Observaciones sobre la propuesta regulatoria al proyecto de Identificación de Medidas para Mitigar el Fraude Cibernético por medio de servicios móviles.

Luis Alfonso Arias

Dirección Jurídica y de Regulación.

Inalambria Internacional SAS.

23 de junio de 2026.

Introducción.

Inalambria se permite presentar las siguientes observaciones al proyecto regulatorio de la referencia desde una convicción que ha guiado su operación: el fraude cibernético erosiona la confianza en el SMS como canal y constituye, por ello, una amenaza directa a la sostenibilidad misma del ecosistema del que hacemos parte.

Combatirlo no es para nosotros una obligación impuesta, sino un interés propio y permanente, en cuya defensa hemos invertido capacidades técnicas y humanas a lo largo de más de dos décadas en la prestación de servicios de mensajería A2P empresarial en el país.

Es precisamente ese conocimiento del negocio, de su operación técnica, de la heterogeneidad de los mensajes que cursa, de la dinámica de los actores legítimos y de los patrones reales mediante los cuales opera el fraude, el que nos lleva a compartir sin reservas el objetivo del proyecto y, al mismo tiempo, a advertir con responsabilidad sobre los efectos que algunas de las medidas propuestas podrían generar sobre servicios legítimos, sobre los derechos de los usuarios y sobre la participación de los pequeños y medianos agentes del ecosistema digital.

Si bien el objetivo del proyecto regulatorio, reducir el fraude cibernético y proteger a los usuarios, resulta legítimo y compatible con las funciones de la CRC, algunas de las medidas propuestas pueden generar efectos colaterales no deseados sobre servicios legítimos de comunicaciones móviles, sobre los derechos de los usuarios en general y sobre la participación de pequeños y medianos agentes económicos en el ecosistema digital y la economía en general.

Entendemos que el proyecto regulatorio no pretende eliminar el modelo de negocio de los IT; por el contrario, busca fortalecerlos, buscando la profesionalización del mercado y la reducción del fraude, penalizando aquellos agregadores informales o aquellos con controles débiles de fraude y conocimiento del cliente.

La presencia de externalidades no pecuniarias, que afectan la conducta de los agentes como asimetrías de información, el problema de acción colectiva relacionado con la existencia de incentivos no alineados entre los agentes del ecosistema y la pérdida de confianza en los sistemas de mensajería (SMS) como un “bien público”; efectivamente requiere de compensación institucional que faciliten la solución de problemas de coordinación complejos, mientras se observan principios de necesidad, proporcionalidad, eficiencia, libre competencia y promoción de la transformación digital consagrados en la Ley 1341 de 2009.

Las siguientes anotaciones se formulan, por tanto, con ánimo constructivo y técnico, no para controvertir el fin que perseguimos en común, sino para contribuir a que los medios escogidos resulten necesarios, proporcionales y efectivos, en línea con los principios consagrados en la Ley 1341 de 2009.

1. No todos los SMS constituyen un riesgo de fraude.

Problema identificado.

El proyecto parte de la premisa de que el canal SMS constituye como tal, un factor de riesgo para la materialización de fraudes cibernéticos.

Si bien lo anterior es cierto, como cualquier otro canal (email, chats OTT, entre otros), el universo de mensajes SMS es heterogéneo y comprende múltiples usos legítimos que en su mayoría no presentan características asociadas con el fraude.

En la práctica, la gran mayoría de mensajes de texto A2P que cursa nuestra plataforma se utilizan para:

- Notificaciones transaccionales.
- Confirmaciones de servicios.
- Alertas operativas.
- Códigos OTP.
- Avisos institucionales.

Por el contrario, y como ilustración, los mensajes identificados como fraude, que bloqueamos durante el mes de mayo de 2026 y que representaron cerca del 0.24% del total de los mensajes procesados en ese mes, comparten un elemento común: La inclusión de URLs o enlaces con invitaciones a acceder a sitios externos para acceder a información sensible.

