



RESOLUCIÓN No. **6218** DE 2021

*"Por la cual se resuelve la solicitud de autorización de terminación de la relación de acceso e interoperabilidad para el envío de mensajes cortos de texto SMS entre **COMUNICACIÓN CELULAR S.A** y **HABLAME COLOMBIA S.A.S E.S.P.** **EXP.3000-32-2-3**".*

## **LA SESIÓN DE COMISIÓN DE COMUNICACIONES DE LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES**

En ejercicio de sus facultades legales y en especial las que le confiere el artículo 22 de la Ley 1341 de 2009, y la Resolución CRC 5050 de 2016 y,

### **CONSIDERANDO**

#### **1. ANTECEDENTES**

Mediante comunicación 2019303006 del 3 de septiembre de 2019, **COMUNICACIÓN CELULAR S.A.**, en adelante **COMCEL**, puso en conocimiento de la Comisión de Regulación de Comunicaciones -CRC- el presunto incumplimiento por parte de **HABLAME COLOMBIA S.A.S E.S.P.**, en adelante **HABLAME**, de las obligaciones pactadas en virtud del Contrato de Acceso e Interoperabilidad para el envío de mensajes cortos de texto SMS<sup>1</sup>, con ocasión del uso de 12 códigos cortos para el envío de mensajes con contenido aparentemente fraudulento. Con fundamento en lo anterior, solicitó autorización a la CRC para la terminación del referido contrato de acceso.

El 22 de octubre de 2019, la CRC a través de comunicación 2019525480 solicitó a **COMCEL** información adicional sobre los códigos cortos mencionados en su solicitud, con el fin de determinar las acciones a seguir por la Comisión respecto de los mismos por su naturaleza de recursos escasos, frente a lo cual, **COMCEL** el 18 de noviembre de 2019 mediante respuesta 2019303974, reiteró y amplió la información dada en la comunicación del 3 de septiembre, indicando además que la recuperación de códigos cortos no solucionaba la situación que motivó su solicitud.

Posteriormente, **COMCEL** el 9 de diciembre de 2019 mediante radicado 2019304280, dio alcance a la comunicación del 18 de noviembre, reiterando que la recuperación de códigos cortos no solucionaba la situación que se presentaba con **HABLAME** en el marco de la relación de acceso.

Por otra parte, la CRC mediante comunicación 2019530096 del 24 de diciembre de 2019, puso en conocimiento de **HABLAME** la solicitud de **COMCEL** para que se pronunciara sobre la misma, sin respuesta identificada a la fecha.<sup>2</sup>

<sup>1</sup> Contrato No. 29966 de 2017.

<sup>2</sup> De conformidad con el numeral 6 del artículo 20 de la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, los términos de las actuaciones administrativas de competencia de la Sesión de Comisión de Comunicaciones de la CRC que se encontraban en curso, se suspendieron desde la entrada en vigencia de la Ley 1978 y hasta el 3 de febrero de 2020, fecha en la cual quedó conformada la referida Sesión de Comisión.

El 6 de mayo de 2020, a través del radicado 2020804472, **COMCEL** reiteró su solicitud bajo los mismos argumentos, y manifestó que pese a las diversas comunicaciones dirigidas a **HABLAME**, persistían los envíos de mensajes con contenido presuntamente fraudulento, relacionando los códigos cortos desde donde salían y las fechas de los envíos.

El 14 de mayo de 2020, mediante radicado 2020510015, la CRC envió, por un lado, comunicación a **COMCEL** solicitando que informara si la relación entre las partes podía estar menoscabando la red o los servicios que se proveen, o si a la fecha se presentaba alguna potencial deficiencia o incumplimiento de requisitos técnicos en la relación de acceso. Por otro lado, se requirió nuevamente a **HABLAME** para que se pronunciara sobre la solicitud de autorización para la terminación de la relación de acceso interpuesta por **COMCEL**, sin obtener respuesta del PCA.

En la respuesta bajo radicado 2020808523 presentada por **COMCEL** el 3 de agosto de 2020, éste reiteró los argumentos expuestos en anteriores comunicaciones, respuesta de la cual se corrió traslado a **HABLAME**.

Mediante comunicación del 11 de agosto de 2020, radicada internamente bajo el número 2020808915, y reiterando los argumentos expuestos en las comunicaciones antes relacionadas, **COMCEL** solicitó a la CRC adoptar las medidas necesarias para que **HABLAME** garantizara el cese de las acciones que a su consideración desencadenaban en el incumplimiento del contrato de Acceso e Interoperabilidad para el envío de mensajes cortos de texto SMS, y que en caso de que ello no sucediera, se facultara a **COMCEL** para proceder a la desconexión inmediata de la referida relación de acceso. Todo lo anterior, invocando la aplicación del artículo 4.1.7.5 de la Resolución 5050 de 2016.

