

Chia, Cundinamarca 23 de junio de 2026

Señores

COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC)

Sesión de Comisión de Comunicaciones

Administrador de los Recursos de Identificación

Bogota

Asunto: Comentarios de Hablame Colombia S.A. E.S.P. al proyecto de resolución "Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones".

Respetados señores:

Diego Valdivieso, Apoderado General de Hablame Colombia S.A. E.S.P. (NIT 900.994.857-4), presento los comentarios de la compañía al proyecto de resolución del asunto, dentro del término de la consulta pública y con fundamento en el numeral 8 del artículo 8 del CPACA y en los artículos 2.2.13.3.2 y 2.2.13.3.3 del Decreto 1078 de 2015.

1. La desconexión y la oposición al acceso no pueden quedar en manos de un agente privado

El artículo 8, al modificar el artículo 6.1.1.8, faculta al PRSTM para suspender la relación de acceso y, ante la reincidencia, para solicitar la desconexión definitiva del integrador o del PCA. El artículo 5 completa ese esquema con dos causales nuevas, los numerales 4.1.2.6.4 y 4.1.2.6.5, que le permiten oponerse a un nuevo acceso. El efecto combinado es que un particular queda habilitado para suspender, terminar o impedir el acceso de otro agente a la red, esto es, para sacarlo del mercado. Y ese particular no es neutral: en el ecosistema A2P el PRSTM es a la vez competidor y árbitro, porque el propio proyecto lo habilita como asignatario de código corto A2P y de SENDER ID. Ninguna razón de política pública justifica poner una decisión de esa magnitud en manos de quien tiene un interés directo en el resultado.

El acceso y la interconexión no son una concesión del operador, sino una obligación legal que la Comisión regula y vigila. El artículo 50 de la Ley 1341 de 2009 obliga a permitir el acceso a todo proveedor que lo solicite, en condiciones no discriminatorias y bajo las reglas que fija la CRC, y los artículos 42 y 43 reservan a la Comisión la solución de las controversias de acceso. El proyecto invierte ese diseño y traslada al operador una facultad decisoria que la ley puso en cabeza del regulador. Que un PRSTM resuelva por su cuenta suspender o terminar el acceso no es un asunto de orden técnico, es una decisión que la ley no le permite tomar.

Hay algo más grave que el reparto de competencias. Otorgar al operador la facultad de desconectar a otros agentes es, en sí mismo, dotarlo de un instrumento de abuso de posición



Autopista Norte
Km 19 Centro Empresarial
Tyla Chia - Colombia



experiencia@hablame.co

Página 1 de 7



Seguridad y salud
en el trabajo
ISO 45001:2018



Gestión de
la calidad
ISO 9001:2015



Seguridad
información
ISO 27001:2015



Gestión
ambiental
ISO 14001:2013

dominante. El régimen de protección de la competencia, contenido en la Ley 1340 de 2009 y en el artículo 50 del Decreto 2153 de 1992, califica como abuso de la posición dominante, entre otras conductas, obstruir o impedir a terceros el acceso a los mercados o a los canales de comercialización y aplicar condiciones discriminatorias que dejen a un competidor en desventaja. Esa lista no es taxativa: lo que la norma persigue es impedir que quien tiene poder de mercado lo use para excluir a sus rivales. Una facultad de desconexión en manos del operador es, por definición, una herramienta de exclusión, porque le permite cortar el acceso a la red a un competidor, degradar su operación o expulsarlo del mercado. El proyecto, entonces, no solo deja de cumplir el mandato que la ley le da a la CRC de prevenir el abuso de posición dominante (numeral 5 del artículo 22 y artículo 19 de la Ley 1341), sino que le entrega al operador el medio para cometerlo.

Este riesgo no es teórico. El operador de mayor peso ya fue declarado dominante. La CRC calificó a Claro (Comcel) como operador con posición dominante en el mercado de servicios móviles mediante la Resolución CRC 6146 de 2021, confirmada en reposición, y por esa razón le impuso medidas asimétricas en la Resolución CRC 7285 de 2024. La posición dominante es justamente el presupuesto que la ley de competencia exige para que una conducta exclusoria se califique como abuso. Dicho de otro modo, el agente sobre el que recaería esta facultad ya reúne la condición que convierte su uso en abuso de posición dominante. El marco asimétrico que la propia Comisión construyó para contener a Claro quedaría contradicho por una resolución que le entrega una herramienta nueva para excluir competidores. La CRC estaría desarmando con una mano lo que reforzó con la otra.