Según nuestra experiencia, la materialización del fraude se facilita cuando la característica anterior está presente: URLs maliciosos.

Observación regulatoria.

Así como la propuesta diferencia el tratamiento de SMS P2P frente a SMS A2P, también podría diferenciar entre categorías de mensajes según su nivel de riesgo, siendo los que contienen URLs los que pueden representar un riesgo mayor.

No resulta proporcional someter a idénticos controles:

- Un SMS que simplemente informa una transacción bancaria.
- Un mensaje de alerta temprana emitido por una autoridad.
- Una notificación de confirmación o re-agendamiento de una cita médica.
- Un código OTP para autenticación.

La ausencia de una segmentación regulatoria puede generar restricciones innecesarias sobre comunicaciones de bajo riesgo y trasladar cargas de cumplimiento a mensajes que, por su naturaleza y contenido, no presentan características asociadas a esquemas de fraude.

De igual manera, el régimen de plantillas propuesto podría incorporar criterios de gestión de riesgo asociados tanto al contenido como al origen del mensaje. En particular, la obligación de registro, aprobación o validación previa de plantillas podría concentrarse en aquellos mensajes que incluyan exclusivamente elementos que históricamente han estado asociados a campañas de fraude, tales como:

- La originación de mensajes a través de mayoristas internacionales o empresas que facilitan la interconexión de Colombia con proveedores de servicios de internet globales debido a que la gran mayoría de actores maliciosos buscan "esconderse" detrás de cadenas internacionales largas de interconexión SMS, evitando su trazabilidad.
- La presencia de URLs o enlaces externos como se menciona anteriormente.

Mensajes cuyo contenido corresponda exclusivamente a comunicaciones transaccionales, operativas, informativas o de interés público podrían estar sujetos a un régimen simplificado o incluso exentos de controles asociados a plantillas.

Este enfoque permitiría focalizar los esfuerzos regulatorios sobre los segmentos de mayor riesgo (mensajes originados por agregadores internacionales y mensajes con URLs) reduciendo simultáneamente los costos de cumplimiento para los remitentes legítimos y disminuyendo los efectos no deseados sobre servicios esenciales y comunicaciones de interés general.

Para efectos ilustrativos, el segmento de negocio de mayoristas-internacionales de Inalambria representó en mayo del 2026 el 16.3% del volumen total de mensajes cursados. Si bien la gran mayoría de dichos mensajes son legítimos y de valor, es exclusivamente en este segmento donde se identificaron los dos casos de fraude que no lograron ser detectados por nuestros sistemas internos de prevención de fraude y que terminaron iniciando un proceso de control por parte de la CRC. De otro lado, el 100% del total de casos de fraude detectados y bloqueados por nuestros sistemas, que corresponden al 0.24% del volumen total de mensajes cursados en dicho mes,

contenían URLs peligrosas. Por esta razón hemos enfocado todos nuestros esfuerzos técnicos antifraude en la inspección profunda y análisis de mensajes con URLs utilizando una combinación de tecnología propietaria y modelos de inteligencia artificial recientes.

Utilizar el registro obligatorio de empresas que envían mensajes como la única dimensión para control de fraude es insuficiente e ineficaz. Otras dimensiones de control de fraude como el origen de los mensajes (sin son generados por clientes locales fácilmente identificables o clientes internacionales difícilmente rastreables) o las particularidades de sus contenidos (contienen características específicas propias de fraude) podrían alinearse con la propuesta que compartimos con Asobancaria, en donde resulta primordial contar con un compendio consolidado de las casuísticas más recurrentes que permitan analizar los principales patrones de fraude reportados.

Recomendación.

Implementar un esquema de gestión de riesgo basado en el contenido y origen de los mensajes. Contemplando eventualmente un régimen simplificado de validación, o incluso la exclusión de determinadas obligaciones asociadas al registro y aprobación previa de plantillas.