Una vez más, esta Comisión, mediante radicado de salida 2020515853 de fecha 18 de agosto de 2020, remitió a **HABLAME** copia de la solicitud presentada por **COMCEL** para que presentara sus consideraciones en un término de diez (10) días hábiles. En esta oportunidad, **HABLAME** respondió la referida comunicación, mediante escrito del 24 de agosto de 2020, radicado bajo el número 2020809578. Posteriormente, **HABLAME** complementó su respuesta mediante comunicación bajo radicado 2020301189 del 2 de septiembre de 2020.

En su respuesta, **HABLAME** sustentó las razones con fundamento en las cuales considera no estar incurriendo en incumplimiento contractual alguno, así como las medidas que ha adoptado para contrarrestar y mitigar el envío de mensajes con contenido presuntamente fraudulento a través de los códigos cortos asignados.

En desarrollo de los análisis requeridos para dar trámite a la solicitud de **COMCEL**, se identificó la necesidad de remitir a éste las comunicaciones allegadas por **HABLAME** el 24 de agosto y el 2 de septiembre de 2020, para que presentara sus consideraciones, según consta en radicado 2020518362 del 23 de septiembre de 2020. Lo anterior, teniendo en cuenta además que mediante comunicación 2020810343, **COMCEL** solicitó copia de las actuaciones adelantadas dentro del trámite de autorización de desconexión desde el 18 de agosto de 2020.

A su vez, mediante comunicación del 2 de octubre de 2020 bajo radicado 2020811614, **COMCEL** solicitó la complementación de la documentación remitida por **HABLAME**, manifestando que no le había sido posible descargar algunos de los anexos de la respuesta de éste. Por lo anterior la CRC procedió a requerir a **HABLAME** para que remitiera nuevamente los documentos faltantes, los cuales fueron allegados a la Comisión el 16 de octubre de 2020 mediante comunicación bajo radicado 2020812274.

Los anexos en comento fueron remitidos a **COMCEL** el 26 de octubre de 2020 mediante comunicación con radicado 2020812274. Finalmente, y como consta en el radicado 2020813564 del 10 de noviembre de 2020, **COMCEL** se pronunció integralmente sobre lo manifestado por **HABLAME** en relación con la solicitud de autorización para la terminación del contrato de acceso e interoperabilidad entre ellos celebrado.

## **2. ARGUMENTOS DE LAS PARTES**

### **2.1. ARGUMENTOS DE COMCEL**

Como se anticipó en el acápite anterior, **COMCEL** solicitó ante esta Comisión, que en caso de persistir los presuntos incumplimientos contractuales por parte de **HABLAME** en el marco de su

contrato de acceso e interoperabilidad No. 29966 de 2017<sup>3</sup>, se le autorizara a dar por terminado el mismo, y en consecuencia proceder de manera inmediata a la desconexión material.

Como sustento de la anterior solicitud, **COMCEL** adujo que **HABLAME** ha incumplido reiteradamente sus acuerdos de acceso, **(i)** al no controlar el contenido presuntamente fraudulento que circula por medio de los mensajes cortos de textos SMS que circulan bajo los códigos cortos asignados por la CRC, y **(ii)** por negarse a actualizar las condiciones de la garantía contractual.

Sobre el primer punto, **COMCEL** manifestó que desde el 2019 ha identificado en repetidas oportunidades mensajes de presunta procedencia engañosa o fraudulenta, cuyo fin al parecer era el de propiciar que los usuarios suministraran información financiera confidencial. A modo de ejemplo, mencionó que recibió queja de un usuario donde informaba que, como cliente de Bancolombia, recibió un mensaje de texto donde se le invitaba a relevar información financiera y sensible a través del diligenciamiento de un formulario que con posterioridad lo redirigía a una página web con un dominio distinto al de Bancolombia.

Así mismo, expuso que en su momento, se informó a **HABLAME** que a partir de incidentes como el anteriormente descrito, se realizó una validación de tráfico, evidenciando que a través del código 890018 se había enviado un mensaje igual al descrito, a nombre de varias entidades financieras, y que sobre el particular, **HABLAME** sólo había manifestado que el contenido de los mensajes era generado por sus usuarios y no por la compañía.

Manifestó que durante la comunicación cruzada con **HABLAME** siempre se le puso de presente que en virtud de lo establecido en el contrato, el PCA es directa y exclusivamente responsable de garantizar la adecuada prestación del servicio, así como "*de la información transportada a través de los mensajes cortos de texto SMS que se origine para ser enviado a los usuarios móviles y de COMCEL.*", y que pese a que **HABLAME** manifestó haber adoptado medidas tendientes a la prevención de conductas fraudulentas, dichas medidas no resultaban idóneas ni eficaces dado que persistían este tipo de inconvenientes.

