



Bogotá, D.C., 23 de junio de 2026

SGAC-GAPRS-109-2026
CECO: S2026

Doctor
FELIPE AUGUSTO DÍAZ SUAZA
Director Ejecutivo
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Calle 59a bis # 5 - 53, Ed Link Siete Sesenta P9
Correos electrónicos: medidasantifraude@crcom.gov.co y atencioncliente@crcom.gov.co

Asunto: Comentarios al borrador de resolución *“Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones”*.

Respetado doctor Díaz,

La Empresa de Telecomunicaciones de Bogotá S.A. E.S.P. – ETB- agradece a la Comisión de Regulación de Comunicaciones, en adelante CRC o la Comisión, la oportunidad de participar en el presente proceso regulatorio y reconoce la importancia de las iniciativas orientadas a fortalecer la protección de los usuarios, incrementar la confianza en los servicios de comunicaciones y reducir los riesgos asociados a las distintas modalidades de fraude que actualmente afectan el ecosistema digital.

ETB considera que el fenómeno del fraude cibernético en los servicios de comunicaciones ha evolucionado hacia un ecosistema digital complejo, dinámico y multisectorial, en el cual intervienen múltiples actores que participan en distintas etapas de la cadena de valor de las comunicaciones, incluyendo la originación, distribución, transporte y terminación de las comunicaciones.

En este contexto, el fraude ya no puede ser entendido ni abordado como un fenómeno exclusivo de las redes de telecomunicaciones, en la medida en que las principales modalidades actuales como el smishing, vishing, phishing, la suplantación de identidad y la distribución de enlaces maliciosos se originan y gestionan principalmente en plataformas digitales, aplicaciones de mensajería, redes sociales, proveedores de contenidos, integradores tecnológicos y otros actores del ecosistema digital, incluyendo agentes internacionales.

Bajo esta realidad, los PRST desempeñan en muchos casos un rol de transporte o acceso dentro de la cadena de comunicaciones, sin ejercer control material sobre el contenido, origen o finalidad de las campañas fraudulentas. Esta condición introduce una asimetría estructural en la distribución de responsabilidades regulatorias, en la medida en que las obligaciones de prevención, detección y mitigación tienden a concentrarse en los PRST, mientras que otros actores con capacidad efectiva de control sobre la generación del riesgo no siempre se encuentran sujetos a obligaciones equivalentes.

En consecuencia, ETB estima que el diseño de las medidas regulatorias debe fundamentarse en un principio de corresponsabilidad funcional basada en el control efectivo, según el cual las obligaciones deben asignarse a los distintos actores del ecosistema digital en proporción a su capacidad real de prevenir, detectar, mitigar o corregir los riesgos asociados al fraude.



Este enfoque implica reconocer tres elementos fundamentales:

1. La existencia de una cadena de valor digital distribuida, en la que el fraude puede originarse en puntos distintos en el ecosistema digital.
2. La necesidad de asignar responsabilidades regulatorias de manera proporcional al grado de control técnico, operativo y económico que cada actor ejerce sobre el riesgo.
3. La importancia de evitar que los PRST asuman cargas desproporcionadas sobre eventos cuya generación o mitigación depende de terceros fuera de su esfera de control.

Desde esta perspectiva, el rol del regulador no consiste únicamente en reforzar obligaciones sobre los operadores de telecomunicaciones, sino en promover un marco regulatorio integral que asegure la participación coordinada de todos los actores del ecosistema digital, incluyendo proveedores de contenidos y aplicaciones (PCA), plataformas OTT, integradores tecnológicos, carriers internacionales y demás agentes involucrados en la cadena de comunicaciones.

Asimismo, el análisis de impacto regulatorio debe garantizar que cualquier intervención cumpla con los principios de necesidad, proporcionalidad, eficiencia, sostenibilidad económica y mínima carga regulatoria, evaluando de manera integral los efectos sobre la competencia, la inversión, la estructura del mercado y la capacidad operativa diferenciada de los distintos tipos de agentes, como los OMV.

De igual manera, ETB considera que las medidas orientadas a la mitigación del fraude deben evitar generar incentivos no deseados de sustitución tecnológica o migración del riesgo hacia plataformas no reguladas, y en su lugar promover un enfoque integral, coordinado y tecnológicamente viable, que garantice su efectividad real dentro del ecosistema digital.