De esta manera, la regulación estaría alineada con un enfoque de supervisión basado en riesgo, concentrando los recursos de control sobre los tipos de mensajes que estadísticamente presentan una mayor probabilidad de utilización fraudulenta (los que contienen URLs y son originados por mayoristas internacionales), sin afectar innecesariamente comunicaciones legítimas que cumplen funciones económicas, sociales y de interés público.

2. Existen mensajes cuya entrega inmediata es crítica para la protección de derechos fundamentales.

Problema identificado.

El proyecto introduce mecanismos de validación y control que pueden generar retrasos operativos en el envío de mensajes afectando a usuarios financieros como a otros tipos de usuarios definidos por la Ley.

Sin embargo, en Colombia existen múltiples categorías de SMS cuya utilidad depende precisamente de su inmediatez. Por ejemplo:

En la gestión del riesgo de desastres:

- Alertas por inundaciones.
- Alertas por deslizamientos.
- Alertas meteorológicas.
- Sistemas de evacuación.

En el sistema financiero:

- Avisos de transacciones.
- Alertas de fraude.
- Confirmaciones de pagos.

En el sistema de salud:

- Re-agendamiento de citas médicas.
- Aprobación de procedimientos.
- Avisos de disponibilidad de medicamentos.
- Recordatorios de tratamientos.
- Campañas de vacunación.

En servicios públicos:

- Suspensiones del servicio programadas.
- Restablecimiento de servicios.
- Alertas de emergencia.

Observación regulatoria.

La imposición de controles previos, validaciones o procesos de aprobación podría afectar la oportunidad de mensajes cuyo retraso puede generar riesgos para la vida, riesgos para la salud, pérdidas económicas y afectaciones de servicios esenciales.

Recomendación.

Revisar la posibilidad de aplicar validaciones sólo para aquellos mensajes de texto que realmente puedan ser sujetos de fraude y que cumplan las características observadas previamente: Originación a partir de mayoristas internacionales y presencia de URLs.

3. El mecanismo de recuperación de códigos cortos y la estructura del sistema de sanciones al fraude planteados podría llevar en el corto plazo a la desaparición de un grupo importante de agentes del ecosistema: Los ITs.

Problema identificado.

En el esquema planteado para la suspensión del tráfico, el bloqueo de códigos cortos y terminación de los contratos con ITs por parte de los PRSTs, con conflicto de interés en tanto que los PRSTs actúan como ITs en competencia regulada con otros ITs, se generan incentivos perversos para conductas anti-mercado por parte de los PRSTs y que podrían devenir en la supresión de un importante agente en el ecosistema: Los ITs.

La desaparición de un eslabón de la cadena de valor como los IT / agregadores llevaría a una concentración del mercado de suministro de servicios mediante el uso de mensajes de texto, de un mercado de competencia a un duopolio y, como corolario, la consecuente pérdida de eficiencia del mercado. No debería existir un "trade off" entre eficiencia de mercado y eficacia institucional frente al control del fraude.

Observación regulatoria.

La regulación del mercado de mensajería de texto ha funcionado en términos de eficiencia, pero menos en términos de seguridad. Las ganancias de las reducciones del precio regulado han sido trasladadas a los clientes de los IT. El precio de SMS en Colombia es 10 veces inferior al de los países vecinos, sin embargo, la regulación propuesta podría ser discriminatoria para los IT, respecto de los PRSTs.

Recomendación.

El logro de los objetivos de seguridad y de eficacia, no necesariamente debe reñir con los logros de eficiencia del mercado SMS hoy día obtenidos gracias a la regulación del mercado por parte de la CRC en los últimos años y es importante incorporar la nueva realidad del negocio de las telecomunicaciones móviles en el país para evitar que el negocio de A2P termine en manos de un duopolio. El mecanismo de recuperación de códigos cortos debería ser usado como una medida de último recurso para situaciones de negligencia y en donde el IT o PCA no hayan podido justificar su incapacidad para detectar fraude y demostrar su capacidad de gestión en la prevención.

4. El proyecto privilegia la protección frente al fraude financiero, pero puede afectar otros derechos constitucionales.

Problema identificado.