Mencionó haber evidenciado que los días 16 y 17 de agosto de 2019, **HABLAME** envió 68.558 mensajes desde 12 códigos cortos<sup>4</sup> hacia móviles de la red de **COMCEL** con mensajes contentivos de ataques tipo phishing vía SMS, sobre los cuales recibió quejas de parte de Davivienda y algunos de sus usuarios, cifras que en cada comunicación de **COMCEL** reportaban un significativo aumento.

Como factor común en las comunicaciones del solicitante, se encontraron referencias y citas de las disposiciones contractuales en virtud de las cuales alega que **HABLAME** es responsable de la información transportada a través de los mensajes cortos de texto SMS que origine para ser enviados a los usuarios de móviles de **COMCEL**, y en general, todas las condiciones contractuales que a su consideración han sido incumplidas por parte del PCA. Sobre el particular, hizo especial énfasis en que **HABLAME** ha incumplido el Catálogo de Prácticas Prohibidas establecido en el contrato, al no implementar sistemas de seguridad o medidas correctivas suficientes e idóneas para mitigar eventos fraudulentos, lo cual, a su consideración, también contraviene lo establecido en la Resolución CRC 5050 de 2016 sobre la prevención de fraudes.

Mencionó a lo largo de sus comunicaciones que entre enero y abril de 2020, evidenció más de 764.000 mensajes con contenido presuntamente fraudulento enviados desde 17 códigos cortos asignados a **HABLAME** y que como medida preventiva a su cargo, se abstuvo de entregar a los usuarios finales, los mensajes provenientes de los códigos cortos asignados al PCA.

Indicó que con ocasión de los hechos antes relatados, el 17 de abril de 2020 se llevó a cabo un Comité Mixto de Acceso y un Subcomité Técnico del Contrato de Acceso, donde se socializó nuevamente el posible uso del código 899991 para fines fraudulentos. Así mismo, con el fin de hacer énfasis en la falta de diligencia de **HABLAME** para prevenir el uso fraudulento de los códigos cortos que le fueron asignados, **COMCEL** mencionó que el 23 de abril de 2020, se detectó un nuevo mensaje con posible contenido de fraude bancario, proveniente del código 899440, indicando además que una vez se le informó al PCA, éste procedió al bloqueo del mensaje.

<sup>3</sup> El contrato sobre el cual versa la solicitud de COMCEL tiene por objeto: "(...) establecer las condiciones técnicas, comerciales, financieras, operativas y jurídicas que regirán el acceso del PCA en su calidad de Proveedor de Contenidos y Aplicaciones (PCA) a la red de telefonía móvil celular de COMCEL para el envío de mensajes de texto SMS a los usuarios de la red de COMCEL y de otros PRST si así fue definido por las partes, de conformidad con los términos y con los alcances que para el efecto fija la ley y la regulación vigente."

<sup>4</sup> 890001, 890005, 890007, 890008, 890018, 890024, 890025, 890026, 899400, 899410, 899420 y 899300

Puso de presente que, a partir del seguimiento realizado durante el mes de mayo de 2020, evidenció el registro de 12.679 envíos de mensajes de texto SMS con potencial contenido de fraude bancario desde distintos orígenes correspondientes a códigos cortos de **HABLAME**, frente a lo cual éste nuevamente manifestó adoptar controles que, a consideración de **COMCEL**, no han resultado efectivos.

Mencionó que siempre ha sido **COMCEL** quien ha detectado e informado al PCA la circulación de SMS presuntamente fraudulentos, y que el mismo **HABLAME** reconoció en su comunicación la ocurrencia de ese tipo de situaciones, por lo que concluye que ello denota su falta de diligencia para prevenir y proteger a los usuarios de ser víctimas de conductas fraudulentas. De igual forma, afirmó que lo anterior constituye el incumplimiento de **HABLAME** de lo pactado en el contrato de acceso y de la regulación general, vigente sobre la materia.

De todo, se destaca que en cada comunicación, **COMCEL** reportaba significativos incrementos de la cifra de mensajes presuntamente fraudulentos, aparentemente circulados a través de los códigos cortos asignados a **HABLAME**, y el especial énfasis que hizo en que las conductas omisivas del PCA, tales como, la falta de controles de seguridad idóneos y eficaces, generan riesgos significativos al patrimonio e integridad de los usuarios, así como a la reputación de **COMCEL**, pues para los usuarios, el generador de los mensajes es el operador móvil con quien suscribieron su contrato, desconociendo que en realidad es generado a través de un código corto administrado por un PCA, en este caso, **HABLAME**. A partir de lo anterior, concluyó que se está desnaturalizando la finalidad y utilidad para las cuales fue concebido y celebrado el contrato de acceso.

