De: CRISTIAN CAMILO CANTILLO <cristiancamilocantillo445@gmail.com>
Enviado: martes, 16 de junio de 2026 8:43 p. m.
Para: atencioncliente <atencioncliente@crcom.gov.co>
Asunto: DERECHO DE PETICIÓN

Señores: COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC) E. S. D.

ASUNTO: DERECHO DE PETICIÓN EN INTERÉS GENERAL Y TÉCNICO (Art. 23 C.P. y Ley 1755 de 2015). REFERENCIA: Observaciones, comentarios y cuestionamiento técnico-jurídico al Proyecto de Resolución *"Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles"*.

de manera respetuosa comparezco ante ustedes con el fin de ejercer formalmente el DERECHO CONSTITUCIONAL DE PETICIÓN EN INTERÉS GENERAL, de acuerdo con lo previsto en el Artículo 23 de la Constitución Política de Colombia, en concordancia con los Artículos 13 y siguientes del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA - Ley 1437 de 2011, sustituido por la Ley 1755 de 2015).

El objeto de la presente solicitud es formular de manera formal y motivada una serie de observaciones, comentarios y un cuestionamiento técnico-jurídico indispensable para la debida motivación del Proyecto de Resolución de la referencia, con el fin de que las respuestas emitidas por este regulador sean incorporadas de forma explícita en la Matriz de Respuestas a Comentarios y en el correspondiente Análisis de Impacto Normativo (AIN).

A continuación, sustento la petición bajo las siguientes preguntas técnicas:

Bloque 1: Delimitación Conceptual del Tráfico A2P vs. Comunicaciones Propias del Operador

1. ¿Cómo define la Comisión el tráfico A2P cuando el originador es el propio Operador de Servicios de Telecomunicaciones (PRM u OMV) utilizando numeración móvil convencional de diez (10) dígitos (MSISDN)? Si el operador envía notificaciones regulatorias, de facturación o de servicio al cliente a sus propios usuarios desde su plataforma interna, ¿este tráfico será tipificado y tasado como A2P comercial, o mantendrá la condición de comunicación de red/servicio?
2. En el evento en que un operador no utilice códigos cortos (números de 5 o 6 dígitos) sino numeración móvil ordinaria para interactuar con sus usuarios de manera automatizada: ¿Estas líneas telefónicas móviles convencionales deberán registrarse obligatoriamente ante el Validador Centralizado bajo la figura de *Sender ID*? De ser afirmativo, ¿cómo se garantizará que los sistemas de filtrado de los operadores de red no bloqueen de forma errónea este tráfico legítimo bajo la sospecha de *proceder de una línea móvil personal*?

Bloque 2: Aplicación del Sistema de Plantillas y Validación Previa

3. ¿Estarán las comunicaciones operativas, regulatorias y de servicio al cliente de los propios operadores (PRM y OMV) sujetas a la aprobación previa de plantillas ante el Validador Centralizado? De ser así, ¿cómo planea la CRC mitigar el impacto en la inmediatez de las comunicaciones de emergencia, alertas de fraude en tiempo real para el usuario o suspensiones de servicio, si estas dependen de un proceso de aprobación exante por parte de un tercero?
4. Frente al principio de neutralidad de red y la naturaleza del negocio OMV: Si un OMV utiliza la infraestructura de mensajería de su operador anfitrión para enviar notificaciones de red a sus usuarios desde números móviles ordinarios, ¿el operador anfitrión tendrá la facultad regulatoria de inspeccionar, filtrar o rechazar este contenido bajo el argumento de "mitigación de fraude", afectando la relación comercial directa del OMV con su cliente?

Bloque 3: Impacto Económico y Doble Imposición de Cargas

5. ¿El envío de mensajes de texto (SMS) informativos propios del operador a su base de usuarios generará el pago de tasas o contraprestaciones económicas a favor del Validador Centralizado? Exigir un pago por validar las comunicaciones obligatorias que la misma regulación de la CRC (RPU - Régimen de Protección de Usuarios) le impone al operador (como avisar la fecha de corte o el consumo de datos), ¿no configuraría una doble carga económica desproporcionada para el prestador del servicio?