Por todo lo anterior, nuestra posición es que la desconexión de un integrador tecnológico no cabe en ningún escenario y debe salir del proyecto. La función del integrador es técnica y consiste en proveer la infraestructura que hace posible la interoperabilidad de los mensajes. Excluirlo no combate el fraude; el fraude se combate identificando y rastreando al originador. Y si pese a todo la Comisión considerara mantener alguna forma de desconexión como medida regulatoria, los principios de igualdad, neutralidad, proporcionalidad y no discriminación obligan a aplicarla al PRSTM en las mismas condiciones en que se pretenda aplicar al integrador o al PCA. No es admisible un régimen en el que el PRSTM pueda desconectar o limitar a otros agentes y, al mismo tiempo, quede exento de esa consecuencia. La asimetría es, en sí misma, el vicio que debe corregirse. En consecuencia, el parágrafo que faculta al PRSTM para suspender el acceso y solicitar la desconexión, en cuanto el artículo 8 modifica el 6.1.1.8, y los numerales 4.1.2.6.4 y 4.1.2.6.5 del artículo 4.1.2.6 deben eliminarse.

2. Las causales de recuperación del código corto A2P deben limitarse a la conducta propia del titular

El artículo 12 subroga el Capítulo 4 del Título VI y concentra en el artículo 6.4.3.2 las causales para recuperar el código corto A2P, junto con los criterios de uso eficiente del artículo 6.4.3.1 y la suspensión prevista en sus párrafos. Conviene ser claros sobre lo que está en juego. Para

el integrador, el código corto A2P es el recurso sobre el que se sostiene toda su operación. Perderlo no es una sanción más, equivale a cerrar el negocio y a dejar sin servicio a todos sus clientes. Una consecuencia de esa gravedad solo puede proceder por una conducta propia, directa, comprobada y atribuible al titular del código. Es la aplicación elemental del debido proceso, de la tipicidad y del principio de que nadie responde sino por sus propios actos (artículo 29 de la Constitución). El integrador no puede pagar por lo que hagan terceros ni por obligaciones que la norma asigna al PRSTM, al validador, al originador, al PCA o al asignatario del SENDER ID. Revisadas una a una, varias causales rompen esa regla y deben corregirse.

2.1. Envío sin SENDER ID o sin plantilla vigente (numeral 6.4.3.2.5)

Esta causal permite recuperar el código por el envío de mensajes sin SENDER ID asignado o sin plantilla vigente. El problema es que el control que verifica esos requisitos no es del integrador, es del operador. El artículo 6.13.4.7.2 obliga al PRSTM a comprobar, antes de enrutar cada mensaje, que existan código corto, SENDER ID y plantilla válidos, y a bloquear el que no cumpla. Si el filtro está en cabeza del operador y aun así un mensaje sin SENDER ID o sin plantilla llega a cursarse, la falla es del filtro, no del integrador. Sancionar al integrador por un mensaje que el operador tenía el deber de bloquear es trasladarle la responsabilidad de una obligación ajena. A esto se suma que la asignación del SENDER ID y la aprobación de la plantilla dependen del PCA y del validador, de modo que el integrador ni siquiera controla los elementos cuya ausencia se le reprocha. Esta causal debe eliminarse respecto del asignatario del código corto A2P, salvo que se acredite una conducta propia y deliberada de este.

2.2. Mensajes atribuibles al mal uso de plantillas (numeral 6.4.3.2.6)

La causal habilita la recuperación por mensajes que potencialmente puedan atribuirse al mal uso de las plantillas. La palabra potencialmente es incompatible con cualquier régimen sancionatorio serio, porque permite retirar el recurso sobre una mera posibilidad, sin certeza ni prueba, lo que vulnera la seguridad jurídica y el principio de tipicidad. Además, el contenido de los mensajes y su correspondencia con la plantilla aprobada son responsabilidad de quien origina, que es el asignatario del SENDER ID, no el integrador. Como está redactada, la causal castiga al operador técnico por un hecho que ni controla ni decide. Debe reformularse para que solo proceda cuando se acredite que el asignatario del código, con conocimiento, permitió o facilitó el envío de tráfico no autorizado, y debe eliminarse la palabra potencialmente.