La motivación principal del proyecto está asociada al fraude financiero y la protección patrimonial a sus usuarios, los consumidores financieros. Sin embargo, la regulación debe analizar integralmente todos los derechos involucrados.

Derechos potencialmente afectados:

- Derecho a la información: Artículo 20 de la Constitución.
- Derecho a la salud: Artículo 49 de la Constitución.
- Derecho a la vida e integridad personal: Artículos 11 y 12 de la Constitución.
- Acceso a servicios públicos de telecomunicaciones: Artículos 365 y siguientes de la Constitución.

Observación regulatoria.

La regulación parece concentrarse en la reducción del riesgo financiero sin valorar adecuadamente los costos regulatorios asociados a la restricción de comunicaciones legítimas para otros tipos de usuarios o consumidores declarados por la ley. La regulación parece construida principalmente para mitigar riesgos asociados al fraude financiero, pero sus efectos recaen sobre la totalidad de los usuarios del ecosistema de comunicaciones electrónicas, incluyendo sectores que no participan en las dinámicas que originan el problema regulatorio.

La protección contra el fraude no puede convertirse en una limitación desproporcionada de otros derechos fundamentales, relacionados con usuarios de servicios públicos domiciliarios, de servicios de salud, del sistema de seguridad social, de transporte y otros, que tienen la misma relevancia constitucional que los usuarios financieros.

Bajo tal panorama, la CRC tendría que justificar por qué el beneficio regulatorio supera los riesgos para otros derechos constitucionalmente protegidos.

Recomendación.

La CRC debería incorporar un análisis de proporcionalidad que evalúe los beneficios esperados, las afectaciones a otros derechos y mecanismos alternativos que resulten menos restrictivos.

5. El sistema de exclusión puede afectar la economía popular y la inclusión digital.

Problema identificado.

El proyecto contempla mecanismos que restringen o condicionan el acceso al canal SMS por parte de pequeñas y medianas empresas obligando el registro, asignación de códigos cortos y/o Sender ID para cualquier empresa o persona originadora de mensajes de texto.

Aunque la regulación propuesta por su complejidad podría ser viable cumplirla en grandes empresas, podría resultar excesivamente onerosa para pequeños y medianos actores económicos.

Hoy los mensajes de texto son usados por tenderos, ferreterías, carpinteros, talleres, comerciantes de barrio, microempresas, emprendedores, profesionales independientes, entre otros; para informar entregas, confirmar pedidos, avisar disponibilidad de productos, promocionar sus productos y servicios y muchas más aplicaciones de valor.

Observación regulatoria.

La regulación corre el riesgo de generar una barrera de entrada económica y administrativa para pequeños negocios que carecen de departamentos de cumplimiento, asesores jurídicos y recursos tecnológicos especializados; produciendo un efecto contrario a las políticas públicas de transformación e inclusión digital, fortalecimiento de MIPYMES y de desarrollo de la economía popular.

Recomendación

La CRC debería incorporar un régimen simplificado para pequeños remitentes, que contemple la posibilidad de:

- Compartir recursos de identificación, de tal manera que los integradores puedan agruparlos de manera controlada y responsable.
- Diseñar procedimientos abreviados con menores cargas documentales y validación simplificada.

Garantizando el acceso asequible al canal SMS.

6. La recuperación de códigos cortos no es un fenómeno exclusivo de los Integradores Tecnológicos.

Problema identificado.

El proyecto regulatorio parte de la necesidad de fortalecer los controles institucionales sobre los ITs asignatarios de códigos cortos A2P debido a la utilización indebida de estos recursos de numeración.

Sin embargo, la experiencia regulatoria demuestra que la recuperación de códigos cortos ha ocurrido respecto de distintos tipos de asignatarios del ecosistema de comunicaciones, incluyendo PRSTs. Como ilustración cabe mencionar la Resolución 8218 de 2026 donde, por denuncia de un banco, la CRC recupera el código corto 85377 asignado a Movistar. O la Resolución 8190 mediante la cual, por denuncia de un usuario, la CRC recupera el código corto 55100 asignado al PRST Partners Telecom. Igualmente, al PRST Colombia móvil mediante Resolución 8199 de 2026 se le recupera el código Corto 85377, sin embargo, la resolución no está disponible en la página de la CRC y no es posible identificar la causal de recuperación.

