificación del uso autorizado de la numeración y exigibilidad jurídica. Este tipo de tráfico facilita la implementación de controles ex ante, auditorías periódicas, cláusulas contractuales de responsabilidad, así como la adopción de medidas correctivas graduales sin afectar de manera indiscriminada el servicio. Además, al tratarse de actores plenamente identificables y sometidos al ordenamiento jurídico colombiano, se habilitan mecanismos reales de judicialización en caso de uso indebido del servicio de voz.

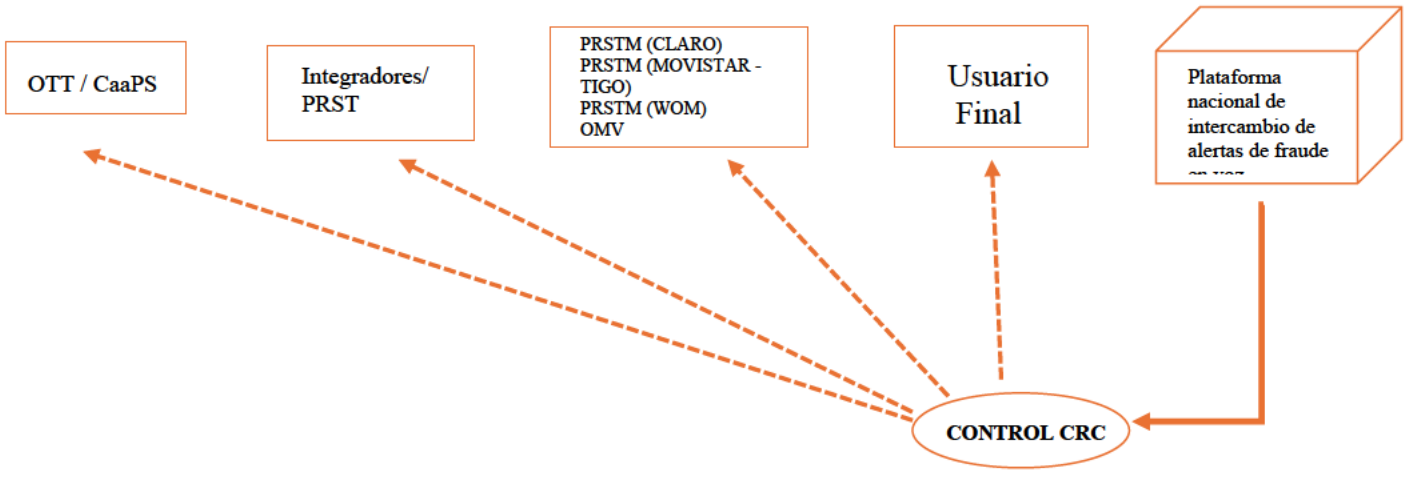


Por el contrario, el tráfico internacional en cadena presenta retos adicionales derivados de la fragmentación del origen de la llamada, la multiplicidad de intermediarios técnicos y comerciales, y la diversidad de jurisdicciones involucradas. No obstante, esta mayor complejidad no puede equipararse automáticamente a una presunción de fraude. El tráfico en cadena cumple un rol esencial en la conectividad global, en la prestación de servicios legítimos de voz transfronteriza y en la integración de Colombia al ecosistema internacional de telecomunicaciones. Por ello, el riesgo regulatorio no radica en la existencia de este tipo de tráfico, sino en la ausencia de deberes claros y proporcionales de trazabilidad progresiva a lo largo de la cadena.



Desde esta perspectiva, la gestión diferenciada del riesgo debe enfocarse en exigir que cada eslabón de la cadena, y no únicamente el operador móvil que termina la llamada, asuma obligaciones mínimas de identificación del cliente inmediato, conservación de registros técnicos y cooperación ante alertas verificadas. Pretender trasladar toda la carga de control al operador móvil, bajo el argumento de que es quien tiene visibilidad completa del tráfico, desconoce que la información crítica sobre el origen real de la llamada se pierde aguas arriba y que la terminación en red móvil es solo el último punto de materialización del riesgo, no su causa.

Asimismo, una regulación que trate de manera homogénea el tráfico directo nacional y el tráfico internacional en cadena introduce un riesgo elevado de exclusión de actores legítimos, como OTT, CaaPS y operadores de tránsito, que operan conforme a modelos de negocio válidos, generan empleo y aportan al desarrollo económico del país. Este enfoque no solo resulta desproporcionado, sino que favorece una concentración indebida del control del tráfico de voz en un número reducido de operadores móviles, con efectos potenciales sobre la libre competencia, la innovación y la evolución del sector.



En consecuencia, la oportunidad regulatoria no se encuentra en bloquear rutas, centralizar el control o restringir el acceso al mercado de servicios de voz internacionales, sino en diseñar un esquema de gestión del riesgo basado en

trazabilidad incremental, responsabilidades distribuidas y validación posterior a la terminación de la llamada, donde el reporte del usuario final tenga un rol central. Este enfoque reconoce que la naturaleza fraudulenta de una llamada solo puede confirmarse una vez culminada la comunicación y reportada como tal, y que cualquier medida preventiva debe ser técnica, jurídicamente viable y respetuosa de los derechos de los usuarios y de los actores legítimos del ecosistema.

¿Qué mecanismos, herramientas o procedimientos tiene actualmente implementados su organización para detectar, prevenir y controlar el spoofing en llamadas de voz? ¿Qué nivel de efectividad han observado en estas medidas y qué retos técnicos y operativos han enfrentado en su aplicación?

En el ecosistema de servicios de voz, los mecanismos actualmente implementados para la detección, prevención y control del spoofing se concentran principalmente en análisis estadístico y comportamental del tráfico, tales como la identificación de patrones atípicos de oxigenación, picos inusuales de volumen, recurrencia de llamadas en ventanas de tiempo reducidas, duraciones anómalas o coincidencias entre rangos de numeración y destinos específicos. A estos mecanismos se suman listas internas de números previamente reportados, reglas heurísticas y modelos de detección basados en umbrales, los cuales son aplicados mayoritariamente por los operadores móviles en el punto de terminación de la llamada.

No obstante, la efectividad de estas herramientas es estructuralmente limitada. El spoofing en llamadas de voz se sustenta, precisamente, en la capacidad de rotar de manera constante la identidad del número llamante (CLI), lo cual fue posible gracias a una asignación histórica masiva e indiscriminada de SIM Cards y numeración móvil, sin esquemas robustos de identificación del titular real ni mecanismos efectivos de trazabilidad. En este contexto, los sistemas de detección basados en listas negras o reincidencia pierden eficacia, dado que los actores fraudulentos pueden cambiar rápidamente de número, reutilizar rangos distintos o simular identidades legítimas, sin que ello implique un costo operativo significativo para ellos.