2.3. Infracciones de datos personales o de propiedad intelectual (numeral 6.4.3.2.10)

Esta causal permite recuperar el código por infracciones a las normas de protección de datos personales o de propiedad intelectual. Esas infracciones recaen sobre quien decide y controla el contenido y los datos, es decir, sobre el originador. La Ley 1581 de 2012 distingue con precisión entre el responsable del tratamiento, que define los fines y los medios, y el encargado, que se limita a tratar los datos por instrucción del responsable. El integrador encaja en la segunda categoría, porque transmite por cuenta del originador y no decide sobre el contenido ni sobre los datos. Imputarle a él una infracción de contenido desconoce esa distinción legal y termina sancionando a quien no es responsable. La causal debe reservarse al asignatario del SENDER ID y eliminarse respecto del asignatario del código corto A2P.

2.4. Incumplimiento de obligaciones generales y especiales (numerales 6.4.3.2.1 y 6.4.3.2.2)

Estas dos causales remiten de forma genérica al incumplimiento de las obligaciones generales y especiales del régimen. El problema es que entre esas obligaciones especiales figura el artículo 6.13.4.5.1, redactado como obligación de resultado mediante la palabra garantizar. Esa redacción convierte al integrador en garante de hechos que no dependen de él, sino del validador, del operador y del originador. Una causal de recuperación anclada en una obligación imposible de cumplir es, en la práctica, una causal abierta, porque siempre habrá un resultado que el integrador no pudo garantizar por no estar en sus manos. La solución pasa por reformular el artículo 6.13.4.5.1 como una obligación de medios, exigible cuando el integrador consultó los registros del validador y del SIGRI y actuó de buena fe, y por limitar estas causales al incumplimiento propio y comprobado del titular del código.

2.5. Criterio de uso eficiente que exige tráfico siempre verificado (numeral 6.4.3.1.7)

Este criterio de uso eficiente exige que el integrador curse únicamente tráfico de originadores con SENDER ID vigente y plantilla aprobada. Con ello se le impone ser garante permanente del estado de validación de terceros, un estado que administra el validador y que puede cambiar en cualquier momento sin que el integrador lo sepa. Si un SENDER ID o una plantilla pierden vigencia por una decisión del validador o del PCA, el integrador no tiene forma de anticiparlo en tiempo real. Convertir esa circunstancia en uso ineficiente, con la consecuencia de perder el código, es sancionarlo por algo que no controla. El criterio debe entenderse cumplido cuando el integrador consulta los registros del validador y del SIGRI antes de cursar el tráfico, y la pérdida sobrevenida de vigencia en cabeza de un tercero no puede imputársele.

2.6. Razones de interés general o seguridad nacional (numeral 6.4.3.2.9)

Esta causal permite recuperar el código por razones de interés general o de seguridad nacional, sin precisar el supuesto que la activa ni el procedimiento que debe seguirse. Una cláusula tan abierta deja al titular sin saber cuándo puede perder el recurso y habilita decisiones discrecionales, contrarias a la seguridad jurídica y al debido proceso. El interés general y la seguridad nacional son fines legítimos, pero su invocación no puede sustituir la motivación ni el procedimiento. La causal debe condicionarse a un acto administrativo motivado, con una causa concreta y demostrada, observancia del debido proceso y aplicación del principio de proporcionalidad, indicando siempre la medida menos gravosa disponible.