A partir de las anteriores consideraciones, presentamos las siguientes observaciones, comentarios y propuestas de mejora al proyecto:

1. La necesidad de una visión regulatoria que trascienda a los PRST, el fraude digital es un fenómeno multisectorial y no exclusivamente de telecomunicaciones

Respetuosamente consideramos que el principal desafío del proyecto regulatorio radica en que continúa concentrando la mayor parte de las obligaciones regulatorias, operativas, tecnológicas, económicas y sancionatorias sobre los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM), pese a que el fraude digital ha evolucionado hacia un ecosistema mucho más amplio, complejo y descentralizado.

Las modalidades actuales de fraude, tales como el smishing, vishing, phishing, la suplantación de identidad y la distribución de enlaces maliciosos, son concebidas, administradas y ejecutadas a través de plataformas OTT, aplicaciones de mensajería, redes sociales, agregadores tecnológicos, integradores internacionales, proveedores de contenidos y otras plataformas digitales que operan tanto dentro como fuera del territorio nacional.

En muchos casos, como lo reconoce la Comisión, las redes de telecomunicaciones constituyen únicamente el último eslabón de transporte dentro de una cadena mucho más extensa, siendo utilizadas como mecanismo de acceso o contacto con el usuario, mientras que las decisiones relacionadas con el contenido, la identidad utilizada, la campaña fraudulenta, los mecanismos de



distribución y la infraestructura tecnológica desde la cual se origina la actividad son adoptadas por actores que actualmente no se encuentran sujetos a obligaciones equivalentes de trazabilidad, autenticación, monitoreo, validación o gestión de riesgos.

Bajo esta realidad, resulta preocupante que el proyecto continúe trasladando la mayor parte de las cargas de cumplimiento a los PRST, aun cuando estos no tienen control material sobre el contenido de las comunicaciones ni sobre el origen de las campañas fraudulentas.

En ese sentido, el proyecto propuesto configura una asimetría regulatoria en la cual se exige al PRST asumir responsabilidades que, bajo criterios de eficiencia regulatoria y control efectivo del riesgo, deberían recaer principalmente sobre quienes originan, administran, comercializan o facilitan dichas comunicaciones. Por esta razón, estimamos que la efectividad de las medidas propuestas podría verse limitada si la respuesta regulatoria continúa enfocándose predominantemente en los operadores de telecomunicaciones, mientras otros actores con capacidad real de intervención en la prevención del fraude permanecen al margen de obligaciones similares.

En este contexto, consideramos que la CRC se encuentra ante la oportunidad de liderar una evolución regulatoria que promueva un modelo de corresponsabilidad funcional entre todos los participantes de la cadena de generación, originación, transporte y terminación de las comunicaciones digitales, basado en el principio de control efectivo. Ello implica identificar de manera precisa a los actores que controlan el contenido y a aquellos que controlan la infraestructura donde se materializan los riesgos, de manera que cada uno asuma obligaciones proporcionales a su capacidad real de prevenir, detectar, mitigar y contrarrestar el fraude.

En consecuencia, estimamos necesario ampliar progresivamente el alcance regulatorio más allá de los PRST e incorporar obligaciones específicas para los Proveedores de Contenidos y Aplicaciones (PCA), Integradores Tecnológicos (IT), plataformas OTT, proveedores de mensajería digital, agregadores internacionales, carriers internacionales de larga distancia y demás entidades originadoras de tráfico masivo.

En particular, resulta relevante el papel de los PCA e Integradores Tecnológicos, quienes mantienen la relación comercial directa con las marcas, administran campañas masivas de mensajería y tienen control efectivo sobre el contenido transmitido. Desde una perspectiva de eficiencia regulatoria, las medidas de monitoreo, autenticación, validación y prevención deberían ejecutarse prioritariamente en el punto de originación del tráfico y no únicamente en la terminación del mismo.

De igual forma, consideramos necesario que la CRC fortalezca los mecanismos de coordinación institucional con el Ministerio TIC, la Superintendencia Financiera de Colombia, la Superintendencia de Industria y Comercio, COLCERT y demás autoridades competentes, con el fin de desarrollar estrategias integrales que permitan abordar también los canales OTT y demás entornos digitales donde actualmente se concentra la parte creciente de las actividades fraudulentas, pues como ya ha ocurrido con otras medidas una vez se intervienen los canales de telecomunicaciones tradicionales, la actividad de fraude migra casi en su totalidad a entornos digitales.