Por consiguiente, la recuperación de códigos cortos no puede considerarse un instrumento efectivo para que los ITs cambien su conducta, pues resulta ser un instrumento inefectivo al momento de aplicarse a PRSTs.

Observación regulatoria.

La existencia histórica de procesos de recuperación de códigos cortos asociados a diversos agentes del mercado evidencia que el riesgo de incumplimiento regulatorio no depende de la naturaleza jurídica del actor, sino de la conducta concreta desplegada por el cliente final del cliente del asignatario del recurso.

En consecuencia, no resulta razonable construir un esquema regulatorio que imponga cargas extraordinarias sobre los IT bajo la premisa de que constituyen el principal foco de riesgo del ecosistema, mientras los PRSTs se asumen inmune a los intentos de fraude.

Si la problemática también se ha presentado respecto de otros actores, incluyendo PRST, la respuesta regulatoria debería concentrarse en:

- Los comportamientos de riesgo (ej: mensajes con URLs).
- Los patrones de fraude (ej: mensajes originados por mayoristas-internacionales).
- Los mecanismos efectivos de supervisión.

y no en trasladar cargas regulatorias desproporcionadas a una categoría específica del ecosistema A2P.

Riesgo de sesgo regulatorio.

La regulación podría generar un tratamiento diferenciado injustificado entre actores que participan en el mismo ecosistema de mensajería.

Mientras los ITs asumirían obligaciones reforzadas de:

- KYC.
- Monitoreo permanente.
- Validación de cierto tipo de mensajes (URLs ó originados por mayoristas internacionales).
- Gestión de SenderID.
- Controles antifraude.

los PRST continuarían conservando ventajas estructurales derivadas de:

- Su acceso directo a la infraestructura.
- Monopolio local del acceso a su propia red.
- Su capacidad financiera.
- Su integración vertical.
- Su posición dominante en la cadena de valor, ahora duopolio.

La CRC debe continuar considerando la existencia del monopolio de los PRSTs sobre su propia red, lo que ha sido históricamente una poderosa razón para la regulación de las condiciones de acceso hoy vigente.

Lo anterior podría producir una distorsión competitiva incompatible con los principios de neutralidad tecnológica y promoción de la competencia previstos en la Ley 1341 de 2009.

Recomendación

La CRC debería incorporar dentro de la memoria justificativa y del análisis de impacto regulatorio:

1. Un estudio comparativo de las recuperaciones de códigos cortos ocurridas durante los últimos años en línea con lo recomendado por la ASOBANCARIA.
2. La identificación del tipo de asignatario de Código Corto involucrado en cada caso.

3. El estudio debe tener en cuenta las características de los clientes de los ITs, condiciones técnicas de interconexión (APIs), herramientas utilizadas para la identificación del cliente y otros métodos para la identificación del cliente problema, entre otras variables.
4. El porcentaje de recuperaciones atribuible a ITs, PCAs y PRSTs.
5. El número de SMS maliciosos como % del tráfico total.
6. La demostración de que las obligaciones propuestas guardan relación directa con el riesgo efectivamente identificado.

En ausencia de esta evidencia, existe el riesgo de que la regulación se fundamente en una presunción generalizada de riesgo respecto de los ITs que no se encuentra suficientemente soportada en datos objetivos.

7. La selección adversa como explicación económica de la concentración del fraude en determinados segmentos del ecosistema.

La teoría económica ha identificado el fenómeno de la selección adversa como una consecuencia de las asimetrías de información existentes en determinados mercados.

