Carrera 8 No 20 – 70 Piso 1 Oficina de Correspondencia ETB
Código Postal: 110311
Conmutador: 242 2000

Bogotá, D.C., 27 de mayo de 2021

AC-DRRI-130-2021
CECO: AC030

Doctor
SERGIO MARTÍNEZ MEDINA
Director Ejecutivo
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Calle 59A Bis No. 5-53 Edificio Link Siete Setenta Piso 9
Ciudad
digitalizacionrpu@crcom.gov.co

Asunto: *Comentarios frente a la propuesta de modificación de la Decisión Andina 638 de 2006, que trata sobre los "Lineamientos para la Protección al Usuario de Telecomunicaciones de la Comunidad Andina"*

Respetado doctor Martínez,

Por medio de la presente comunicación, la Empresa de Telecomunicaciones de Bogotá S.A. E.S.P. (ETB) presenta oportunamente sus comentarios frente a la propuesta de modificación de la Decisión Andina 638 de 2006, que trata sobre los "Lineamientos para la Protección al Usuario de Telecomunicaciones de la Comunidad Andina" y agradece a la Comisión de Regulación de Comunicaciones la oportunidad de participar en este espacio.

1. Frente a Las disposiciones generales de objeto y ámbito de aplicación de la Decisión

Consideramos que el objeto de la Decisión 638 se debe mantener tal como está en la versión vigente, esto es, *"establecer lineamientos comunitarios de protección al usuario, que los Países Miembros deberán tener en cuenta al definir sus normativas internas en materia de telecomunicaciones, con el fin de garantizar un tratamiento armónico en la Subregión".* Lo anterior dado que es necesario que las autoridades de los Países Miembros evalúen los lineamientos previstos por la Comunidad Andina a la luz de la realidad de su país y realicen los ajustes necesarios en las normatividades internas ya definidas sobre la materia.

Por el contrario, al ajustar el objeto y el ámbito de aplicación de la Decisión como se propone en este proyecto, esto es, dictando los lineamientos y ordenando directamente que estos sean cumplidos por parte de los operadores, proveedores, prestadores y comercializadores de redes y servicios de telecomunicaciones, y Tecnologías de la Información y las Comunicaciones, entre otros, sin necesidad de ajuste de la normatividad interna, se crearían dos marcos jurídicos distintos (el comunitario y el interno), los cuales serían inconsistentes entre sí respectos de varios aspectos, al menos para el caso colombiano. Esta circunstancia generaría inseguridad jurídica para los agentes del sector dado que tendrían que decidir entre cumplir el uno o el otro.

Cabe resaltar adicionalmente que Colombia ya cuenta con un marco regulatorio robusto en materia de protección a usuarios de servicios de comunicaciones -incluso podría decirse que es un sector sobre regulado en relación con otros sectores de la economía-, por lo que introducir automáticamente otra normatividad al respecto, de obligatorio cumplimiento para los proveedores de redes y servicios sin que la CRC pueda armonizar la normatividad interna de manera previa,

generará inevitablemente choques que no son convenientes ni para las empresas ni para los usuarios.

Por otro lado, es preciso advertir que, con en esta propuesta de modificación del objeto de la Decisión, puede entenderse que todo tipo de servicios de comunicaciones, incluyendo las comunicaciones privadas, corporativas y las soluciones a la medida, deben observar los mismos lineamientos generales. Esto va en contravía de la normatividad colombiana vigente donde se prevé la posibilidad de exceptuar este tipo de servicios de la aplicación del régimen de protección de los derechos de los usuarios de servicios de comunicaciones, en tanto se contempla la capacidad de este tipo de clientes de negociar las condiciones técnicas, económicas y jurídicas aplicables al servicio contratado, por lo que requieren un menor nivel de protección. Así las cosas, respetuosamente se sugiere acotar el objeto de la Decisión en el sentido de excluir a los servicios corporativos.

2. Frente a las disposiciones relacionadas con la protección de los datos personales y la protección de los derechos relativos a la confidencialidad, intimidad, integridad e inviolabilidad de las comunicaciones

El artículo 15 de la Constitución Política de Colombia reconoce el derecho fundamental al *habeas data,* esto es, a la intimidad, a la protección de datos personales, a la privacidad y a la inviolabilidad de las comunicaciones.

Es preciso resaltar que la Constitución reconoce estos derechos fundamentales para *todas las personas en el territorio colombiano* y no únicamente para los usuarios de servicios de comunicaciones o de Tecnologías de la Información y las Comunicaciones. Por lo tanto, no consideramos pertinente que las condiciones y los requisitos que rigen la protección de estos derechos sean dispuestos en una norma específica de usuarios de servicios de comunicaciones, puesto que estas medidas deben considerar aspectos transversales a todos los sectores de la economía.