Desde el punto de vista técnico y jurídico, existe además una limitación insalvable, ningún actor del ecosistema (ni operadores, ni intermediarios, ni plataformas tecnológicas) puede determinar de manera objetiva si una llamada es fraudulenta antes de su terminación. El contenido de la comunicación no puede ser interceptado, grabado ni analizado, en tanto ello vulneraría derechos fundamentales como la privacidad. En consecuencia, cualquier mecanismo que pretenda calificar una llamada como fraudulenta en tiempo real solo puede basarse en indicios indirectos, lo que incrementa significativamente el riesgo de falsos positivos y afectaciones al tráfico legítimo.

En la práctica, esto implica que los mecanismos actuales operan de manera reactiva, apoyándose en el reporte posterior del usuario final como principal insumo para confirmar la naturaleza fraudulenta de una llamada. El usuario es,

en efecto, el primer y único actor que puede identificar el engaño, dado que el fraude se configura a partir de información parcialmente real cómo, el nombre, tipo de producto producto, entidad, saldo, obligaciones existentes, entre otras, que induce al error. Esta realidad demuestra que las soluciones centradas exclusivamente en filtros técnicos ex ante no solo son insuficientes, sino conceptualmente equivocadas, pues desconocen la forma en que se materializa el fraude en servicios de voz.

Adicionalmente, los retos operativos se agravan cuando las llamadas fraudulentas ingresan por rutas internacionales o cadenas de intermediarios, donde la información sobre el originador real se diluye progresivamente. En estos escenarios, los operadores que terminan la llamada no cuentan con herramientas efectivas para verificar la autenticidad del CLI ni para reconstruir, en tiempo real, la cadena de responsabilidades. Pretender que el operador móvil asuma un rol absoluto de control en este punto equivale a trasladarle una obligación imposible de cumplir de manera plena, al tiempo que se invisibiliza la responsabilidad estructural asociada a la administración inicial de la numeración.

En este contexto, los mecanismos actuales de detección y control del spoofing solo pueden considerarse instrumentos complementarios, útiles para mitigar impactos puntuales, pero incapaces de resolver el problema de fondo. Su efectividad depende necesariamente de que se acompañen de una política estructural orientada a la identificación efectiva del titular de la numeración, al fortalecimiento de los mecanismos de reporte ciudadano, a la trazabilidad progresiva de las llamadas y a esquemas de control que distribuyan responsabilidades a lo largo de toda la cadena de valor del servicio de voz. Sin estos elementos, cualquier esfuerzo técnico continuará siendo fragmentario, reactivo y, en última instancia, insuficiente para enfrentar de manera sostenible el fenómeno del spoofing en Colombia.

¿Qué efectos positivos y negativos prevé en la prohibición de llamadas internacionales con identidad de línea llamante CLI nacional? ¿Qué excepciones o consideraciones deberían contemplarse para no afectar la prestación de servicios legítimos?

La prohibición de llamadas internacionales que presenten un identificador de línea llamante (CLI) nacional puede generar, en apariencia, un impacto positivo inmediato en la reducción de ciertos esquemas de suplantación, particularmente aquellos en los que actores fraudulentos simulan ser entidades locales, cómo bancos, operadores, entidades públicas o empresas de servicios, para inducir al error al usuario final. Desde una lógica estrictamente reactiva, esta medida permitiría bloquear una tipología específica de fraude asociada al spoofing internacional con numeración nacional.

Sin embargo, una evaluación más profunda evidencia que esta prohibición conlleva riesgos estructurales significativos y puede producir efectos adversos desproporcionados sobre el ecosistema de comunicaciones de voz en

Colombia. En primer lugar, una restricción absoluta desconoce la realidad operativa del mercado global de telecomunicaciones, en el que múltiples servicios legítimos utilizan infraestructuras internacionales para originar llamadas que, por razones técnicas, contractuales o de continuidad del negocio, presentan un CLI nacional. Este es el caso de empresas multinacionales con centros de atención ubicados en el exterior, plataformas de servicios compartidos, contact centers internacionales, soluciones de continuidad operativa, servicios corporativos de roaming inverso y plataformas tecnológicas que prestan servicios a usuarios colombianos desde otras jurisdicciones.

La prohibición generalizada de este tipo de llamadas podría traducirse, en la práctica, en una barrera artificial a la prestación transfronteriza de servicios, afectando no solo a empresas legalmente constituidas, sino también a los propios usuarios finales, quienes podrían dejar de recibir comunicaciones legítimas relacionadas con servicios financieros, de salud, logísticos o de soporte técnico. Desde una perspectiva regulatoria, esta medida resulta problemática en tanto vulnera principios como la neutralidad tecnológica, la proporcionalidad y la promoción de la competencia, al imponer una restricción que no distingue entre tráfico legítimo y tráfico fraudulento.

Adicionalmente, esta prohibición podría generar un efecto de concentración del mercado, al fortalecer la posición de los operadores móviles que terminan las llamadas, quienes pasarían a controlar de manera casi exclusiva el acceso del tráfico internacional hacia usuarios móviles en Colombia. Tal escenario es particularmente delicado en un contexto en el que el país cuenta con un número reducido de PRSTM, lo cual incrementa el riesgo de prácticas restrictivas, control de precios y limitación de la innovación. En lugar de mitigar el fraude, la medida podría terminar consolidando un modelo en el que quienes históricamente contribuyeron al desorden inicial, mediante la asignación masiva y poco controlada de SIM Cards, se posicionan como los únicos “guardianes” del sistema.

Desde el punto de vista técnico, la prohibición tampoco resuelve el problema de fondo. Los actores fraudulentos pueden adaptar rápidamente sus esquemas, migrando a CLI internacionales, rotando numeración o utilizando técnicas alternativas de ocultamiento de identidad. En este sentido, la medida actúa únicamente sobre una manifestación del fraude, pero no sobre su causa estructural, que radica en la falta de identificación efectiva del originador real de la llamada y en la ausencia de mecanismos robustos de trazabilidad a lo largo de toda la cadena de valor.

Por ello, cualquier restricción al uso de CLI nacional en llamadas internacionales debe ser selectiva, condicionada y basada en criterios objetivos de verificación, y no una prohibición absoluta. Resulta indispensable contemplar excepciones claras para tráfico legítimo, soportadas en esquemas de registro del originador, acuerdos de confianza entre operadores, mecanismos de autenticación progresiva y procesos de validación ex post que permitan identificar responsabilidades en caso de abuso. Estas excepciones no solo protegen la

continuidad de servicios legítimos, sino que también preservan la apertura del mercado y la integración de Colombia en el ecosistema global de telecomunicaciones.

¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema que permita el enmascaramiento de la identidad de la línea llamante CLI en llamadas internacionales, siempre que estas sean etiquetadas en el dispositivo del usuario como "No verificada" o "Probable fraude"? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la prevención del fraude, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

La implementación de un esquema que permita el enmascaramiento de la identidad de la línea llamante (CLI) en llamadas internacionales, acompañado de un etiquetado informativo visible en el dispositivo del usuario final, constituye una alternativa regulatoria más equilibrada, proporcional y compatible con la realidad técnica del servicio de voz que las propuestas de bloqueo o prohibición absoluta. Este enfoque reconoce una premisa fundamental, en los servicios de voz no es posible determinar con certeza la naturaleza fraudulenta de una llamada antes de su terminación, y, por tanto, cualquier solución efectiva debe necesariamente involucrar al usuario final como actor central del proceso de mitigación del riesgo.

A diferencia de las medidas de filtrado ex ante, el etiquetado informativo no interrumpe ni censura la comunicación, sino que introduce un elemento de transparencia contextual que permite al usuario tomar una decisión informada. Al identificar una llamada como "No verificada" o "Probable fraude", el sistema no afirma categóricamente que se trate de un acto ilícito, sino que comunica una condición objetiva, y es la imposibilidad técnica o contractual de autenticar plenamente el origen de la llamada dentro de la cadena internacional de tráfico.

Desde la perspectiva de protección al usuario, este esquema resulta especialmente valioso, pues reduce la asimetría de información que actualmente existe entre quien origina la llamada y quien la recibe. Hoy, el usuario final se enfrenta a un identificador de llamada que aparenta legitimidad (frecuentemente con numeración nacional) sin contar con elementos que le permitan discernir si esa identidad es real o suplantada. El etiquetado introduce una señal de advertencia que refuerza la prevención sin imponer una carga excesiva sobre el sistema ni sobre los actores intermedios.

No obstante, la eficacia de esta medida depende críticamente de evitar etiquetados excesivamente agresivos o indiscriminados. Un etiquetado mal diseñado puede generar efectos contraproducentes, tales como la desconfianza generalizada en el servicio de voz, la estigmatización de tráfico legítimo internacional o la exclusión indirecta de actores como OTT, CAPS, operadores de tránsito y proveedores de servicios corporativos que operan de manera lícita. Por ello, el etiquetado debe sustentarse en criterios objetivos, trazables y

verificables, tales como la ausencia de información suficiente sobre el originador en la cadena de interconexión, la falta de registro previo del número o la imposibilidad técnica de validar el CLI, y no en presunciones automáticas de fraude.

Desde el punto de vista técnico, la implementación de este esquema exige interoperabilidad entre redes, estandarización de señales y coordinación entre operadores móviles, operadores internacionales y plataformas tecnológicas. Es indispensable que la Comisión defina lineamientos claros sobre los estándares mínimos de señalización, presentación del etiquetado en los dispositivos y responsabilidades de cada actor en la cadena. Asimismo, debe garantizarse que el etiquetado sea consistente entre redes, evitando escenarios en los que una misma llamada sea presentada de manera distinta según el operador de destino, lo cual generaría confusión y fragmentación de la experiencia del usuario.

En términos de experiencia de usuario, el etiquetado debe ser claro, comprensible y no alarmista. Mensajes como “No verificada” o “Origen no autenticado” resultan más adecuados que calificaciones categóricas, en la medida en que informan sin inducir pánico o rechazo automático. Este enfoque se alinea con experiencias internacionales exitosas y con el funcionamiento de herramientas ampliamente aceptadas por los usuarios, como las aplicaciones de identificación de llamadas, que no bloquean el tráfico, sino que ofrecen contexto adicional para la toma de decisiones.

Este esquema permite avanzar hacia un modelo de control distribuido, en el que la mitigación del fraude no recae exclusivamente en los operadores móviles que terminan la llamada, sino que se apoya en una combinación de transparencia, pedagogía, reporte ciudadano y trazabilidad progresiva. De esta forma, el enmascaramiento del CLI con etiquetado informativo se consolida como una herramienta que protege al usuario sin sacrificar la apertura del mercado, preserva la evolución de las telecomunicaciones en Colombia y evita que, bajo el pretexto de la seguridad, se impongan soluciones que concentren poder y restrinjan derechos.

¿Qué oportunidades y retos identifica en la adopción de protocolos de autenticación comoSTIR/SHAKEN/RCD? ¿Qué condiciones técnicas y regulatorias serían necesarias para su implementación efectiva? ¿Considera que, con la implementación de este protocolo de autenticación, no resulta necesaria la implementación de medidas de filtrado de tráfico o listas de no originación (DNO)?

Los protocolos de autenticación de identidad de llamadas como STIR/SHAKEN y RCD representan, en términos conceptuales, un avance relevante en la mitigación del spoofing en servicios de voz, en la medida en que buscan garantizar la integridad del identificador de la línea llamante (CLI) mediante mecanismos criptográficos y de señalización estandarizada. Su principal aporte consiste en permitir que el operador que origina la llamada certifique, con

distintos niveles de confianza, que el número presentado corresponde efectivamente al usuario o entidad autorizada para utilizarlo.

No obstante, la adopción de estos protocolos en el contexto colombiano enfrenta limitaciones estructurales que impiden considerarlos como una solución integral o autosuficiente frente al fenómeno del fraude en llamadas de voz. En primer lugar, la efectividad de STIR/SHAKEN depende de un supuesto que no siempre se cumple en la práctica, la existencia de una identificación previa, verificable y confiable del originador de la llamada. En escenarios donde la numeración fue asignada de manera masiva, sin controles robustos de identidad, o donde el tráfico se origina a través de cadenas internacionales con múltiples intermediarios, la capacidad de certificar el origen real de la llamada se ve seriamente comprometida.

Desde una perspectiva técnica, estos protocolos funcionan de manera óptima en entornos relativamente cerrados o con alto grado de madurez institucional, donde los operadores comparten estándares homogéneos, existe interoperabilidad plena y la cadena de interconexión es corta y transparente. Sin embargo, el ecosistema colombiano de voz se caracteriza por una alta fragmentación, con la coexistencia de PRSTM, operadores de tránsito, OTT, CAPS y plataformas tecnológicas internacionales, lo que dificulta la implementación uniforme de STIR/SHAKEN y reduce significativamente su alcance en el tráfico que ingresa por rutas internacionales o esquemas indirectos.