2. Necesidad de enfocar el AIN hacia criterios de proporcionalidad y sostenibilidad económica

ETB reconoce y valora los avances metodológicos incorporados por la Comisión durante el desarrollo del Análisis de Impacto Normativo (AIN). En particular, destacamos positivamente la evolución en la definición del problema regulatorio, al pasar de una ausencia de herramientas regulatorias a una caracterización más precisa que tiene en cuenta el nivel de efectividad de los mecanismos existentes. Este ajuste metodológico refleja adecuadamente que el sector ya cuenta con instrumentos regulatorios para combatir el fraude, pero que la creciente sofisticación de las amenazas exige fortalecerlos, actualizarlos y complementarlos para mejorar su efectividad, sobre todo cuando el fraude ya permea todo el ecosistema digital.

Asimismo, resaltamos el esfuerzo realizado por la CRC al combinar metodologías de análisis multicriterio, análisis costo-beneficio y evaluación de cargas administrativas para valorar las diferentes alternativas regulatorias. Este enfoque se encuentra alineado con las mejores prácticas internacionales en materia de regulación basada en evidencia y constituye un avance importante en la construcción de medidas regulatorias técnicamente sustentadas.

No obstante, consideramos que el AIN aún presenta desafíos estructurales que deberían ser revisados antes de la expedición definitiva de la intervención regulatoria, particularmente en lo relacionado con la proporcionalidad de las obligaciones propuestas, su sostenibilidad económica, sus impactos competitivos y la distribución adecuada de las cargas regulatorias.

En primer lugar, observamos una fragmentación entre la denominada Fase I y la Fase II del proyecto regulatorio. Mientras la Fase I incorpora obligaciones que implican una elevada carga tecnológica, operativa y financiera, como la implementación de sistemas de monitoreo en tiempo real, motores de detección de fraude, mecanismos de autenticación, validaciones automáticas e integraciones mediante APIs con el Validador Centralizado, entre otras, la revisión del esquema de remuneración del servicio SMS A2P fue trasladada a una etapa posterior.

Desde la perspectiva del AIN, esta separación genera un desbalance regulatorio relevante, pues las cargas de inversión y operación son exigibles de manera inmediata, mientras que los mecanismos que eventualmente permitirían recuperar dichos costos permanecen indefinidos. En consecuencia, se produce una desconexión entre las obligaciones regulatorias impuestas y las fuentes de financiación requeridas para su implementación, situación que compromete el principio de proporcionalidad regulatoria y pone en riesgo la sostenibilidad económica de los operadores obligados.

Por esta razón, consideramos que la entrada en vigencia de las obligaciones técnicas más complejas debería estar condicionada a la definición y entrada en operación de los mecanismos económicos que permitan garantizar su sostenibilidad, de manera que ambas fases sean evaluadas de manera integral como una única unidad económica y regulatoria.

Adicionalmente, estimamos fundamental que el AIN incorpore de manera mucho más profunda los impactos económicos, operativos y competitivos derivados de las obligaciones tecnológicas previstas en el proyecto. Si bien las medidas propuestas pueden resultar razonables para operadores con infraestructura propia, integración vertical, amplias economías de escala y una posición dominante dentro del mercado móvil, sus efectos son sustancialmente distintos para



operadores con estructuras operativas diferentes, como es el caso de los Operadores Móviles Virtuales -OMV-.

En este punto resulta indispensable que la Comisión reconozca expresamente la realidad competitiva actual del mercado móvil colombiano. Hoy el mercado presenta una elevada concentración y, en términos prácticos, opera bajo una dinámica que puede calificarse como un duopolio táctico, con operadores que cuentan con una infraestructura propia nacional, capacidad de inversión y economías de escala proporcionales a su tamaño. Esta situación les permite absorber con mayor facilidad nuevas obligaciones regulatorias, distribuir sus costos de cumplimiento sobre bases de usuarios significativamente más amplias y aprovechar sinergias operativas que no están disponibles para los demás competidores.

Por otro lado, hay operadores que, como ETB participan en el mercado bajo OMV, sin infraestructura propia de acceso móvil, con una alta dependencia de terceros para la provisión de elementos esenciales de red y sin acceso a las economías de escala que caracterizan a los principales operadores del sector. Adicionalmente, ETB no percibe cargos de terminación mayorista asociados a los servicios de voz y SMS, u otros ingresos asociados a la red móvil que le permitan financiar inversiones de gran magnitud en sistemas de monitoreo, validación, integración tecnológica y gestión antifraude.