En cuanto al incumplimiento o deficiencia de requisitos técnicos de la relación de acceso, **COMCEL** adujo el incumplimiento contractual de **HABLAME** al no responsabilizarse por el contenido de la información transportada y cita varias cláusulas del contrato que a su consideración se están viendo vulneradas, entre éstas, las concernientes a la implementación de sistemas de seguridad y el uso de firewall.

Así mismo, trajo a colación las disposiciones regulatorias concernientes a la responsabilidad sobre el contenido de mensajes de texto, para manifestar que de acuerdo con la misma, los PRST podrán imponer restricciones a contenidos de otros proveedores cuando por disposición legal, reglamentaria o regulatoria, éstos estén prohibidos o restringidos.

Adicionalmente, y frente al argumento expuesto por **HABLAME** sobre la efectividad de sus medidas preventivas y la presunta disminución del tráfico de mensajes fraudulentos, **COMCEL** afirmó que el cumplimiento de lo pactado en el contrato y de la regulación debe ser cabal y permanente y no parcial o excepcional.

Finalmente, expuso que **HABLAME** también ha incumplido lo pactado en su contrato de acceso, al no actualizar las condiciones, especialmente, el valor del amparo de la garantía contractual que cubre el cumplimiento del mismo, y que la actualización del valor amparado realizada en el mes de agosto de 2020, se calculó con base en el tráfico cursado en 2019, por lo cual solicitaría nuevamente su ajuste.

## **2.2. ARGUMENTOS DE HABLAME**

Pese a los reiterados traslados y requerimientos que se hicieron a **HABLAME** para que se pronunciara sobre la solicitud de autorización de desconexión presentada por **COMCEL**, el PCA sólo se pronunció sobre el particular hasta agosto de 2020.

**HABLAME** centró sus argumentos en que no ha incurrido en los incumplimientos contractuales aducidos por **COMCEL**, y que por el contrario, ha adoptado los controles de seguridad necesarios para mitigar que los códigos cortos que tiene asignados sigan siendo usados con fines fraudulentos.

Al respecto manifestó que, si bien es cierto lo afirmado por **COMCEL** sobre el uso de códigos cortos para el envío de mensajes con contenido presuntamente fraudulento, no es cierto que dicha circunstancia haya sido solo detectada y afrontada por **COMCEL**.

Indicó que **COMCEL** reportó en su solicitud 12 códigos cortos, dando a entender que todos correspondían a **HABLAME**, omitiendo mencionar que varios de ellos estaban asignados a otros PCA e incluso a PRST, mencionando a Colombia Móvil, y que tal circunstancia denota que el uso de

códigos cortos para fines presuntamente fraudulentos es una problemática que afecta a diferentes entidades del sector y no sólo a **HABLAME**.

Adujo que **COMCEL** contravino la regulación general en materia de acceso, al bloquear códigos cortos arbitrariamente sin estar facultado para ello, y que dicho proceder afecta a miles de usuarios, dado que por esos códigos cursan contenidos de miles de clientes.

Afirmó que la cláusula del contrato que establece que al "PCA" le corresponde "responsabilizarse por la información transportada" hace referencia a la obligación de transportar un SMS enviado por un cliente de **HABLAME**, sin que de modo alguno éste genere su contenido o deba responsabilizarse del mismo.

Aseguró que, contrario a lo afirmado por **COMCEL**, **HABLAME** no ha incurrido en "Prácticas Prohibidas", sino que, por el contrario, las combate y realiza permanentemente acciones para detectar, combatir y controlar los SMS con contenido presuntamente fraudulento y que dichos procedimientos han resultado efectivos, en la medida que el porcentaje de este tipo de mensajes para el 2020 en promedio fue sólo del 0.157%.

Adicionalmente, y como medidas adoptadas para mitigar las conductas fraudulentas ya descritas, **HABLAME** mencionó la implementación de una herramienta y campañas de control de fraude, SMS de alerta dirigidos a los usuarios para que no accedan a links sospechosos, que se ha solicitado apoyo del grupo de Ciberseguridad de las entidades financieras como Bancolombia, que cuenta con un Sistema de Gestión Integral SGI certificado bajo las Normas ISO 9001, ISO 14001, ISO 18001, ISO 27001 SEGURIDAD DE LA INFORMACIÓN, que tiene establecida una "lista negra" de alrededor de palabras 1.460<sup>5</sup>, cuyo objetivo principal es realizar el filtro, control y bloqueo de palabras a los contenidos previo al envío de éstos, que la misma es alimentada y actualizada diariamente y cuenta con palabras claves como los nombres de las entidades financieras, gubernamentales, departamentales y demás que puedan ser suplantadas con fines fraudulentos.