Adicionalmente, la implementación de estos protocolos implica costos económicos y operativos relevantes, tanto para los operadores móviles como para otros actores del sector. La adecuación de redes, la actualización de sistemas de señalización, la gestión de certificados digitales y la operación continua del esquema de autenticación pueden resultar desproporcionadas para actores más pequeños, lo que podría generar barreras de entrada o exclusión indirecta, contrarias a los principios de libre competencia y neutralidad tecnológica que deben orientar la regulación del sector.

Desde el punto de vista regulatorio, resulta igualmente problemático asumir que la adopción de STIR/SHAKEN elimina la necesidad de otras medidas de mitigación del fraude. Estos protocolos no previenen el fraude en sí mismo, sino que autentican la integridad del CLI; es decir, certifican que el número no fue alterado durante la transmisión, pero no garantizan que el titular del número no esté incurriendo en conductas fraudulentas. En consecuencia, incluso llamadas plenamente autenticadas pueden ser utilizadas para cometer estafas, especialmente cuando el fraude se basa en el uso de información parcialmente real y en técnicas de ingeniería social.

Por esta razón, no es adecuado plantear que la implementación de STIR/SHAKEN haga innecesarias medidas complementarias como los esquemas de reporte del usuario, las listas de no oxigenación (DNO) o los mecanismos de etiquetado informativo. El usuario final continúa siendo el único

actor capaz de identificar el engaño en el momento en que se materializa, y su reporte sigue siendo un insumo esencial para activar procesos correctivos, administrativos y, eventualmente, judiciales.

En este sentido, los protocolos de autenticación deben ser entendidos como herramientas habilitantes, que aportan información adicional al ecosistema, pero que requieren integrarse dentro de un modelo de control distribuido, donde la mitigación del fraude no recaiga exclusivamente en una capa tecnológica ni en un solo actor del mercado. Su implementación debe ser progresiva, flexible y compatible con otros mecanismos ya existentes, evitando enfoques maximalistas que pretendan resolver un problema estructural mediante una única solución técnica.

¿Qué parámetros y tecnologías considera más adecuados para estandarizar los modelos de monitoreo y filtrado de tráfico de voz? ¿Cómo garantizar que no se generen falsos positivos (que terminen afectando el tráfico legítimo), así como la protección de la privacidad de las comunicaciones y la proporcionalidad de las medidas?

Los modelos de monitoreo y filtrado de tráfico de voz destinados a mitigar el fraude deben construirse necesariamente sobre parámetros técnicos objetivos, observables y no intrusivos, que respeten los límites constitucionales y legales del servicio de telecomunicaciones. En el caso específico de las llamadas de voz, cualquier esquema regulatorio debe partir de una premisa ineludible, cómo el contenido de la comunicación no puede ser inspeccionado, grabado ni analizado, pues ello vulneraría el derecho fundamental a la privacidad de los usuarios. En consecuencia, los modelos de detección solo pueden operar sobre metadatos y comportamientos de red, nunca sobre la conversación en sí misma.

En este contexto, los parámetros más adecuados para el monitoreo del tráfico de voz son aquellos asociados a patrones de comportamiento anómalos, tales como volúmenes inusuales de llamadas en periodos cortos, intentos repetitivos hacia múltiples destinos, duraciones atípicas, ratios elevados de llamadas no contestadas, correlaciones entre rangos de numeración y destinos específicos, o cambios abruptos en la geolocalización lógica del tráfico. Estos indicadores, analizados de manera conjunta y contextual, pueden servir como señales de alerta temprana, pero no constituyen prueba suficiente de fraude por sí mismos.

Precisamente por esta razón, el filtrado automático y definitivo del tráfico basado únicamente en modelos algorítmicos representa un riesgo significativo de falsos positivos, con impactos directos sobre comunicaciones legítimas. El bloqueo indebido de llamadas afecta no solo la prestación del servicio, sino también derechos fundamentales como el acceso a la información, la libertad de empresa y la confianza de los usuarios en el canal de voz. En un entorno donde empresas, entidades de salud, instituciones financieras y usuarios dependen de la telefonía para comunicaciones críticas, un error de filtrado puede tener consecuencias graves y desproporcionadas.

Desde la perspectiva del principio de proporcionalidad, cualquier medida de filtrado debe cumplir tres condiciones esenciales: idoneidad, necesidad y proporcionalidad en sentido estricto. Esto implica que el filtrado no puede ser la primera ni la única respuesta frente a una alerta, sino una medida gradual, sujeta a verificación posterior. Las señales de riesgo deben activar procesos de análisis adicionales, contrastarse con información histórica, cruzarse con reportes de usuarios y, en caso de duda razonable, permitir la continuidad del tráfico mientras se adelantan las verificaciones correspondientes.

Asimismo, resulta indispensable que los esquemas de monitoreo y filtrado incorporen mecanismos claros de reclamación y corrección, tanto para los usuarios finales como para los actores del sector afectados por bloqueos o marcaciones indebidas. La existencia de canales ágiles para impugnar decisiones automáticas, solicitar revisiones técnicas y obtener restablecimientos oportunos del servicio no solo protege derechos, sino que fortalece la legitimidad del sistema y la confianza en las medidas regulatorias adoptadas.

En términos de gobernanza, el monitoreo del tráfico de voz no puede quedar sujeto a decisiones opacas o discrecionales de un número reducido de operadores. Es fundamental que la Comisión establezca estándares mínimos comunes, criterios transparentes y obligaciones de trazabilidad sobre las decisiones de filtrado, de manera que estas puedan ser auditadas posteriormente. La auditoría regulatoria cumple un rol clave para evitar abusos, prácticas discriminatorias o el uso del filtrado como herramienta de control del mercado bajo el pretexto de la lucha contra el fraude.

La protección de la privacidad debe ser un eje transversal de cualquier modelo de monitoreo. Esto implica limitar estrictamente el tratamiento de datos al mínimo necesario, garantizar la anonimización cuando sea posible, definir tiempos claros de retención de información y asegurar que los datos recolectados no sean reutilizados con fines distintos a la prevención del fraude. Cualquier desviación de estos principios no solo sería ilegal, sino que erosionaría la confianza de los usuarios y expondría al sistema a riesgos jurídicos significativos.

¿Qué actores deberían participar en una plataforma nacional de intercambio de alertas sobre fraudes en llamadas? ¿Qué mecanismos de gobernanza y protección de datos serían necesarios?

Una plataforma nacional de intercambio de alertas sobre fraudes en llamadas de voz debe estructurarse bajo un modelo de participación amplia, plural y equilibrada, que refleje la realidad del ecosistema de telecomunicaciones y evite trasladar el control del sistema a un número reducido de operadores móviles. En este sentido, los actores que deben participar no pueden limitarse exclusivamente a los PRSTM, sino que deben incluir a usuarios finales, operadores móviles, operadores de tránsito, PSRT, OTT, CaaPS, integradores

tecnológicos, y autoridades competentes, con roles claramente diferenciados y complementarios.