Más aún cuando, al tratarse de derechos fundamentales, su reglamentación en Colombia tiene reserva de ley estatutaria, esto es, debe tener un trámite legislativo cualificado con el propósito de someter la materia a mayor discusión democrática y control, debido a su importancia para el Estado Social de Derecho. En efecto, siguiendo ese mandato constitucional, en Colombia fue expedida la Ley Estatutaria No. 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales"*, la cual prevé, en conjunto con sus respectivos decretos reglamentarios, todo un marco normativo robusto que regula la materia.

Por otro lado, resulta fundamental traer a colación que, según lo dispuesto por la Corte Constitucional de Colombia mediante la Sentencia C-252 de 2019, *"los tratados internacionales económicos, de inversión o comerciales tienen, en general, la jerarquía normativa de las leyes ordinarias"*, por lo que no pueden desconocer ni contradecir lo dispuesto en las normas que integran el bloque de constitucionales ni en las leyes estatutarias. En esta misma línea, se debe recordar que los tratados de la Comunidad Andina de Naciones no hacen parte del bloque de constitucionalidad según lo ha aclarado la misma Corte en reiterada jurisprudencia, dado que no involucran el reconocimiento y la protección de derechos humanos, al menos en forma directa. En particular en la Sentencia C-256 de 1998, reiterada en la Sentencia C-491 de 2019 la Corte dispuso que *"'ni los tratados de integración ni el derecho comunitario se acomodan a los supuestos normados por el artículo 93 constitucional, ya que sin perjuicio del respeto a los principios superiores del ordenamiento constitucional […] su finalidad no es el reconocimiento de los derechos humanos sino la regulación de aspectos económicos, fiscales, aduaneros, monetarios,*

técnicos, etc., de donde surge que una prevalencia del derecho comunitario andino sobre el orden interno, similar a la prevista en el artículo 93 de la Carta, carece de sustento".

Es así como, al incluir principios y reglas adicionales e incluso contrarias a las previstas en la legislación interna vigente, se puede considerar que esta propuesta de modificación de la Decisión Andina 638 excede el campo de aplicación del tratado de la Comunidad Andina de Naciones (CAN) y choca con normas de mayor jerarquía del ordenamiento jurídico colombiano, generando así inseguridad jurídica, tanto para las empresas responsables y encargadas del tratamiento de datos personales, como para los titulares de estos.

Por todo lo anterior, respetuosamente solicitamos a la CRC, así como a las demás entidades del estado que participan por Colombia en el Comité de Autoridades Andinas de Telecomunicaciones (CAATEL) de la Comunidad Andina de Naciones (CAN) que se pronuncien sobre la inconveniencia e inconstitucionalidad de pretender incluir disposiciones relacionadas con derechos fundamentales en una norma comunitaria relativa a la protección de usuarios de servicios de comunicaciones.

Sin perjuicio de lo anterior, a continuación presentamos algunas observaciones específicas frente a lo dispuesto en los Capítulos II y III de la propuesta de modificación de la Decisión:

- A pesar de que el Parágrafo 2 del Artículo 3 señala que el alcance de cada principio, derecho, así como sus mecanismos y autoridades competentes de protección de datos personales será el establecido en la regulación interna de cada País Miembro, es importante anotar que la legislación colombiana sobre la materia no prevé los principios rectores de lealtad, legitimación y proporcionalidad. Con lo anterior, es fundamental que, de acogerse esta propuesta de modificación de la Decisión 638, se indique internamente cómo se deben entender y aplicar estos principios.

- Es confuso el entendimiento del libre ejercicio del tratamiento de datos personales en la Comunidad Andina expresado en el inciso cuarto del Artículo 3, versus la libre circulación de datos expresada en el Artículo 5 del presente. Máxime cuando este párrafo describe menos restricciones que en el del Artículo 5. Se sugiere precisar o eliminar este inciso.

- El régimen de datos personales de Colombia no exige informar al titular, al momento de obtener la autorización, cuál va a ser la duración del tratamiento.

- Se solicita se aclare el alcance de lo referido en el Parágrafo 3 del Artículo 3 del proyecto de modificación en cuanto a que *"Todas las empresas o personas a las cuales le es aplicable esta Decisión deberán adoptar medidas útiles, eficientes, necesarias y pertinentes para acreditar el cumplimiento de lo dispuesto en esta Decisión respecto del Tratamiento de Datos Personales"*. Lo anterior teniendo en cuenta que no es claro qué se entendería como medidas útiles, eficientes y necesarias, y tampoco es claro cómo debe darse aplicación a la norma en el caso en que la normativa internacional no se alinee con la legislación y regulación interna sobre la materia.