Este fenómeno resulta particularmente relevante en el análisis del fraude cibernético y del smishing. Los actores maliciosos conocen de antemano sus verdaderas intenciones, mientras que operadores, integradores tecnológicos, proveedores de contenidos y autoridades regulatorias únicamente pueden inferir el riesgo a partir de patrones de comportamiento, monitoreo de tráfico o mecanismos de detección.

Como consecuencia de esta asimetría de información, los estafadores no distribuyen sus actividades de manera uniforme entre todos los participantes del ecosistema. Por el contrario, buscan de forma sistemática aquellos segmentos que ofrecen menores niveles de control, supervisión o detección.

En términos prácticos, los agentes maliciosos tienden a concentrarse en:

- Los proveedores con menores exigencias de vinculación y conocimiento del cliente
- Los canales con controles limitados de monitoreo, como podría ser el caso de los mensajes P2P.
- Los mecanismos de validación más débiles
- Los mercados con menores costos de acceso

- Los ecosistemas regulatorios o tecnológicos más fáciles de vulnerar

Por esta razón, la existencia de fraude en determinados segmentos del mercado no constituye evidencia suficiente para concluir que todos los actores del ecosistema presentan niveles equivalentes de riesgo. Antes bien, puede indicar que los agentes maliciosos han identificado puntos específicos de vulnerabilidad y han concentrado allí sus actividades.

La experiencia internacional en servicios de mensajería, pagos electrónicos y prevención del fraude demuestra que cuando un proveedor implementa mecanismos robustos de control, tales como inteligencia artificial para detección de fraude, sistemas de reputación de remitentes, monitoreo transaccional, validación reforzada de identidad o controles preventivos automatizados, los actores fraudulentos tienden a migrar rápidamente hacia otros proveedores con menores niveles de protección.

Este fenómeno de migración del fraude evidencia que el problema regulatorio no necesariamente radica en la totalidad del ecosistema, sino en aquellos segmentos donde los incentivos económicos y tecnológicos facilitan la actividad ilícita.

En consecuencia, una regulación eficiente debería orientarse a identificar y corregir los puntos específicos donde efectivamente se concentra el fraude, en lugar de asumir que todos los Integradores Tecnológicos, Proveedores de Contenidos y Aplicaciones o asignatarios de códigos cortos presentan niveles equivalentes de riesgo.

De igual forma, la regulación debería privilegiar mecanismos de evaluación basados en resultados verificables antes que esquemas uniformes de cumplimiento formal. Indicadores como las tasas efectivas de fraude, el volumen de tráfico malicioso detectado, el número de reclamaciones asociadas a campañas fraudulentas o la efectividad de los mecanismos de mitigación permiten identificar con mayor precisión los segmentos que requieren intervención regulatoria.

La imposición de cargas regulatorias idénticas para todos los participantes, independientemente de su desempeño real en materia de prevención del fraude, puede generar efectos contraproducentes y de selección adversa. En particular, puede trasladar costos significativos a aquellos actores que ya han realizado inversiones sustanciales en herramientas tecnológicas, inteligencia artificial, monitoreo y controles preventivos, sin generar incentivos adicionales para mejorar los resultados efectivos de seguridad.

Por lo anterior, la CRC debería evaluar si las medidas propuestas reconocen adecuadamente las diferencias existentes entre los distintos segmentos del mercado

y si los costos regulatorios son asignados de manera proporcional al riesgo efectivamente identificado.

La teoría de la selección adversa sugiere que el fraude debe combatirse mediante mecanismos focalizados en los segmentos donde efectivamente se concentra el riesgo, privilegiando indicadores de información, desempeño y resultados verificables sobre esquemas uniformes de cumplimiento formal generalizado que pueden terminar afectando a actores que han demostrado niveles adecuados de control y prevención.

8. La facultad de suspensión inmediata por parte de los PRST genera riesgos para el debido proceso, la competencia y la neutralidad regulatoria.

Problema identificado.

El proyecto contempla mecanismos que permitirían a los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) suspender de manera directa el tráfico asociado a determinados códigos cortos cuando consideren que estos están siendo utilizados para la distribución de contenido malicioso o fraudulento.