Como consecuencia de ello, las inversiones (CAPEX) y los costos operativos recurrentes (OPEX) derivados de la implementación de las obligaciones previstas en el proyecto resultan proporcionalmente mucho más gravosos para los operadores como los OMV no tienen acceso al manejo de la red y, además, cuentan con una menor escala frente a los operadores de red dominantes. Esta circunstancia no parece haber sido evaluada de manera suficiente dentro del AIN y es fundamental que se tenga en cuenta.

En efecto, la imposición de obligaciones homogéneas sobre agentes con capacidades económicas, tecnológicas y operativas profundamente diferentes puede generar efectos anticompetitivos no deseados. Pues en la práctica, las cargas regulatorias adicionales terminan convirtiéndose en barreras económicas que fortalecen las ventajas estructurales de los operadores dominantes y dificultan la permanencia, expansión y crecimiento de actores de menor tamaño.

Por ello, consideramos que el AIN debe incorporar expresamente una evaluación de impacto sobre competencia, analizando si las medidas propuestas podrían reforzar la concentración existente en el mercado móvil colombiano y consolidar aún más las ventajas competitivas derivadas del actual escenario de duopolio táctico. La regulación no debe convertirse en un mecanismo que, aun de manera indirecta, termine favoreciendo a quienes cuentan con mayores capacidades económicas para absorber los costos de cumplimiento regulatorio.

Adicionalmente, el análisis debería considerar que los operadores móviles tradicionales no solo compiten entre sí, sino también con plataformas OTT globales que ofrecen servicios sustitutos de voz y mensajería sin estar sujetas a obligaciones regulatorias equivalentes en materia de autenticación, monitoreo, trazabilidad, prevención del fraude o reporte de información.

En este escenario, la imposición de mayores costos regulatorios exclusivamente sobre los PRST puede generar incentivos económicos para que una parte creciente del tráfico legítimo migre hacia plataformas digitales no reguladas. Este fenómeno no solo afecta la sostenibilidad de los servicios



tradicionales, sino que puede producir un resultado contrario al perseguido por la regulación, trasladando progresivamente las comunicaciones hacia entornos sobre los cuales las autoridades colombianas cuentan con menores capacidades de supervisión, trazabilidad e intervención frente a actividades fraudulentas.

Por estas razones, consideramos indispensable que el AIN evalúe expresamente los efectos de concentración de mercado, las asimetrías competitivas existentes entre operadores, el impacto diferenciado sobre los OMV, los riesgos derivados del actual esquema de duopolio táctico y los posibles efectos de sustitución hacia plataformas OTT, garantizando que las medidas finalmente adoptadas sean efectivas, proporcionales, sostenibles y compatibles con los principios de promoción de la competencia establecidos en la Ley 1341 de 2009.

3. Particularidades técnicas y operativas de los OMV

Adicional a lo expuesto desde el punto de vista de la competencia, solicitamos respetuosamente a la Comisión considerar de manera expresa las particularidades técnicas, operativas y económicas de los modelos de OMV dentro del diseño regulatorio propuesto. Si bien los OMV son responsables del cumplimiento de las obligaciones regulatorias que les resulten aplicables, su capacidad de implementación material difiere sustancialmente de la de los operadores con infraestructura propia, circunstancia que debe reflejarse en el alcance, gradualidad y exigibilidad de las medidas contempladas en el proyecto.

Los OMV desarrollan su actividad mediante el uso de infraestructura, plataformas y elementos de red administrados por terceros, incluyendo operadores anfitriones, carriers y otros proveedores especializados que intervienen en la prestación del servicio. Como consecuencia de ello, una parte significativa de las funcionalidades relacionadas con la señalización, el transporte de tráfico, la mensajería, el monitoreo en tiempo real, la detección de patrones de fraude, la autenticación de comunicaciones, la validación de identificadores y la ejecución de bloqueos o etiquetados preventivos depende de plataformas y sistemas sobre los cuales el OMV no tiene administración ni control directo.

En este contexto, la implementación de varias de las obligaciones previstas en el proyecto regulatorio no depende exclusivamente de la voluntad o capacidad de gestión del operador móvil virtual, sino que requiere necesariamente desarrollos tecnológicos, integraciones, adecuaciones de red, procesos de interoperabilidad, pruebas y configuraciones que deben ser ejecutadas por los proveedores de red. Esta situación resulta particularmente relevante frente a las obligaciones asociadas al monitoreo de tráfico en tiempo real, la interacción con el Validador Centralizado, la gestión de Sender ID, los mecanismos de autenticación de comunicaciones y las medidas de detección y mitigación de fraude previstas en el proyecto.