Así mismo, mencionó que ha fortalecido su planta de personal en el área de control de fraude, que hace revisión manual 24/7 como complemento de su herramienta de control. Haciendo referencia a sus mecanismos de control, describió que en el momento en que detecta un SMS con contenido presuntamente fraudulento por cualquier ruta de atención, procede a realizar lo establecido en el Tratamiento y Reporte De Incidentes De Fraude (MEJ-INS-017):

- "a. Notificar mediante el grupo interno Control Fraude a todos los interesados.*
- b. Bloquear de inmediato el contenido en la herramienta de control fraude, como la cuenta asociada con este hecho.*
- c. En caso de que el intento de presunto fraude sea bancario, notificar mediante correo electrónico al contacto asociado al grupo de ciberseguridad de la entidad financiera.*
- d. En caso de que el posible fraude contenga un link sospechoso, se debe notificar a la PONAL de manera inmediata. Este reporte estará a cargo del Director de Calidad. Infraestructura generará diariamente el listado de los Links de posible fraude.*
- e. Reporte en Google: el Director de Calidad una vez reciba la notificación del posible Link de riesgo reportará en el Safe Browsing de Google.*
- f. El área de Control fraude procederá a realizar el respectivo reporte ante los ISP pertinentes".*

Aclaró entonces que **HABLAME** no solo bloquea los SMS, sino que reporta las URL's que son a su parecer, la principal fuente de fraude tipo phishing.

Como medidas adicionales de control, mencionó una herramienta de control de fraude con varios filtros de control de seguridad la cual es vigilada 24/7 por su área técnica; SMS de alerta que son remitidos de manera automática a los usuarios cuando se detecta riesgo de fraude; campañas de control de fraude que adelanta su área de *Marketing and Advertising* a través de redes sociales; un directorio activo de contactos de ciberseguridad con información de las entidades financieras, otros operadores y la Policía Nacional de Delitos Informáticos, para trabajar articuladamente ante los casos de fraude; controles de seguridad preestablecidos, como el bloqueo de palabras, ampliación del personal en el área de fraude, canales de atención, entre otras; y finalmente mencionó las denuncias ante la Fiscalía General de la Nación.

<sup>5</sup> De acuerdo con lo descrito por **HABLAME**, se puede inferir que se trata de un listado contentivo de las palabras de uso recurrente en el envío de mensajes con contenido presuntamente fraudulento.

Con todo, aseguró que contrario a lo expuesto por **COMCEL**, no ha incurrido en incumplimiento de los preceptos contractuales invocados, y que por el contrario, ha mostrado diligencia en la adopción de medidas para la prevención de fraude a los usuarios y que ello se evidencia a partir de la disminución en la cifra de SMS fraudulentos transmitidos desde códigos cortos asignados **HABLAME** y a través de la red de **COMCEL**.

En lo referente al incumplimiento de la obligación contractual de actualizar de la garantía, mediante comunicación del 2 de septiembre de 2020, allegó a esta Comisión la correspondiente actualización, la cual a su vez fue remitida a **COMCEL** para su conocimiento y fines pertinentes.

### **3. CONSIDERACIONES DE LA CRC**

Como se pudo observar en el contexto fáctico anteriormente expuesto, **COMCEL** y **HABLAME** celebraron un contrato de acceso en el cual se definen las condiciones técnicas, comerciales, financieras, operativas y jurídicas para que **HABLAME**, en calidad de PCA, acceda a la red de **COMCEL** para el envío de mensajes de texto SMS a los usuarios de la red de **COMCEL** y de otros PRST.

Así mismo, se tiene que **COMCEL** acudió a esta Comisión para solicitar que, en caso de persistir los presuntos incumplimientos contractuales por parte de **HABLAME** en el marco de esa relación de acceso, se le autorice a terminar la misma y proceder a la desconexión material automática.

Los argumentos del solicitante se concretan en que el reincidente incumplimiento de **HABLAME** de obligaciones contractuales sobre la implementación de controles de seguridad efectivos para prevenir el envío de contenidos fraudulentos a través de los mensajes de texto SMS que circulan por la red de **COMCEL**, genera riesgos significativos para los usuarios finales y para la reputación de su compañía.

Por su parte, **HABLAME** aduce que no ha incurrido en los referidos incumplimientos, que ha adoptado diversas medidas de seguridad que han resultado efectivas y que no afecta de modo alguno la red del PRST. Así mismo, alega el incumplimiento de **COMCEL** de la regulación general al bloquear algunos de sus códigos cortos sin tener la facultad para hacerlo y la consecuente afectación de miles de usuarios que envían mensajes de texto SMS a través de dichos códigos.