Si bien la protección de los usuarios constituye un objetivo legítimo y necesario, la atribución de facultades de suspensión directa a agentes que simultáneamente participan en el mercado plantea importantes riesgos regulatorios y competitivos.

En efecto, los PRST no actúan únicamente como operadores de red, sino que también participan activamente en distintos segmentos del mercado de mensajería móvil y servicios de telecomunicaciones, compitiendo en determinados casos con Integradores Tecnológicos, Proveedores de Contenidos y Aplicaciones y otros agentes del ecosistema.

Por lo anterior, la atribución de facultades de suspensión unilateral podría generar situaciones en las cuales un participante del mercado termina ejerciendo, de facto, funciones cuasi regulatorias respecto de otros agentes económicos con los cuales mantiene relaciones de competencia o intereses comerciales concurrentes, en un claro escenario de conflicto de interés.

Observación regulatoria.

La determinación de que un código corto está siendo utilizado para actividades fraudulentas puede implicar valoraciones técnicas, jurídicas y probatorias complejas.

No toda reclamación, reporte o indicio de fraude constituye evidencia suficiente para justificar la suspensión inmediata de un recurso de numeración cuya utilización legítima puede soportar:

- Servicios financieros.
- Servicios de salud.
- Comunicaciones empresariales.
- Sistemas de autenticación.
- Servicios gubernamentales.
- Comunicaciones de interés público.

La suspensión errónea de un código corto puede producir consecuencias significativas para usuarios, empresas y entidades públicas, incluyendo la interrupción de servicios esenciales, la afectación de operaciones comerciales, la pérdida de confianza de los usuarios, perjuicios reputacionales y afectaciones económicas directas.

Por esta razón, la decisión de suspender un recurso de numeración no debería quedar exclusivamente en cabeza de agentes privados con intereses económicos propios dentro del mercado.

Riesgo de afectación a la libre competencia.

La facultad de suspensión unilateral puede generar incentivos incompatibles con los principios de libre competencia y neutralidad tecnológica.

Incluso en ausencia de conductas anticompetitivas deliberadas, la sola posibilidad de que un operador pueda suspender directamente el tráfico de un tercero genera incertidumbre regulatoria para:

- Integradores Tecnológicos.
- Proveedores de Contenidos y Aplicaciones.
- Remitentes empresariales.
- Nuevos entrantes.

Ello resulta especialmente sensible en mercados caracterizados por altos niveles de concentración y por relaciones verticales entre infraestructura, transporte y prestación de servicios.

En consecuencia, las decisiones que impliquen la suspensión de recursos de numeración deberían estar sujetas a supervisión y validación por parte de una autoridad regulatoria independiente.

Recomendación.

Se propone que la facultad de ordenar la suspensión de códigos cortos permanezca en cabeza de la Comisión de Regulación de Comunicaciones (CRC), como autoridad competente en materia de administración de recursos de identificación y numeración.

1. El PRST que identifique una presunta utilización fraudulenta deberá presentar una solicitud motivada ante la CRC.
2. La solicitud deberá contener los elementos probatorios mínimos que soporten la existencia del riesgo o del comportamiento fraudulento.
3. La CRC deberá evaluar la evidencia presentada y adoptar una decisión dentro de un procedimiento sumario y expedito.
4. La decisión deberá emitirse dentro de un término máximo de veinticuatro (24) horas contadas a partir de la recepción de la solicitud.
5. En casos de extrema urgencia y riesgo inminente para los usuarios, el PRST podrá implementar medidas transitorias de mitigación técnica mientras la CRC adopta la decisión definitiva.

Este modelo permitiría mantener una respuesta rápida frente a amenazas reales, sin sacrificar los principios de imparcialidad, debido proceso, seguridad jurídica y libre competencia.

La propuesta regulatoria parece apartarse de un principio históricamente reconocido por la propia Comisión de Regulación de Comunicaciones según el cual las decisiones de desconexión o suspensión de relaciones esenciales para la prestación de servicios de telecomunicaciones no pueden quedar sujetas a la decisión unilateral de uno de los participantes del mercado.