Por lo anterior, consideramos necesario que la regulación incorpore expresamente el principio de control efectivo de la red, de manera que las obligaciones técnicas recaigan sobre el actor que efectivamente administra los elementos de red y las plataformas donde deben ejecutarse las funcionalidades exigidas por la regulación. Pues imponer a los OMV responsabilidades asociadas a funciones que dependen materialmente de terceros podría generar escenarios de incumplimiento involuntario frente a aspectos que escapan de su esfera real de control y decisión.



Asimismo, resulta indispensable que la Comisión considere estas dependencias operativas al momento de definir los cronogramas de implementación. Los plazos propuestos en el proyecto no parecen reflejar la complejidad técnica que implica coordinar desarrollos simultáneos entre OMV, OMR's, carriers internacionales, proveedores tecnológicos, PCA, actores financieros y demás actores involucrados en el ecosistema. La implementación efectiva de estas medidas requerirá procesos de análisis, diseño, desarrollo, contratación, integración, pruebas de interoperabilidad y estabilización operacional que, por su naturaleza, exceden ampliamente los tiempos inicialmente previstos.

En consecuencia, solicitamos que la CRC contemple esquemas de implementación diferenciados para los OMV, reconozca expresamente las limitaciones derivadas de la dependencia tecnológica respecto de terceros y adopte plazos de transición acordes con la complejidad de los desarrollos requeridos. Lo anterior contribuirá a una implementación efectiva de las medidas regulatorias, brindará seguridad jurídica respecto de las responsabilidades de cada actor de la cadena y permitirá alcanzar los objetivos de mitigación del fraude sin desconocer las particularidades técnicas y operativas de los modelos de operación móvil virtual.

4. Riesgos asociados al Validador Centralizado

El proyecto establece un esquema de validación previa de comunicaciones que depende del funcionamiento permanente, continuo y oportuno del Validador Centralizado. Si bien comprendemos los objetivos perseguidos por esta herramienta en materia de autenticación y reducción de actividades fraudulentas, consideramos que el Análisis de Impacto Normativo no desarrolla de manera suficiente los riesgos operativos, tecnológicos y sistémicos asociados a la creación de un componente centralizado que se convertiría en un elemento crítico para el funcionamiento de todo el ecosistema nacional de mensajería.

Desde una perspectiva de arquitectura de redes y continuidad operacional, la implementación de un mecanismo de consulta obligatoria previa introduce un punto único de falla ("single point of failure") cuya indisponibilidad, degradación o mal funcionamiento podría generar afectaciones masivas sobre múltiples servicios esenciales. La dependencia de una plataforma centralizada implica que cualquier incidente tecnológico, falla de conectividad, error de integración, degradación de desempeño, ataque cibernético o problema de capacidad podría impactar simultáneamente a todos los operadores, integradores y entidades que dependen de dicho mecanismo para la validación de sus comunicaciones.

Particular preocupación genera la ausencia de un análisis detallado sobre los efectos que podrían derivarse de incrementos en las latencias de respuesta. El proyecto contempla tiempos de validación extremadamente exigentes, sin que exista evidencia suficiente sobre el comportamiento real de una plataforma de esta naturaleza bajo condiciones de carga masiva, eventos de contingencia o crecimiento acelerado del tráfico. Una degradación marginal en los tiempos de respuesta podría traducirse en retrasos significativos en la entrega de comunicaciones críticas para millones de usuarios.

Este riesgo adquiere una dimensión aún mayor en sectores altamente dependientes de la mensajería transaccional, como el financiero, asegurador, salud, transporte, comercio electrónico, servicios públicos y gobierno digital. Actualmente, una parte significativa de las operaciones de autenticación y seguridad depende del envío oportuno de mensajes OTP (One Time Password),



códigos de verificación, alertas de transacciones, confirmaciones de pagos, validaciones biométricas y notificaciones críticas cuya utilidad desaparece si no son entregadas dentro de ventanas de tiempo extremadamente reducidas.

En este sentido, un retraso de pocos segundos derivado de una falla de sincronización, una indisponibilidad temporal del Validador Centralizado o una congestión de las APIs de integración podría generar la interrupción de procesos financieros legítimos, procesos de validaciones de identidad y afectar la experiencia de millones de usuarios y producir impactos económicos significativos para múltiples sectores de la economía.