2.7. Efecto en cascada sobre los SENDER ID vinculados (parágrafo 1 del artículo 6.4.3.2)

El parágrafo dispone que la recuperación del código corto A2P afecta a todos los SENDER ID vinculados y concede treinta días hábiles para que cada uno migre a otro proveedor. La medida traslada la sanción a clientes que no incurrieron en ninguna conducta y, además, fija un plazo que en el mundo real es imposible de cumplir. Un banco, una entidad pública o una gran superficie no pueden adelantar una contratación, cambiar de integración tecnológica y certificarse en treinta días hábiles. El resultado sería la interrupción de servicios críticos como la autenticación, las alertas de seguridad y las notificaciones transaccionales. El propio proyecto reconoce el problema en otro lugar: el parágrafo 1 del artículo 6.1.1.8 ordena, cuando la

recuperación afecta a usuarios, una transición de seis meses a un año. No hay ninguna razón para que aquí, donde el número de afectados es mayor, el plazo se reduzca a treinta días. La consecuencia debe recaer sobre el SENDER ID o la plantilla responsable, sin arrastrar a los demás, y, cuando haya usuarios afectados, debe aplicarse la transición de seis meses a un año, preservando la continuidad del tráfico crítico.

2.8. Suspensión temporal durante el trámite (parágrafo 2 del artículo 6.4.3.2)

El parágrafo permite suspender el código hasta por seis meses mientras se tramita la actuación por las causales de los numerales 6.4.3.2.5 y 6.4.3.2.6. Una suspensión de esa duración, adoptada antes de cualquier decisión de fondo, equivale a sancionar de manera anticipada. Para cuando se resuelva si hubo o no infracción, la operación del integrador y la de sus clientes ya habrán sufrido un daño difícil de revertir. El efecto es todavía más desproporcionado si se considera que ambas causales se relacionan con conductas de terceros o con el contenido, frente a las cuales el integrador no es responsable. Una medida cautelar de esta gravedad solo puede proceder con prueba sumaria seria, mediante decisión motivada, por el término estrictamente necesario y de manera proporcional, y nunca cuando la causal se funde en conductas atribuibles a terceros.

Para dar coherencia a todo lo anterior, el artículo 6.4.3.2 debería incluir una regla expresa de imputación: la recuperación del código corto A2P solo procede por conducta propia, directa, comprobada y atribuible a su asignatario, y no por el uso indebido que hagan terceros ni por el incumplimiento de obligaciones que la resolución asigna al PRSTM, al validador, al asignatario del SENDER ID, al originador o a cualquier otro agente.

3. El esquema de plantillas es una censura previa del contenido y debe sustituirse por la identificación del originador

Los artículos 6.13.4.1, 6.13.4.3 y 6.13.4.7.2 condicionan el envío de cada mensaje a que su contenido cuente con una plantilla previamente aprobada, y obligan al operador a bloquear el mensaje que no la tenga. Llamemos las cosas por su nombre: esto es revisar y autorizar el contenido antes de que se transmita, es decir, una censura previa. El artículo 20 de la Constitución garantiza a toda persona el derecho a recibir información, y ese derecho no admite autorización ni revisión previa por parte del Estado o de un particular. En un servicio básico de telecomunicaciones, impedir que el usuario reciba un mensaje por el solo hecho de que su contenido no fue aprobado de antemano es una restricción que la Constitución no permite.

La jurisprudencia constitucional es clara y consistente. La Corte ha sostenido que sobre la información solo caben controles posteriores y nunca previos (Sentencia C-488 de 1993), y que los intermediarios no tienen el deber ni la facultad de revisar el contenido antes de su difusión, porque hacerlo equivaldría a una censura proscrita (Sentencia T-121 de 2018). A ello se suma el bloque de constitucionalidad: el artículo 13 de la Convención Americana sobre Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos prohíben la censura previa y protegen tanto el derecho a difundir como el derecho a recibir información.

La forma más clara de ver el problema es con un ejemplo. Exigir que cada mensaje tenga una plantilla aprobada antes de enviarse es equivalente a que una autoridad pretendiera revisar y aprobar una noticia antes de publicarla, un mensaje en redes sociales antes de difundirlo o un anuncio antes de que circule. Nadie aceptaría ese esquema para la prensa o para las redes, y no hay razón para aceptarlo en el SMS. La CRC no puede convertirse en validador previo del contenido de los mensajes, ni puede trasladar esa función a los operadores o a los validadores privados. Su finalidad legítima es otra y más sencilla: lograr que el usuario sepa quién le está escribiendo, para que decida por sí mismo si confía en lo que recibe. La regulación debe enfocarse en identificar al originador, no en aprobar el contenido.