En efecto, el artículo 4.1.7.5 de la Resolución CRC 5050 de 2016 dispone expresamente que ninguna controversia, conflicto o incumplimiento de los acuerdos de acceso e interconexión podrá dar lugar a la desconexión de los proveedores sin autorización previa de la CRC, manteniéndose las condiciones de acceso e interconexión mientras dicha autorización no sea otorgada.

Aunque la situación regulada en dicha disposición corresponde al régimen de acceso e interconexión, la regla refleja un principio de neutralidad, debido proceso e intervención regulatoria independiente que busca evitar que agentes económicos que participan en el mercado adopten unilateralmente decisiones con capacidad de afectar la operación de otros proveedores.

Bajo esta lógica, la facultad de suspender códigos cortos o interrumpir el tráfico de un Integrador Tecnológico debería permanecer bajo supervisión y control de la CRC, como autoridad competente para la administración de los recursos de identificación y numeración, evitando trasladar facultades materialmente regulatorias a agentes privados con intereses económicos concurrentes dentro del mismo mercado.

Conclusión.

La lucha contra el fraude no debe traducirse en la delegación de facultades materialmente sancionatorias o regulatorias a agentes privados que participan en el mismo mercado sobre el cual recaen dichas decisiones.

La suspensión de códigos cortos constituye una medida de alto impacto económico y operativo que debe ser adoptada por una autoridad independiente, garantizando simultáneamente la protección de los usuarios, el debido proceso y la preservación de condiciones adecuadas de competencia dentro del ecosistema de comunicaciones móviles.

9. Conclusión General.

El proyecto persigue un objetivo legítimo: reducir el fraude cibernético. Sin embargo, las medidas propuestas deben ajustarse para evitar que la mitigación del riesgo financiero termine afectando desproporcionadamente:

- Servicios legítimos de mensajería y comunicaciones de interés público.
- Derechos fundamentales de los usuarios.
- La inclusión digital, la economía popular y las microempresas.

Una regulación basada en riesgo y focalizada en el eslabón de la cadena productiva donde ocurre la falla de mercado, diferenciada por categorías de tráfico y proporcional al nivel real de amenaza permitiría alcanzar los objetivos de protección al usuario sin sacrificar la eficiencia, accesibilidad y utilidad social del canal SMS en Colombia. En este sentido, estamos de acuerdo con los comentarios enviados por la ASOBANCARIA.

Se hace igual de importante profundizar en los efectos colaterales no deseados de la regulación tanto en sus impactos sobre el ecosistema, la estructura productiva y el mercado de mensajería instantánea, así como en la consideración de todos los usuarios de los distintos sistemas definidos por la Ley.

Reiteramos la inconveniencia de trasladar de la CRC a los PRSTs la autoridad para desconectar o suspender tráfico de mensajes cursados por ITs y PCAs. Resultaría

contradictorio que ahora se permita a un PRST suspender unilateralmente la operación de un código corto o de un IT sin intervención previa de la Comisión.

Por último, vale la pena preguntarse si los mecanismos actuales de recuperación de códigos cortos ya permiten sancionar y excluir a los asignatarios que incumplen las reglas, independientemente de que sean IT, PCA o PRST.

Agradecemos a la Comisión de Regulación de Comunicaciones el espacio de participación que ha dispuesto y la oportunidad de exponer estas observaciones, que formulamos con ánimo constructivo y desde nuestra experiencia operativa en el ecosistema de mensajería A2P. Confiamos en que los planteamientos aquí presentados sean valorados en el marco del análisis del proyecto, y reiteramos nuestra entera disposición para participar en las mesas técnicas, aportar información y construir conjuntamente una regulación que combata eficazmente el fraude preservando la eficiencia, la libre competencia y la utilidad social del canal SMS en Colombia.

Cordialmente,

_____

Luis Alfonso Arias
Director Jurídico y de Regulación.
Inalambria Internacional SAS.