Por lo anterior, consideramos indispensable que la Comisión analice la exigencia económica, técnica y operativa de la propuesta, frente a la efectividad de la medida, pues se requieren de inversiones, que dada la situación actual del sector, son significativas, ya que las medidas a implementar requieren requisitos robustos de continuidad operativa, alta disponibilidad, redundancia geográfica, planes de contingencia, mecanismos de operación degradada, esquemas de respaldo y protocolos de recuperación ante desastres, redefinición de niveles mínimos de servicio (SLA), estructuración de mecanismos de compensación ante fallas, procedimientos de contingencia cuando el Validador no se encuentre disponible y las responsabilidades asociadas a eventuales afectaciones derivadas de incidentes atribuibles al administrador de dicha plataforma.

Igualmente, estimamos necesario que la Comisión evalúe alternativas arquitectónicas menos centralizadas o mecanismos de validación distribuidos que permitan mitigar los riesgos inherentes a la concentración de funciones críticas en un único componente tecnológico. Máxime cuando la medida no cubre a las OTT, pues esto implica que los PRST hacen todo un esfuerzo para mitigar fraudes y, la delincuencia ante las limitaciones que encuentra en los servicios tradicionales migran su esquema a espacios no regulados, lo que compromete seriamente la efectividad de la medida.

5. Necesidad de un régimen de Puerto Seguro (Safe Harbor)

El proyecto asigna a los operadores responsabilidades crecientes en materia de monitoreo, detección, bloqueo y etiquetado de comunicaciones potencialmente fraudulentas. Sin embargo, es importante reconocer que ningún sistema de analítica, inteligencia artificial, detección de patrones o correlación de eventos ofrece niveles absolutos de precisión.

La experiencia internacional demuestra que incluso los sistemas más sofisticados de prevención del fraude generan inevitablemente falsos positivos y falsos negativos. Esta realidad es inherente a cualquier modelo de detección basado en comportamiento, reputación, aprendizaje automático o reglas dinámicas de riesgo.

En consecuencia, si bien es cierto es muy positivo la posibilidad de realizar acciones ante la posibles actividades que impliquen riesgos para los usuarios, también lo es que la posibilidad de bloquear, retrasar o etiquetar como sospechosas comunicaciones legítimas representa un riesgo operativo significativo para los operadores y para los usuarios finales. Este riesgo resulta particularmente sensible cuando se trata de comunicaciones transaccionales, servicios financieros, autenticaciones, alertas de seguridad o comunicaciones asociadas a servicios esenciales.

Bajo el esquema actualmente propuesto, los operadores podrían enfrentar simultáneamente dos riesgos regulatorios contrapuestos: por un lado, ser cuestionados por no bloquear oportunamente



una comunicación fraudulenta; y por otro, ser objeto de reclamaciones, investigaciones o sanciones por bloquear una comunicación legítima como resultado de un falso positivo razonable.

Este escenario genera incertidumbre jurídica y puede incentivar conductas excesivamente conservadoras o, por el contrario, limitar la efectividad de los mecanismos de mitigación ante el temor de asumir responsabilidades por decisiones automatizadas.

Por estas razones, consideramos indispensable la Comisión incorpore una disposición expresa en el sentido que los PRST no serán objeto de responsabilidad o sanción cuando ejecuten o adopten medidas de bloqueo, etiquetado o mitigación sustentadas en criterios objetivos de riesgo, indicadores de fraude reconocidos por la industria, información proveniente de autoridades competentes o parámetros definidos por la propia regulación, siempre que hayan actuado de manera diligente y dentro del ámbito de control que razonablemente les corresponde

Aquí es necesario reiterar que reconocer que ningún sistema de detección de fraude es infalible. Siempre existirán errores inevitables, porque los mecanismos de monitoreo funcionan con probabilidades, patrones de comportamiento y análisis automatizados.

La existencia de un esquema de esta naturaleza fortalecería la seguridad jurídica de los actores obligados, facilitaría la adopción efectiva de las medidas previstas en la regulación y promovería una respuesta más ágil frente a amenazas emergentes.

Esta solicitud cobra especial relevancia si se tiene en cuenta que las obligaciones previstas en el proyecto trascienden en muchos casos el ámbito de control directo de los operadores. Como se ha expuesto, una parte significativa de las conductas fraudulentas se origina en plataformas OTT, aplicaciones de mensajería, redes sociales, proveedores de contenidos, integradores tecnológicos, carriers internacionales y otros actores sobre los cuales los PRST no tienen control material ni capacidad de intervención directa. De igual manera, en el caso de los OMV, numerosas funcionalidades asociadas al monitoreo, autenticación, validación, detección y bloqueo dependen de infraestructura y plataformas administradas por terceros, como los operadores de red.