La identificación del originador no solo es la opción constitucionalmente correcta, también es la única viable técnicamente. El identificador del originador viaja de forma nativa en el campo de origen del mensaje, de modo que verificar quién envía es perfectamente posible. En cambio, revisar el contenido de cada mensaje para compararlo con una plantilla no tiene soporte técnico a la velocidad y el volumen del tráfico nacional. La regulación estaría exigiendo un control que, además de constituir censura, no se puede ejecutar.

La alternativa que proponemos es un esquema de identificación y marcación. El validador realiza el conocimiento y la verificación del cliente, bajo la denominación que use el proyecto. Cuando el originador, PCA o remitente ha sido validado, sus mensajes se entregan con un SENDER ID certificado, que le indica al usuario que se trata de una fuente verificada. Cuando el mensaje no cuenta con un SENDER ID validado, no se bloquea ni se deja a criterio del operador: se entrega al usuario con una marcación obligatoria, visible y clara que advierte que el originador no ha sido validado. Así el usuario recibe siempre la información y decide con base en ella, exactamente como ocurre en la voz, donde la llamada sospechosa entra y se muestra una etiqueta en pantalla. Este modelo, además, resuelve el problema de las aplicaciones extranjeras sin sede en el país, que podrían cursar su tráfico bajo la marca de originador no validado mientras completan su verificación, en lugar de quedar excluidas por completo. En consecuencia, debe eliminarse la aprobación previa de plantillas como condición de envío y reemplazarse por este esquema, modificando en ese sentido los artículos 6.13.4.1 y 6.13.4.7.2.

4. Otras observaciones

Quien financia el validador debe participar en su gobierno. El artículo 18 deja la selección del validador en manos de los operadores, mientras que el artículo 6.13.1.2 traslada su financiación a los asignatarios de código corto A2P. El resultado es que quien paga no decide, porque ni elige al proveedor ni interviene en la tarifa que tendrá que asumir. Esa separación entre quien soporta el costo y quien toma la decisión es una fuente previsible de sobrecostos. Los asignatarios de código corto A2P deben tener voz y voto en la selección del validador y en la fijación y revisión de su tarifa, con un tope y con costos verificables.

Las decisiones del comité no pueden crear obligaciones por fuera de control. El numeral 6.13.5.1.11 vuelve obligatorias decisiones técnicas del Comité Técnico de Seguimiento recogidas

en actas que, según el mismo proyecto, no son actos administrativos ni admiten recursos, y el artículo 16 exceptúa de publicación algunas resoluciones. Por esa vía se imponen cargas sin acto motivado, sin publicidad y sin posibilidad de impugnación, lo que desconoce el debido proceso. Toda obligación nueva debe nacer de un acto administrativo motivado, publicado y susceptible de recursos, y la excepción de publicación debe limitarse a lo estrictamente técnico.

5. Seguridad jurídica y control judicial

Las observaciones anteriores no son reparos de forma. En conjunto, las medidas comentadas comprometen la igualdad, el debido proceso, la libertad de información y la libre competencia, entregan a un operador dominante un instrumento de abuso de posición dominante y desbordan el marco de la Ley 1341 de 2009 y el régimen de acceso e interconexión. Una resolución con estos contenidos no resistiría el control judicial. Si se expide en los términos actuales, será demandada en nulidad ante la jurisdicción de lo contencioso administrativo, sin perjuicio de las actuaciones que correspondan ante la autoridad de competencia. Confiamos en que la Comisión acoja las correcciones aquí planteadas y ajuste el proyecto antes de su expedición.

Atentamente,



Firmado digitalmente por
Diego Damian Valdivieso
Pinilla
Fecha: 2026.06.23 23:25:44
-05'00'

Diego Damian Valdivieso Pinilla
Apoderado General

Con Copia:

Cielo Elaine Rusinque Urrego
Supertendente de Industria y Comercio
superintendente@sic.gov.co

Gregorio Eljach Pacheco
quejas@procuraduria.gov.co
Procurador General de la Nación

Carina Murcia Yela
minticresponde@mintic.gov.co
Ministerio TIC

Gustavo Petro Urrego
contacto@presidencia.gov.co
Presidente de la República de Colombia