El usuario final debe ser reconocido como un actor central del sistema, en tanto es el primer eslabón capaz de identificar con certeza la materialización del fraude. Su participación se materializa a través de mecanismos sencillos, accesibles y estandarizados de reporte, que alimenten la plataforma con alertas cualificadas. Excluir al usuario o relegarlo a un rol pasivo desconoce la naturaleza misma del fraude en servicios de voz, que solo se evidencia durante la interacción directa.

Los operadores móviles (PRSTM) y los operadores de tránsito cumplen un rol técnico relevante en la aportación de información de enrutamiento, terminación y patrones de tráfico asociados a las alertas reportadas, pero no deben ostentar control exclusivo ni decisorio sobre la validación o las consecuencias de dichas alertas. Su función debe estar delimitada a la colaboración técnica y a la ejecución de medidas proporcionales definidas bajo estándares regulatorios claros.

Los OTT, CaaPS e integradores tecnológicos deben participar activamente, en tanto forman parte real y legítima de la cadena de valor del tráfico de voz, especialmente en escenarios internacionales o híbridos. Su exclusión no solo debilitaría la trazabilidad del sistema, sino que reforzaría una visión fragmentada y sesgada del problema, además de afectar actores que generan empleo, innovación y competitividad en el país.

En cuanto a la administración, la plataforma debe operar bajo un esquema liderado y supervisado por la Comisión, como autoridad técnica e independiente, pero con reglas claras que impidan la captura regulatoria o el uso estratégico de la información por parte de actores dominantes. La Comisión debe definir los estándares mínimos de operación, criterios de validación de alertas, niveles de acceso a la información, responsabilidades de cada actor y mecanismos de auditoría periódica, garantizando transparencia, trazabilidad y rendición de cuentas.

Es fundamental que la gobernanza incorpore un modelo de decisiones no automatizado ni discrecional, en el que las alertas no se traduzcan automáticamente en bloqueos, listas de no oxigenación (DNO) o sanciones, sino que activen procesos graduales de análisis, contraste y verificación. Este enfoque protege el debido proceso, reduce el riesgo de falsos positivos y evita que la plataforma se convierta en un instrumento de exclusión o control del mercado.

En materia de protección de datos, la plataforma debe regirse estrictamente por los principios de minimización, finalidad, proporcionalidad y seguridad de la información. La información compartida debe limitarse a los datos estrictamente necesarios para la mitigación del fraude, evitando el tratamiento del contenido de las comunicaciones y privilegiando el uso de metadatos anonimizados o

seudonimizados cuando sea posible. Asimismo, deben establecerse políticas claras de retención de datos, con plazos definidos y mecanismos de eliminación segura, así como controles de acceso diferenciados según el rol de cada actor.

Adicionalmente, resulta indispensable implementar mecanismos de auditoría técnica y jurídica, que permitan verificar el uso adecuado de la información, detectar posibles abusos y garantizar que las alertas no sean utilizadas con fines distintos a la prevención del fraude, como prácticas anticompetitivas o estrategias de bloqueo selectivo. La confianza en la plataforma dependerá, en gran medida, de la existencia de estas salvaguardas y de la percepción de imparcialidad en su operación.

¿Cuáles considera que serían los retos técnicos y económicos de construir y operar la plataforma de alertas bajo un modelo centralizado vs un modelo distribuido? ¿Qué mecanismos considera deben ser adoptados y estandarizados para validar la veracidad de una alerta antes de su distribución mediante la plataforma de intercambio?

La creación de una plataforma nacional de intercambio de alertas sobre fraude en llamadas de voz debe concebirse como un mecanismo estructural de coordinación sectorial, y no como una herramienta de control centralizado del tráfico. Su diseño debe partir de una premisa esencial que ha sido históricamente subestimada en las discusiones regulatorias: el usuario final es el primer y único actor que puede identificar con certeza cuándo una llamada es fraudulenta, dado que el fraude se materializa a través de la interacción directa y del uso de información parcialmente verdadera que solo se revela durante la conversación.

En este sentido, el insumo principal de la plataforma no debe ser exclusivamente el análisis técnico de tráfico, sino el reporte ciudadano, entendido como una señal cualificada que activa procesos de verificación, trazabilidad y eventual actuación administrativa o judicial. Esta aproximación resulta coherente con la experiencia previa de la Comisión en materia de SMS, donde los mecanismos de denuncia directa por parte de los usuarios permitieron identificar campañas fraudulentas, recuperar recursos de numeración y generar efectos disuasivos reales en el mercado.

Actores participantes y rol de cada uno

Una plataforma de estas características debe involucrar, de manera obligatoria y coordinada, a usuarios finales, PRSTM, operadores de tránsito, OTT, CaaPS, integradores tecnológicos y autoridades competentes, bajo un esquema de gobernanza claro liderado por la Comisión. Cada actor cumple un rol diferenciado y complementario, los usuarios reportan; los operadores y agregadores aportan información técnica de enrutamiento y terminación; los intermediarios internacionales contribuyen a la trazabilidad de la cadena; y las autoridades utilizan la información consolidada para la adopción de medidas regulatorias, sancionatorias o judiciales.

Excluir a alguno de estos actores (en especial a los OTT, CaaPS o proveedores de tránsito) no solo debilitaría la efectividad del sistema, sino que reforzaría un modelo concentrado en el que los operadores móviles que terminan la llamada monopolizan la narrativa, el control y la solución, a pesar de no ser los únicos intervinientes en la cadena ni los únicos responsables del problema estructural.

Modelo centralizado vs. modelo distribuido

Desde el punto de vista técnico y económico, un modelo centralizado de plataforma de alertas presenta riesgos significativos. Concentrar la recepción, validación y distribución de alertas en una única entidad o infraestructura puede derivar en cuellos de botella operativos, altos costos de implementación y mantenimiento, y riesgos de captura regulatoria o uso estratégico de la información. Además, un sistema centralizado puede convertirse, de facto, en un mecanismo de control indirecto del tráfico, con impactos sobre la competencia y la neutralidad del mercado.

Por el contrario, un modelo distribuido (basado en estándares comunes, interoperabilidad y responsabilidades compartidas) ofrece ventajas claras en términos de resiliencia, escalabilidad y neutralidad tecnológica. En este esquema, cada actor mantiene sus propios sistemas de recepción y gestión de alertas, pero comparte información relevante bajo reglas claras y homogéneas definidas por la Comisión. Este enfoque reduce la dependencia de un único punto de control, facilita la participación de actores de distinto tamaño y evita que la plataforma se convierta en una barrera de entrada o en un instrumento de exclusión.