#### **3.1. ALCANCE DE LAS COMPETENCIAS DE LA CRC**

Previo a analizar de fondo la solicitud de **COMCEL**<sup>6</sup>, y considerando que la misma se sustenta en el presunto incumplimiento de obligaciones contractuales por parte de **HABLAME**, resulta necesario manifestar que, en lo que respecta a los posibles incumplimientos contractuales a los que hace alusión **COMCEL**, asociados a obligaciones de prevención de fraudes que puedan afectar a los usuarios, consignadas por las partes en el contrato acceso suscrito por las mismas, esta materia se circunscribe al resorte exclusivo del juez natural del contrato, a quien en efecto correspondería emitir juicios de valor en relación con conductas constitutivas de un posible incumplimiento contractual o de perjuicios indemnizables y, como consecuencia de ello, establecer las medidas respectivas, lo cual a su vez implica que tales asuntos claramente escapan de las competencias administrativas asignadas a esta Comisión por el legislador.

De igual forma, en cuanto a los incumplimientos regulatorios que mutuamente se han "imputado" las partes, es oportuno aclarar que la CRC no tiene competencia para pronunciarse sobre aspectos relativos a posibles infracciones al régimen de telecomunicaciones, razón por la cual copia de esta Resolución y del expediente administrativo será remitido al Ministerio de Tecnologías de la Información y las Comunicaciones- MinTIC, entidad a la que en virtud de lo dispuesto en el artículo 18, numeral 11 de la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, le corresponde ejercer las funciones de vigilancia y control en el sector de Tecnologías de la Información y las Comunicaciones.

<sup>6</sup> En este punto también vale la pena mencionar que, aunque **COMCEL** reiteró en varias oportunidades su solicitud de autorización de desconexión, lo cierto es que la CRC no contaba con elementos suficientes para analizar de fondo dicha solicitud, por un lado, debido a que **COMCEL** no sustentaba con claridad y suficiencia la afectación a su red o a los servicios que provee a **HABLAME** con ocasión de la relación de acceso; y por otro, debido a que entre el primer traslado que se corrió a **HABLAME** de la referida solicitud, y la fecha en que éste se pronunció sobre el particular, transcurrieron más de seis meses, periodo en el que la CRC instó en repetidas oportunidades a dicho proveedor a ejercer su derecho de defensa y contradicción.

Así mismo, y en atención a que **COMCEL** adujo de manera reiterada la eventual afectación de los usuarios por exposición de su información personal y sensible al uso de la misma para fines fraudulentos, se estima necesario remitir copia del expediente administrativo a la Superintendencia de Industria y Comercio- SIC, para que como entidad legalmente facultada para garantizar los derechos de los usuarios de telecomunicaciones y para ejercer la "vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales", adopte las medidas administrativas que estime necesarias. Lo anterior, de conformidad con lo dispuesto en el artículo 37 de la Ley 1978 de 2019 y el artículo 17 de la Ley 1266 de 2008<sup>7</sup>.

Precisado lo anterior, es importante dejar claridad sobre el alcance de las competencias legales atribuidas a esta Comisión en materia de acceso e interconexión de redes de telecomunicaciones, el cual está dado por la facultad de establecer requisitos o términos bajo los cuales los operadores utilizan las redes existentes o las instalaciones esenciales de cualquier otro operador de telecomunicaciones, términos dentro de los cuales sólo de manera excepcional se prevé la posibilidad de desconexión de las relaciones de acceso, previa autorización de la CRC. Sobre la posibilidad excepcional de desconexión, el artículo 4.1.7.5. de la Resolución 5050 de 2016 establece:

*"PROHIBICIÓN DE DESCONEJIÓN. Ninguna controversia, conflicto o incumplimiento de los acuerdos de acceso y/o de interconexión, podrá dar lugar a la desconexión de los proveedores, salvo que la CRC así lo autorice, en cuyo caso deberá dictar las medidas previas que se aplicarán con la finalidad de minimizar los efectos para los usuarios.*

*Mientras no se produzca esta autorización, las condiciones del acceso y/o la interconexión deben mantenerse y, por lo tanto, no puede limitarse, suspenderse o terminarse, so pena de que quién ejecutó, motivó o patrocinó la conducta, incurra en las sanciones previstas para el efecto en las normas correspondientes."*

Así mismo, la regulación en cita establece como causales de desconexión que la relación de acceso, uso e interconexión implique asumir una carga excesiva que la regulación no contempla en la medida en que la misma no cumpla satisfactoriamente con su función natural o represente afectaciones técnicas a alguna de sus partes, la no transferencia oportuna de saldos netos<sup>9</sup>, el mutuo acuerdo o que uno de los extremos de la relación se extinga o pierda la calidad de PRST.<sup>10</sup>

En el marco de lo anterior, se procederá a analizar si las condiciones fácticas, técnicas y jurídicas que concurren en el presente caso, constituyen razón suficiente para autorizar la terminación de la relación de acceso entre **COMCEL** y **HABLAME**, y su consecuente desconexión material.