- El Artículo 4 sobre limitación al tratamiento de datos personales, impone nuevas obligaciones a los responsables de dicho tratamiento dado que la norma interna (artículo 2.2.2.25.2.8 del Decreto 1074 de 2015) prevé dos criterios para el tratamiento del dato -la razonabilidad y la necesidad-, mientras que el proyecto dispone únicamente un criterio de necesidad.

- El Artículo 5 dispone que *"se reconoce y garantiza la libre circulación dentro de los Países Miembros de la CAN de datos personales, cuando el país destinatario de los datos*

personales hubiere sido reconocido como uno que cuenta con un nivel adecuado de protección de datos personales por parte del país transferente". No obstante, no se indica qué entidad o entidades de orden nacional o comunitario determinarán si un país cuenta con niveles adecuados de protección, ni el procedimiento que se seguirá para ello. Adicionalmente, la normatividad interna permite el flujo transfronterizo de datos personales, previo contrato. No obstante, la propuesta de modificación de la Decisión Andina restringe esa facultad al exigir que una autoridad local avale dichos contratos.

- En jurisprudencia de la Corte Constitucional, se ha establecido una clara diferenciación entre los datos públicos, semiprivados y privados. Según la clasificación del dato, se prevén criterios específicos para su transmisibilidad, tratamiento, manejo y protección. etc. El proyecto de modificación de la Decisión 638 no hace una división especifica de los criterios y/o de la clasificación de los datos, sino que los trata de manera transversal, lo que desconoce los criterios desarrollados por la Corte Constitucional sobre este asunto.

- El numeral 1 del Artículo 7 establece la obligación de mantener la confidencialidad de los datos almacenados en los equipos terminales de los usuarios, frente a lo cual los operadores no tienen control ni injerencia, por lo que se solicita acotar el alcance de este lineamiento.

- El numeral 3 del Artículo 7 utiliza la expresión "mensajes electrónicos", se sugiere incluir esta definición en el glosario, con el fin de aclarar si hace referencia a mensajes enviados a través del correo electrónico, mensajes cortos (SMS), multimedia (MMS), instantáneos (Facebook Messenger, Skype, Line, Hangouts, Telegram y WhatsApp) y mensajes similares. Es preciso resaltar que en Colombia sólo está establecida el derecho de los usuarios de ser excluidos para el recibo de SMS promocionales o publicitarios, por lo cual esta normativa requeriría una revisión y modificación de la regulación en Colombia, para lo que se debe tener en cuenta que el bloqueo de correos electrónicos podría implicar la violación al principio de neutralidad de red.

3. <u>Frente a las disposiciones relacionadas con la protección de los derechos de los usuarios a la libertad de elección, el acceso universal, las prácticas comerciales y la ciberseguridad</u>

Frente al Artículo 15 relacionado con el derecho de los usuarios al acceso universal a los servicios de telecomunicaciones y Tecnologías de la Información y las Comunicaciones, consideramos que la obligación de garantizar dicho acceso no puede de ninguna manera recaer en los proveedores de redes y servicios. Por el contrario, se debe considerar como una política de Estado que, como tal, debe ser de responsabilidad de los gobiernos de los Países Miembros. En ese sentido, se solicita respetuosamente el ajuste del artículo en mención en el sentido de precisar que la obligación de garantizar el acceso universal recae sobre los Países Miembros.

Ahora bien, frente a la asequibilidad de los precios de los servicios de telecomunicaciones, se debe tener en cuenta que en Colombia la libre competencia se prevé como uno de los principios orientadores del sector de las TIC, lo que implica que el Estado tiene el deber de propiciar escenarios de libre y leal competencia que incentiven la inversión y que promuevan la concurrencia al mercado. En ese sentido, frente a la exigencia de asequibilidad en los precios de los servicios se debe tener en cuenta que, además de ser un criterio subjetivo por obedecer a las realidades económicas y sociales de cada uno de los Países Miembros, para el caso de Colombia, los precios están dados por las condiciones de mercado, bajo un criterio de libre competencia.

Por otro lado, consideramos que se requiere mayor precisión en lo dispuesto en el numeral 6 del Artículo 16, en tanto no resulta clara la obligación de *"Brindar la posibilidad a los usuarios de*

acceder a los servicios de contenidos por suscripción, que se ofrezcan o se puedan visualizar por Internet y que se hayan contratado en uno de los Países Miembros, cuando dicho usuario se encuentre de manera temporal en cualquier otro país de la Comunidad Andina". En particular se debe aclarar si esta obligación consiste en prestar el servicio de internet fijo o móvil en modalidad de roaming internacional, para lo que se debe tener en cuenta que no todos los operadores tenemos habilitada esa posibilidad, o si la obligación recae en los proveedores de servicios OTT.

Finalmente, en relación con las medidas de seguridad y ciberseguridad tendientes a proteger la información de los usuarios previstas en el Artículo 17, planteamos las siguientes observaciones:

- La ciberseguridad debe estar aplicada en la infraestructura del operador y no debe tener alcance sobre los dispositivos y software de los usuarios.