Validación de alertas y prevención de bloqueos automáticos

Un elemento crítico del diseño de la plataforma es el mecanismo de validación de las alertas. Resulta indispensable evitar que una alerta aislada, no corroborada o maliciosa genere bloqueos automáticos, marcaciones definitivas o inclusión inmediata en listas de no originación (DNO). La validación debe basarse en criterios mínimos estandarizados, tales como la recurrencia del reporte, la coincidencia temporal, la consistencia con patrones previamente identificados y la correlación con información técnica de tráfico.

Este enfoque gradual permite equilibrar la protección del usuario con la preservación del tráfico legítimo y el respeto al debido proceso de los actores involucrados. Las alertas deben entenderse como señales de riesgo, no como pruebas concluyentes, y su función principal debe ser activar análisis adicionales, monitoreo reforzado y, cuando corresponda, actuaciones administrativas por parte de la Comisión.

Gobernanza, transparencia y protección de datos

La plataforma debe operar bajo un modelo de administración transparente, con reglas claras sobre acceso a la información, uso de los datos, responsabilidades y mecanismos de auditoría. Es fundamental garantizar que la información compartida se limite a lo estrictamente necesario para la mitigación del fraude, respetando principios de minimización de datos, anonimización cuando sea posible y tiempos de retención definidos.

Asimismo, la Comisión debe establecer mecanismos de supervisión y auditoría periódica que permitan evaluar el uso de la plataforma, prevenir abusos y asegurar que las alertas no sean utilizadas como herramientas de competencia desleal, bloqueo estratégico o discriminación de actores del mercado. La confianza en el sistema depende, en gran medida, de que todos los participantes perciban reglas claras, equitativas y aplicadas de manera uniforme.

Valor estratégico de la plataforma

Más allá de su función operativa, una plataforma nacional de alertas de fraude en voz constituye una herramienta estratégica de política pública, en tanto permite identificar tendencias, patrones emergentes y modalidades de fraude, alimentar procesos pedagógicos dirigidos a los usuarios y orientar decisiones regulatorias basadas en evidencia. Su valor no radica en el bloqueo inmediato, sino en la construcción progresiva de trazabilidad, responsabilidad y conocimiento colectivo del fenómeno.

¿Qué ventajas y desafíos observa en la creación de rangos exclusivos de numeración para
llamadas comerciales y publicitarias? ¿Considera que esta medida podría ser efectiva para
facilitar la identificación y denuncia de fraudes por parte de los usuarios?

La creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias puede aportar beneficios marginales en términos de identificación visual para el usuario, pero no constituye una solución estructural ni suficiente para la prevención del fraude en servicios de voz. Esta medida parte de una premisa limitada: que el fraude se origina principalmente desde llamadas etiquetadas como comerciales, cuando en la práctica los esquemas fraudulentos evolucionan constantemente y se adaptan rápidamente a cualquier restricción normativa, migrando hacia otros rangos de numeración, incluyendo numeración fija, móvil tradicional o incluso numeración internacional.

Uno de los principales riesgos de esta medida es que desplaza el problema en lugar de resolverlo. Los actores fraudulentos no dependen de un rango específico para operar; por el contrario, su comportamiento se caracteriza por la flexibilidad técnica y la explotación de asimetrías regulatorias. En consecuencia, la asignación de rangos exclusivos podría generar una falsa sensación de seguridad, tanto para los usuarios como para los reguladores,

mientras el fraude continúa manifestándose a través de otros esquemas de numeración menos vigilados.

Adicionalmente, la implementación de rangos exclusivos implica costos operativos y técnicos relevantes para todos los actores del ecosistema de voz. Los operadores y proveedores de servicios deberían adaptar sistemas de enrutamiento, facturación, monitoreo y señalización, así como actualizar bases de datos de numeración y plataformas de atención al usuario. Estos costos no son menores y podrían impactar de manera desproporcionada a actores pequeños o medianos, generando barreras de entrada y afectando la competencia, sin una correlación directa con una reducción efectiva del fraude.

Desde la perspectiva del usuario final, existe también el riesgo de confusión y fatiga informativa, especialmente si la medida no va acompañada de una estrategia sólida de pedagogía y comunicación. La simple existencia de un rango exclusivo no garantiza que el usuario comprenda su significado, sepa cómo actuar frente a una llamada sospechosa o distinga entre una llamada comercial legítima y una fraudulenta. Sin educación clara y sostenida, el etiquetado por rango puede perder rápidamente su efectividad y convertirse en un elemento irrelevante para la toma de decisiones del usuario.

Otro aspecto crítico es que esta medida no aborda el problema central de la trazabilidad y la responsabilidad en la cadena de oxigenación de la llamada. La numeración, por sí sola, no permite identificar con certeza al originador real del tráfico ni garantiza que el uso del número esté debidamente autorizado. En ausencia de controles adicionales sobre autenticación del origen, conservación de registros y cooperación entre actores, los rangos exclusivos pueden ser fácilmente explotados, suplantados o utilizados como fachada para actividades ilícitas.

Asimismo, existe el riesgo de que la creación de rangos exclusivos derive en prácticas de bloqueo preventivo o discriminatorio, especialmente si los operadores móviles deciden tratar todo el tráfico proveniente de dichos rangos como intrínsecamente riesgoso. Este enfoque no solo afectaría llamadas comerciales legítimas (incluidas aquellas relacionadas con servicios esenciales como salud, educación o servicios financieros), sino que también podría vulnerar principios de proporcionalidad, neutralidad y libre prestación de servicios.

En términos regulatorios, la efectividad de los rangos exclusivos depende de su articulación con otras medidas complementarias, como esquemas de reporte por parte del usuario, plataformas de intercambio de alertas, estándares mínimos de monitoreo de tráfico y responsabilidades claras a lo largo de la cadena de intermediación. Sin este enfoque integral, los rangos exclusivos corren el riesgo de convertirse en una solución aislada, reactiva y fácilmente evadible.

¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la transparencia en las comunicaciones, y qué desafíos técnicos, operativos o de experiencia
de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

La implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual, puede constituir una herramienta relevante para fortalecer la transparencia en las comunicaciones de voz y la protección del usuario, siempre que su diseño responda a criterios de proporcionalidad, neutralidad tecnológica y respeto por los modelos legítimos de prestación del servicio. Este tipo de medida no actúa como un mecanismo de bloqueo ni de restricción del tráfico, sino como un instrumento informativo que traslada capacidad de decisión al usuario final, permitiéndole evaluar si desea o no atender la llamada.