En efecto, de la solicitud de desconexión elevada por **COMCEL** y los argumentos expuestos en cada una de sus comunicaciones, es posible evidenciar que éste, recibió de manera reiterada quejas de usuarios y de entidades financieras, en las que se ponían de presente el envío de mensajes de texto de contenido aparentemente fraudulento, a través de mensajes de texto SMS, que al parecer se generaban desde códigos cortos asignados por la CRC a **HABLAME**.

Se observa igualmente en el expediente administrativo que, **COMCEL** puso en conocimiento de **HABLAME** las referidas quejas y que, si bien éste afirma haber adoptado medidas de seguridad necesarias para mitigar tal situación, en cada nueva comunicación de **COMCEL**, se reportó un aumento significativo de mensajes con contenido presuntamente fraudulento, lo cual indica que, al parecer, dichas medidas no han resultado efectivas y suficientes para contrarrestar la problemática.

Por lo anterior, **COMCEL** afirma que se están generando riesgos significativos al patrimonio e integridad de los usuarios finales, así como a la reputación de la compañía, concluyendo que, con todo, se está desnaturalizando la finalidad y utilidad para las cuales fue concebido y celebrado el contrato de acceso.

Así mismo, y teniendo en consideración que la autorización de desconexión procede de manera excepcional, bien sea, por las causales de impago, mutuo acuerdo o extinción de un extremos de la relación de acceso, o cuando en el marco de una actuación administrativa se acredite que la

<sup>7</sup> Ley 1266 de 2008, Artículo 17.

<sup>8</sup> "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."

<sup>9</sup> Resolución 5050 de 2016. ARTÍCULO 4.1.7.6.

<sup>10</sup> Resolución 5050 de 2016.

relación de acceso o interconexión ya no cumple satisfactoriamente con su función natural o representa afectaciones técnicas a alguna de sus partes, la CRC requirió a **COMCEL**, en su calidad de solicitante de la desconexión, para que informara si la relación de acceso constituida con **HABLAME** podía estar menoscabando su red o los servicios que se proveen, o si a la fecha se presentaba alguna potencial deficiencia o incumplimiento de requisitos técnicos en la relación de acceso.

Frente a los anteriores cuestionamientos, en su respuesta bajo radicado 2020808523 del 3 de agosto de 2020, **COMCEL** se refirió a lo ya mencionado sobre incumplimiento de cláusulas contractuales, la afectación a la seguridad de los usuarios y a la reputación de su compañía. En lo concerniente a una deficiencia potencial o incumplimiento de requisitos técnicos en la relación de acceso materialmente entendida, sólo adujo dificultades relativas a la ausencia de un firewall, sin describir condiciones adicionales que sustentaran afectaciones a su red o sus servicios, en efecto, en dicha oportunidad manifestó: *"Que en términos del uso del firewall también se encontró que se está violando lo consagrado en el mencionado catálogo de prácticas prohibidas, respecto a las acciones que se deben implementar entre las partes para garantizar el cumplimiento del mismo, toda vez que en el mismo se establece que ambas partes deberán implementar sistemas de seguridad de manera no limitativa: "(i) firewall; (ii) filtros para verificar el contenido de Mensajes Cortos según políticas definidas anteriormente; (iii) filtros para detectar prácticas de flooding y Spamming (...)"(subraya y negrita fuera del texto)".*

Hasta este punto, y de acuerdo con lo argumentado por **COMCEL**, podría pensarse que **HABLAME** no contaba con las referidas medidas de seguridad, particularmente con un firewall, y que ello podía poner en riesgo la seguridad de la red de **COMCEL**, además de la de los usuarios. Sin embargo, en la comunicación 2020809578 del 24 de agosto de 2020, **HABLAME** manifestó que *"cuenta con una configuración rigurosa en su FIREWALL, así: a. Nuestro firewall cuenta con un listado de palabras y términos para bloquear cierto contenido en los SMS b. Nuestro firewall esta (sic) configurado para no permitir envío de un mismo SMS a un usuario móvil en un periodo de tiempo inferior a 3 horas. c. Nuestro firewall está configurado para limitar las peticiones por segundo que se hacen a la red del operador, así evitar el flooding o ataques de negación de servicio."*

A su vez, **COMCEL** adujo mediante comunicación 2020813564 de 10 de noviembre de 2020 que, si **HABLAME** *"tuviera una configuración rigurosa en su FIREWALL este tipo de situaciones fraudulentas no se presentarían, menos aún en la forma reiterada en que suceden."* Con lo anterior, el solicitante implícitamente reconoce la implementación de un firewall por parte de **HABLAME**, y cuestiona la configuración del mismo sin exponer elementos técnicos que sin asomo de duda denoten una afectación material a su red.