- Los proveedores de redes y servicios de comunicaciones realizamos funciones de transporte de datos, pero no tenemos control de los contenidos que son provistos por empresas generadoras alojadoras de contenido, CDN´s, redes sociales, motores de búsqueda, comercializadoras de bienes y servicios distribuidas por todo el mundo, entre ellas se encuentran como ejemplo: Akamai, Alibaba, Amazon, Cloudflare, Facebook, Google, Imgur. Por lo que habilitar mecanismos de ciberseguridad y protección de datos personales de los usuarios no es posible. En consistencia con lo anterior, se considera importante que se incluya como parte del ámbito de aplicación de la decisión, a los proveedores de contenido CDNs que tienen permitido distribuir en los países miembros su contenido y de la misma manera prestar sus servicios, de manera que no vaya en contravía de las disposiciones legales y regulatorias de cada país.

- Tampoco es posible realizar bloqueos parciales sobre aplicaciones, como fue el caso solicitado para bloquear los servicios de transporte de UBER sin afectar otros servicios que ofrecen con su aplicación como es el ejemplo de UBER EATS, ya que no es posible para un operador entrar al código del prestador del servicio de la aplicación.

- El deber de notificar a la autoridad nacional competente sobre violaciones o brechas de seguridad no debería preverse respecto de *cualquier* evento como se indica en el texto de la propuesta, sino únicamente para aquellos con cierto nivel de criticidad. Si bien se hace la salvedad sobre la existencia de otro plazo regulado al interior de cada país, no se hace la salvedad de los niveles de criticidad como criterio para el reporte del incidente, como sí prevé en la normatividad interna de Colombia.

4. Frente a los deberes de los usuarios

Se sugiere que se contemple como un deber adicional en cabeza de los usuarios la obligación de hacer buen uso del servicio de comunicación contratado, es decir, aspectos de cumplimiento legal como, por ejemplo, no acceder, distribuir y alojar contenidos que atenten contra la integridad de menores de edad consagrado en las diferentes legislaciones; no realizar actividades ilegales cibernéticas como ataques sobre dispositivos y redes de otros usuarios, entre otros.

5. Frente a las obligaciones de los Operadores

Frente a lo dispuesto en el numeral 7 del Artículo 19, si bien en Colombia existen las obligaciones de medición de indicadores de calidad, no existe una disposición expresa que exija que esta sea comparable. Tampoco existe una obligación regulatoria desarrollada respecto de seguridad y ciberseguridad que sea comparable.

Por lo tanto, consideramos que el artículo se debería acotar en el sentido de indicar que la obligación consiste en medir y reportar indicadores de calidad y atención, conforme la normativa interna de los países.

6. Frente a las disposiciones complementarias

El numeral 7 del artículo 25 establece que se debe *"Notificar debida y oportunamente al usuario de la respuesta por medios electrónicos o físicos, de acuerdo a la* ***elección expresa*** *que realice el usuario"*, lo cual implica un retroceso frente a lo dispuesto en la Resolución CRC 6242 de 2021, donde se autorizó que las respuestas a las PQR se enviaran por defecto a través de una canal digital el cual deberá ser previamente informado al usuario, salvo que el usuario manifieste que desea recibir la respuesta por el mismo medio por el cual presentó la PQR. Es decir que, contrario a lo que se exigiría en este artículo, en Colombia no es necesaria la autorización expresa del usuario para enviarle la respuesta a través de medios electrónicos.

Por otro lado, en Colombia no se exige ningún requisito adicional al envío de la respuesta para que la misma se entienda notificada al usuario, por lo que se solicita evitar el uso de la palabra *"notificar"* y en su lugar hablar de *"enviar la respuesta al usuario oportunamente".*

Por último, frente a lo dispuesto en el Artículo 26, es fundamental que, en virtud del principio de costos eficientes que rige la prestación de los servicios de telecomunicaciones, no se interprete que garantizar el acceso a las redes y servicios por parte de las personas con discapacidad implica necesariamente gratuidad en los mismos, y en todo caso, la obligación de garantizar dicho acceso estaría cabeza de los gobiernos de los Países Miembros como política de estado.

Esperamos con estos comentarios contribuir al desarrollo de la propuesta en cuestión.

Cordialmente,

LUDWIG CHRISTIAN CLAUSEN
Director de Regulación y Relaciones Institucionales
Vicepresidencia de Asuntos Corporativos y Estrategia

Elaboró: Ana Isabel Ortiz Bermúdez – Dirección de Regulación y Relaciones Institucionales
Revisó y aprobó: Ludwig Christian Clausen – Dirección de Regulación y Relaciones Institucionales