Desde la perspectiva del usuario, el principal valor del etiquetado radica en la reducción de la asimetría de información. Al recibir una llamada claramente identificada como “Comercial”, “Publicidad” o “Contacto empresarial”, el usuario puede contextualizar la comunicación antes de contestar, sin que ello implique una presunción automática de fraude. Este enfoque resulta especialmente relevante en el servicio de voz, donde la simple visualización del número no ofrece información suficiente para distinguir entre una llamada legítima y una potencialmente abusiva o engañosa.

No obstante, el reto central de este esquema consiste en definir criterios uniformes, verificables e interoperables para la aplicación del etiquetado. La efectividad del modelo depende de que todos los actores del ecosistema (operadores móviles, proveedores de servicios de voz, integradores tecnológicos y originadores de llamadas) apliquen el etiquetado bajo estándares mínimos comunes, evitando interpretaciones discrecionales o prácticas inconsistentes que puedan generar confusión en el usuario o distorsiones en el mercado.

En este sentido, el etiquetado no debe quedar sujeto exclusivamente a la autodeclaración del originador ni a decisiones unilaterales del operador que termina la llamada. Resulta necesario establecer mecanismos de validación progresiva, basados en relaciones contractuales, patrones de tráfico y reportes de usuarios, que permitan corregir usos indebidos del etiquetado sin recurrir a bloqueos generalizados ni sanciones automáticas. Este enfoque reduce el riesgo de falsos positivos y protege a actores legítimos que realizan comunicaciones comerciales lícitas, como entidades financieras, aseguradoras, empresas de servicios públicos o prestadores de salud.

Desde el punto de vista técnico, uno de los principales desafíos es garantizar que el etiquetado sea visible, comprensible y consistente en los distintos dispositivos y sistemas operativos, sin generar una experiencia de usuario alarmista o confusa. Etiquetas excesivamente agresivas, ambiguas o mal contextualizadas pueden provocar rechazo indiscriminado de llamadas legítimas, erosionar la confianza del usuario en el sistema y, paradójicamente, disminuir la efectividad del esquema como herramienta de protección.

Adicionalmente, el etiquetado obligatorio debe diseñarse de forma que no se convierta en un mecanismo encubierto de estigmatización del tráfico comercial, ni en una barrera indirecta a la libre prestación de servicios de voz. En particular, debe evitarse que el etiquetado sea utilizado como justificación para aplicar tratamientos degradados al tráfico, priorizaciones negativas o decisiones de bloqueo basadas únicamente en la categoría de la llamada, sin un análisis técnico individualizado.

En términos regulatorios, esta medida puede aportar valor si se integra dentro de un ecosistema más amplio de gestión del riesgo, que incluya educación al usuario, canales eficaces de denuncia, plataformas de intercambio de alertas y responsabilidades distribuidas a lo largo de la cadena de oxigenación de la llamada. El etiquetado, por sí solo, no previene el fraude, pero sí mejora la capacidad del usuario para identificar patrones sospechosos y reportarlos, fortaleciendo los mecanismos de detección ex post.

¿Qué beneficios y riesgos identifica en la creación de un registro nacional único de números DNO? ¿Qué criterios deberían regir su actualización y acceso?

La creación de un registro nacional único de números de no oxigenación (DNO) puede aportar, en principio, coherencia, estandarización y coordinación institucional en la gestión del fraude en llamadas de voz. Un esquema centralizado permitiría consolidar información sobre numeración reportada como fraudulenta y establecer un marco común de referencia para todos los operadores y actores del ecosistema. Sin embargo, su efectividad real no depende de la existencia formal del registro, sino de cómo se alimenta, cómo se gobierna y, especialmente, cómo se aplica en la práctica por quienes controlan la terminación de las llamadas.

Desde una perspectiva técnica y operativa, el principal riesgo del DNO nacional es que repita las limitaciones estructurales ya observadas en el Registro Nacional de Números Excluidos (RNE). En ambos casos, el éxito del sistema descansa en la actuación diligente de los operadores móviles, quienes son los únicos que tienen la capacidad efectiva de impedir que una llamada se origine o se complete. Si los operadores no integran el DNO de manera obligatoria, automática y verificable en sus sistemas de enrutamiento y control de tráfico, el registro se convierte en una herramienta meramente declarativa, sin impacto real en la experiencia del usuario.

Adicionalmente, un DNO nacional plantea retos significativos en términos de actualización, trazabilidad y temporalidad de los reportes. En el servicio de voz, los esquemas de fraude se caracterizan por la alta rotación de numeración, el uso intensivo de SIM cards y la rápida mutación de los patrones de oxigenación. En este contexto, un número puede ser utilizado de forma fraudulenta durante un período muy corto y, posteriormente, quedar inactivo o ser reasignado. Por ello, un DNO rígido, sin criterios claros de caducidad, revisión y depuración, puede generar bloqueos injustificados de tráfico legítimo, afectando derechos de usuarios finales y de terceros de buena fe.

En cuanto a los criterios de inclusión en el DNO, resulta fundamental que estos se basen en reportes verificables y graduales, y no únicamente en denuncias aisladas o automatizadas. Dado que en el servicio de voz no es posible determinar ex ante el contenido de la llamada ni calificarla como fraudulenta sin la intervención del usuario, el DNO debe construirse a partir de evidencia posterior a la terminación de la llamada, validada mediante patrones repetitivos, análisis técnico del tráfico y corroboración interoperatoria. De lo contrario, se corre el riesgo de convertir el DNO en un mecanismo de censura preventiva del tráfico.

Otro aspecto crítico es la administración del registro. Un DNO nacional requiere reglas claras sobre quién puede reportar, quién valida, quién decide la inclusión y exclusión de números, y bajo qué condiciones se pueden levantar las restricciones. En ausencia de procedimientos transparentes y garantistas, el registro puede convertirse en una herramienta discrecional que afecte la competencia, excluya actores legítimos del mercado o concentre aún más el control del tráfico en cabeza de unos pocos operadores dominantes.

Desde el punto de vista regulatorio, el DNO no debe concebirse como una solución autónoma ni excluyente, sino como un componente más dentro de un esquema de mitigación del fraude basado en responsabilidades distribuidas a lo largo de toda la cadena. El enfoque de “lista negra” resulta insuficiente si no se acompaña de medidas estructurales en la asignación, comercialización e identificación de la numeración, especialmente en la fase inicial de entrega de SIM cards y recursos de numeración a usuarios y empresas.