En este contexto, resulta contrario a los principios de razonabilidad y proporcionalidad exigir a los PRST resultados absolutos frente a riesgos cuya generación, administración o mitigación depende parcial o totalmente de terceros. El ordenamiento jurídico reconoce el principio general según el cual nadie está obligado a lo imposible (*ad impossibilia nemo tenetur*), razón por la cual las obligaciones regulatorias deben evaluarse a la luz de las capacidades reales de actuación y control de los sujetos obligados.

Precisamente por ello, cuando la regulación exige a los operadores desplegar mecanismos de prevención sobre eventos que ocurren fuera de su red, sobre contenidos que no generan, administran ni controlan, o sobre plataformas cuya operación depende de terceros, resulta necesario establecer salvaguardas regulatorias que reconozcan dichas limitaciones objetivas.

6. Fortalecimiento de obligaciones para carriers internacionales

Las modalidades actuales de fraude vinculadas al CLI Spoofing, la manipulación de numeración, la alteración de identificadores de origen, el tráfico gris y la suplantación de identidad presentan una dimensión crecientemente internacional.



Diversos esquemas fraudulentos aprovechan la complejidad de las rutas internacionales de transporte para modificar información de señalización, ocultar el verdadero origen de las comunicaciones o introducir tráfico mediante múltiples intermediarios antes de alcanzar las redes nacionales.

En este contexto, consideramos que el proyecto concentra de manera excesiva las obligaciones de detección y mitigación sobre los operadores receptores nacionales, sin reconocer que una parte sustancial de la capacidad técnica para identificar irregularidades se encuentra precisamente en los carriers internacionales y en los puntos donde se origina o transporta el tráfico hacia Colombia.

Por ello, estimamos necesario que la CRC avance hacia la incorporación de obligaciones explícitas de trazabilidad, auditoría, conservación de registros, validación de identificadores y cooperación operativa para los carriers internacionales que participan en el transporte de tráfico hacia el país.

La mitigación efectiva del fraude internacional requiere controles distribuidos a lo largo de toda la cadena de transporte y no únicamente medidas correctivas en el punto final de terminación. De lo contrario, se corre el riesgo de trasladar ineficiencias técnicas y económicas a los operadores nacionales sin intervenir los eslabones donde realmente se genera o facilita la alteración de la información.

7. Cargas regulatorias, reportes y coherencia regulatoria

Llama particularmente la atención que el proyecto incorpore nuevas obligaciones de monitoreo, reporte, intercambio de información, seguimiento operativo y generación de estadísticas en un momento en el cual la propia Comisión adelanta iniciativas regulatorias orientadas a la simplificación administrativa, racionalización de reportes y reducción de cargas regulatorias.

Desde una perspectiva de buena gobernanza regulatoria, consideramos fundamental que la CRC mantenga una visión integral y transversal de su agenda regulatoria. Las obligaciones no pueden evaluarse de manera aislada o sectorizada, sino considerando el efecto acumulativo que generan sobre los agentes regulados.

La regulación no puede construirse en silos. Cada nueva obligación debe analizarse conjuntamente con las cargas ya existentes, los costos de cumplimiento acumulados y los esfuerzos institucionales orientados a simplificar el marco regulatorio.

En consecuencia, estimamos necesario que el AIN incorpore una valoración integral de las cargas administrativas adicionales que generará éste proyecto y los demás que están en curso frente a la efectividad de las medidas, pues como ya se ha mencionado ya hay eventos en donde las medidas sobre servicios tradicionales hizo que la delincuencia migrara su actuar hacia las OTT, como en los bloqueos de ERON. Desde esta óptica se requiere que se analice la carga de la intervención, su efectividad así como una evaluación de posibles mecanismos de simplificación o sustitución de reportes existentes para evitar duplicidades regulatorias.

8. Observaciones sobre el Comité Técnico de Lucha contra el Fraude

Valoramos positivamente la creación de espacios de coordinación sectorial orientados al intercambio de información y al fortalecimiento de capacidades colectivas para enfrentar el fraude.



Sin embargo, consideramos necesario preservar claramente la diferencia entre funciones de coordinación técnica y funciones regulatorias.

En nuestra opinión, el Comité Técnico de Lucha contra el Fraude debe constituirse como una instancia de articulación, análisis técnico y generación de recomendaciones, pero no como un mecanismo habilitado para introducir obligaciones regulatorias nuevas, modificar condiciones de prestación de servicios o adoptar decisiones con efectos normativos vinculantes sin que se surta el correspondiente AIN.