Con fundamento en lo anterior, en los argumentos expuestos por las partes y la documentación que allegaron en el marco de la presente actuación se tiene que:

- **COMCEL** solicita se ordene a **HABLAME** adoptar medidas que mitiguen de manera efectiva el envío de mensajes con tenido presuntamente fraudulento, a través de su red.
- Así mismo, solicita que, de no cumplirse con lo anterior, se le autorice a terminar con la relación de acceso y proceder a la desconexión material.
- Además de los presuntos incumplimientos contractuales por parte de **HABLAME**, la única afectación técnica que adujo **COMCEL** fue la no implementación de un firewall, sobre lo cual posteriormente manifestó que sí existía el mismo, cuestionando sólo su configuración.
- Igualmente, alegó reiteradamente la eventual afectación a la seguridad de los usuarios, que cómo se indicó, es un asunto que escapa de las competencias de la Comisión.

En síntesis, de lo probado en el expediente se encuentra que **COMCEL** no acredita una afectación de su red con ocasión de la relación de acceso objeto de análisis ni que las medidas que **HABLAME** aduce haber adoptado que no parecen ser lo suficientemente efectivas para la prevención de envío de mensajes de texto SMS con contenido aparentemente fraudulento, generen una afectación a la red de **COMCEL** o de los servicios que éste provee, por lo que de los hechos probados en el expediente, no se evidencia la configuración de ninguna de las causales de desconexión contempladas en la Resolución CRC 5050 de 2016.

Adicionalmente, y como se ha afirmado líneas atrás, la CRC puede, excepcionalmente, autorizar la desconexión de una relación de acceso o interconexión, cuando se evidencie, sin asomo de duda, que dicha relación no cumple satisfactoriamente con su fin natural, o cuando representa a uno de



sus extremos una carga adicional a la que está obligado a soportar, por ejemplo, cuando genera afectaciones a su red.

En el caso que nos ocupa, **COMCEL** ha sido insistente en su solicitud de desconexión, alegando que con ocasión de incumplimientos contractuales por parte de **HABLAME**, concernientes a la no adopción de medidas de seguridad idóneas y efectivas para la prevención del envío de mensajes de texto con contenido fraudulento, no obstante, no argumentó ni probó cómo esos presuntos incumplimientos contractuales, cuyo decreto en todo caso escapa de las competencias de la CRC, generan una afectación técnica a su red o a la prestación de los servicios que provee.

En ese orden de ideas, en esta oportunidad no se evidenció la configuración de ninguna de las causas que habilitan a la CRC a autorizar la terminación de una relación de acceso y la consecuente desconexión material. Lo anterior de manera alguna implica que los proveedores parte de este trámite administrativo no estén obligados a adoptar las medidas necesarias para que el tráfico de SMS que se curse en su relación de acceso, se corresponda con las reglas de protección de datos personales y con las medidas de control de fraude necesarias para salvaguardar la confianza y derechos de los usuarios de los servicios de comunicaciones.

En mérito de lo expuesto,

### RESUELVE

**ARTÍCULO 1.** Negar la solicitud de autorización de terminación de la relación de acceso e interoperabilidad para el envío de mensajes cortos de texto SMS entre **COMUNICACIÓN CELULAR S.A y HABLAME COLOMBIA S.A.S E.S.P**, regida por el contrato de No. 29966 de 2017, de conformidad con lo expuesto en la parte considerativa de la presente resolución.

**ARTÍCULO 2.** Remitir el expediente administrativo 3000-32-2-3 al Ministerio de Tecnologías de la Información y las Comunicaciones, para lo de su competencia.

**ARTÍCULO 3.** Remitir el expediente administrativo 3000-32-2-3 a la Superintendencia de Industria y Comercio, para lo de su competencia.

**ARTÍCULO 4.** Notificar por medios electrónicos la presente Resolución a los representantes legales de **COMUNICACIÓN CELULAR S.A y HABLAME COLOMBIA S.A.S E.S.P**, o a quienes hagan sus veces, de conformidad con lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, advirtiéndoles que contra la misma procede el recurso de reposición, dentro de los diez (10) días siguientes a su notificación.

Dada en Bogotá D.C. a los **11 días del mes de marzo de 2021**

### NOTIFÍQUESE Y CÚMPLASE

  
**CARLOS LUGO SILVA**  
Presidente

  
**SERGIO MARTÍNEZ MEDINA**  
Director Ejecutivo

Expediente No: 3000-32-2-3  
S.C.C. 408 del 10/03/2021

Revisado por: Lina María Duque del Vecchio – Coordinadora de Asesoría Jurídica y Solución de Controversias.  
Elaborado por: María Eucalia Sepúlveda De La Puente- Carlos Ruíz.