Asimismo, debe evitarse que el DNO nacional se utilice como un mecanismo para trasladar la carga del fraude hacia los actores intermedios o internacionales, ignorando que el problema se origina, en gran medida, en el descontrol histórico de la numeración móvil dentro del país. Un enfoque que solo actúa al final del flujo de la llamada (cuando está ya ha transitado por múltiples redes) resulta reactivo y limitado frente a la magnitud del fenómeno.

¿Qué ventajas, retos y posibles impactos identifica en la adopción de un esquema en el que cada PRST mantenga su propia lista de no originación (DNO), bajo un estándar mínimo obligatorio definido por la CRC? ¿De qué manera considera que esta medida podría contribuir a la protección contra el fraude y la suplantación en llamadas de voz, y qué desafíos técnicos, operativos

o de coordinación deberían ser tenidos en cuenta para asegurar su efectividad y coherencia en Colombia?

La adopción de un esquema en el que cada PRST administre su propia lista de números de no oxigenación (DNO), bajo un estándar mínimo obligatorio definido por la Comisión, puede ofrecer mayor flexibilidad operativa y capacidad de reacción inmediata frente a eventos de fraude en llamadas de voz. Este modelo reconoce que los PRST son quienes cuentan con el control técnico directo sobre la oxigenación, el enrutamiento y la terminación de las llamadas, y por tanto están en mejor posición para implementar medidas dinámicas y ajustadas a los patrones reales de tráfico que observan en sus redes.

Desde una perspectiva técnica, una DNO administrada por cada PRST permitiría respuestas más rápidas y contextualizadas, evitando los retrasos propios de esquemas centralizados que requieren validaciones múltiples antes de actuar. En un entorno de fraude de voz caracterizado por alta rotación de numeración, cambios constantes en rutas y uso intensivo de SIM cards, la capacidad de un operador para bloquear de manera ágil un número claramente abusivo puede reducir impactos inmediatos sobre los usuarios finales. Esta agilidad operativa constituye una de las principales ventajas del modelo descentralizado.

Sin embargo, este esquema también plantea riesgos significativos de fragmentación, discrecionalidad y asimetría regulatoria si no se encuentra estrictamente delimitado por reglas claras y mecanismos efectivos de supervisión. En ausencia de un estándar mínimo robusto y de lineamientos homogéneos, cada PRST podría aplicar criterios distintos para incluir o excluir numeración en sus listas DNO, lo que derivaría en tratamientos dispares del mismo número dependiendo del operador que curse o termine la llamada. Esta falta de coherencia puede generar inseguridad jurídica, afectar el tráfico legítimo y distorsionar la competencia en el mercado de voz.

Uno de los principales desafíos del modelo es evitar que las listas DNO por PRST se conviertan en herramientas de bloqueo preventivo excesivo, basadas en criterios internos poco transparentes o en presunciones no verificadas de fraude. Dado que en el servicio de voz no es posible calificar una llamada como fraudulenta antes de su terminación, la inclusión de un número en una DNO debería responder a patrones reiterados, reportes corroborados de usuarios y análisis técnico posterior, y no a eventos aislados o automatizados que puedan generar falsos positivos.

Desde el punto de vista regulatorio, la Comisión debería definir un estándar mínimo obligatorio que incluya, al menos: criterios objetivos de inclusión y exclusión de números, reglas de temporalidad y revisión periódica de las listas, mecanismos de trazabilidad de las decisiones adoptadas por cada PRST, y procedimientos claros para la atención de reclamaciones o solicitudes de levantamiento de bloqueos por parte de usuarios o terceros afectados. Sin estos elementos, el esquema descentralizado corre el riesgo de erosionar la confianza del ecosistema y de los usuarios finales.

Adicionalmente, la efectividad de las DNO por PRST depende de su articulación con un esquema nacional de reporte del usuario, que funcione como insumo común para todos los operadores. El usuario final es quien identifica en primera instancia la posible conducta fraudulenta, y su reporte debe constituir el punto de partida del análisis, sin que ello implique una inclusión automática del número en listas de no oxigenación. La falta de un canal unificado de reporte puede llevar a duplicidades, inconsistencias y pérdida de información relevante para la detección de patrones más amplios de fraude.

Otro riesgo relevante es que este modelo refuerce la concentración de poder de mercado en cabeza de los grandes operadores móviles, quienes cuentan con mayores capacidades técnicas y económicas para implementar sistemas avanzados de monitoreo y filtrado. Si no se establecen obligaciones de interoperabilidad y coordinación, los PRST dominantes podrían imponer de facto sus criterios al resto del ecosistema, afectando especialmente a actores más pequeños, integradores tecnológicos y proveedores legítimos de servicios de voz.

En términos de protección al usuario, las listas DNO por PRST solo resultarán eficaces si se aplican bajo un enfoque proporcional y transparente, evitando bloqueos silenciosos o decisiones opacas que el usuario no pueda comprender ni cuestionar. La CRC debería exigir mecanismos mínimos de rendición de cuentas, como reportes periódicos sobre la gestión de las DNO, estadísticas de números bloqueados, tiempos de permanencia y resultados en términos de reducción efectiva del fraude.

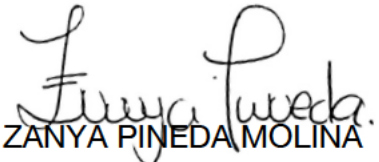
CONCLUSION

La mitigación del fraude en llamadas de voz requiere un enfoque regulatorio que vaya más allá del control técnico del tráfico y que aborde de manera estructural las causas que dieron origen a este fenómeno. Concentrar la gestión del riesgo exclusivamente en los operadores móviles, o atribuirles un rol exclusivo como filtro del tráfico nacional e internacional, no solo resulta insuficiente, sino que introduce riesgos significativos de concentración de mercado, afectación a la libre competencia y exclusión de actores legítimos que dinamizan el ecosistema de las telecomunicaciones en Colombia.

Una política pública eficaz debe partir del reconocimiento de que el usuario final es el primer y principal detector del fraude, y que la identificación de llamadas fraudulentas ocurre necesariamente después de la terminación de la comunicación. En consecuencia, las medidas regulatorias deben fortalecer la pedagogía, los mecanismos de reporte, la trazabilidad progresiva y la transparencia en la identificación de las llamadas, sin recurrir a bloqueos indiscriminados ni a esquemas que limiten la globalización de los servicios de voz. Solo a través de un enfoque integral, proporcional y centrado en el usuario será posible mitigar el fraude de manera efectiva, sin sacrificar la evolución, la

competitividad y la pluralidad del sector de las telecomunicaciones en Colombia.

Cordialmente



ZANYA PINEDA MOLINA
Abogada
[redacted]@gmail.com
Teléfono [redacted]