Bloque 4: Exclusión de Canales Propios de Mensajería, Mensajería In-App y Notificaciones de Red

1. ¿Cuál es el ámbito de aplicación de la resolución frente a los canales propios y cerrados de mensajería del operador (tales como notificaciones *Push* integradas en la App oficial, servicios de mensajería por Applets/STK en la SIM card, o protocolos RCS propios)? Dado que estas comunicaciones no transitan por el canal tradicional de mensajería mayorista SMS A2P de interconexión, sino que viajan cifradas sobre la red de datos del operador hacia su propia base de usuarios, ¿quedan estos canales completamente excluidos de las obligaciones de validación previa, registro de *Sender ID* y uso de plantillas?
2. De no estar excluidos, ¿bajo qué facultad legal la CRC pretende regular el contenido y el envío de notificaciones internas de aplicaciones de software privadas del operador? ¿No consideraría la Comisión que imponer la validación previa de plantillas a las notificaciones *Push* o mensajes *In-App* de un operador constituiría una vulneración flagrante al principio de Neutralidad Tecnológica (Ley 1341 de 2009) y una intervención desproporcionada en la libertad de empresa y el desarrollo de software nativo?
3. Frente a la arquitectura del Validador Centralizado: Si un OMV decide mitigar el fraude de manera autónoma migrando todas sus comunicaciones informativas y transaccionales legítimas a su propio canal digital (App móvil o mensajería web propia), ¿garantizará la CRC que este tráfico de datos no sea inspeccionado, catalogado como "fraude" o bloqueado por el operador de red anfitrión bajo el pretexto de que *no pasó por el Validador Centralizado*?

Bloque 5: Régimen de Responsabilidad por "Falsos Positivos" (Bloqueos Erróneos de Tráfico Legítimo)

El sistema automatizado o el Validador Centralizado van a cometer errores y bloquearán mensajes legítimos (por ejemplo, un código de verificación OTP para que un usuario entre a su banca móvil o un aviso de suspensión de servicio). ¿Quién responde por los daños económicos al usuario o al operador?

1. ¿Cuál será el régimen de responsabilidad administrativa y civil aplicable al Validador Centralizado o al Operador de Red en caso de la ocurrencia de "falsos positivos" (bloqueo erróneo de tráfico legítimo)? Si por una falla en el sistema de plantillas o un error del Validador se suspende el envío de mensajes transaccionales críticos de nuestros usuarios,

afectando la continuidad de su negocio, ¿asumirá la CRC o el Validador los costos por los perjuicios causados, o se pretende trasladar dicho riesgo patrimonial al operador que originó el tráfico?

2. ¿Cuál será el procedimiento perentorio y el tiempo máximo de resolución (SLA) para que un operador pueda apelar y reactivar un *Sender ID* o una plantilla que haya sido bloqueada por sospecha errónea de fraude? Exigimos que la norma no dé un cheque en blanco para bloquear preventivamente de forma indefinida; el debido proceso exige un mecanismo de reactivación en tiempo real (máximo en minutos, no en días hábiles) para no quebrar la operación comercial.

Bloque 6: Ciberseguridad y Propiedad Intelectual en el Sistema de Plantillas

Para que el Validador Centralizado apruebe una plantilla, el operador tiene que "mostrarle" el texto del mensaje. Ahí viaja el core del negocio del operador (estrategias de marketing, copy creativo, ofertas comerciales antes de lanzarlas al mercado).

3. ¿Qué protocolos de ciberseguridad y confidencialidad se le exigirán al Validador Centralizado para garantizar que la base de datos de "plantillas preaprobadas" no sea vulnerable a filtraciones o espionaje industrial? Dado que las plantillas contienen las estrategias comerciales, de fidelización y de precios de los operadores antes de ser enviadas al mercado, ¿cómo garantizará la CRC que el personal del Validador Centralizado (o terceros competidores) no tenga acceso a esta información privilegiada y sensible para el mercado competitivo?

Bloque 7: Costos de Conectividad e Interoperabilidad Técnica

4. ¿Los costos asociados al desarrollo de software, APIs de integración, mantenimiento y servidores necesarios para conectarse en tiempo real con el Validador Centralizado serán asumidos en su totalidad por el tercero que opere el Validador, u obligarán a cada operador a realizar estas inversiones de su propio bolsillo? De ser esto último, ¿ha evaluado la CRC si este costo de implementación fija genera una barrera de entrada desproporcionada para los operadores de menor escala (OMV) en comparación con los grandes operadores establecidos?

5. ¿Qué estándar tecnológico de interoperabilidad (ej. protocolos HTTP REST API, SMPP, etc.) utilizará el Validador Centralizado? Se solicita que la CRC defina desde la resolución un estándar abierto, público y neutral, de modo que no se obligue a los operadores a adquirir software de marcas o proveedores específicos para poder cumplir con la norma.