Pues permitir que se generen obligaciones regulatorias sin agotar los procedimientos de consulta pública, participación ciudadana con el AIN previsto en la Ley 1341 de 2009 podría afectar principios fundamentales de transparencia, seguridad jurídica, publicidad y debido proceso regulatorio.

Por esta razón, consideramos que cualquier obligación adicional que implique costos, inversiones, desarrollos tecnológicos o modificaciones operativas para los agentes regulados debe ser sometida previamente a los procedimientos ordinarios de construcción regulatoria y al correspondiente AIN.

9. Plazos de implementación

Finalmente, consideramos que los plazos de implementación propuestos no reflejan adecuadamente la complejidad técnica, operativa y económica de las medidas previstas en el proyecto.

La implementación de sistemas de monitoreo en tiempo real, motores de analítica antifraude, integraciones con el Validador Centralizado, adecuaciones de plataformas de mensajería, ajustes de señalización, modificaciones contractuales, desarrollos tecnológicos, pruebas de interoperabilidad y procesos de capacitación requiere horizontes temporales significativamente superiores a los contemplados actualmente.

Por ello, consideramos indispensable la realización de mesas técnicas previas a la expedición de la resolución definitiva que permitan definir la Fases I y la Fase II en una sola, los impactos a diferentes sectores transaccionales, así como la validación de estándares de interoperabilidad, especificaciones funcionales, modelos de integración mediante APIs, criterios de validación y procedimientos operativos comunes para toda la industria.

Asimismo, solicitamos un plazo mínimo de veinticuatro (24) meses para su implementación contados a partir de la definición definitiva de los estándares técnicos y de la disponibilidad efectiva de las plataformas requeridas. De igual forma, consideramos necesario establecer cronogramas diferenciados para operadores con dependencia tecnológica de terceros como los OMV, así como desarrollar esquemas graduales de implementación acompañados de ambientes de prueba, pilotos controlados y periodos de estabilización operacional antes de la exigibilidad plena de las obligaciones.

10. Consideraciones finales

ETB reitera su compromiso con la protección de los usuarios y con la implementación de medidas efectivas para combatir el fraude en los servicios de comunicaciones. No obstante, consideramos



que el éxito de cualquier estrategia regulatoria dependerá de su capacidad para reconocer que el fraude es un fenómeno transversal que involucra a múltiples actores del ecosistema digital.

En este sentido, estimamos que el proyecto regulatorio puede fortalecerse mediante un enfoque que complemente las obligaciones aplicables a los PRST con mecanismos progresivos de corresponsabilidad, trazabilidad y cooperación, dirigidos también a los proveedores de contenidos y aplicaciones, plataformas OTT, agregadores, carriers internacionales y demás actores que participan en la originación, facilitación y transporte de las comunicaciones.

Asimismo, resulta clave evaluar la efectividad real de la medida propuesta, considerando que, en el contexto económico actual del sector, podría presentarse el riesgo de que su implementación derive rápidamente en una migración de tráfico o servicios hacia esquemas OTT, reduciendo su impacto regulatorio. Esto podría generar cargas significativas para los PRST en términos de inversión y cumplimiento, sin que se logre una mitigación efectiva del fenómeno, en la medida en que este se traslade hacia otros segmentos del ecosistema.

Adicionalmente, consideramos necesario que las fases del proyecto regulatorio sean unificadas en aras de garantizar mayor coherencia, eficiencia y sostenibilidad en su implementación.

Estamos convencidos de que una visión integral permitirá atacar las causas estructurales del problema, incrementar la efectividad de las medidas regulatorias y distribuir de manera más equilibrada las responsabilidades entre quienes efectivamente intervienen en las distintas etapas de la cadena de comunicaciones.

Agradecemos a la Comisión la oportunidad de participar en este proceso regulatorio y reiteramos nuestra disposición para contribuir a la construcción de medidas que fortalezcan la disponibilidad de información para la toma de decisiones regulatorias, preservando al mismo tiempo la sostenibilidad de las redes, la inversión y la competencia en el sector.

Cordialmente,

LUDWIG CHRISTIAN CLAUSEN NAVARRO

Gerente Asuntos Públicos, Regulación y Sostenibilidad

Elaboró: Tatiana Sedano Cardozo – Gerencia Asuntos Públicos, Regulación y Sostenibilidad