

Rad. 2026201597
Cod. 11000
Bogotá, D.C.

Radicado:	2026531677
Fecha:	21/09/2026 9:57:05 A. M.
Proceso:	11000 PROSPECTIVA ESTRATÉGICA E INNOVACI
Destino:	CONGRESO DE LA REPÚBLICA
Asunto:	OBSERVACIONES AL PROYECTO DE LEY NO. 077 DE 2026 CÁMARA

Honorables Representantes a la Cámara
DANIEL FELIPE BRICEÑO MONTES
EDUAR ALÉXIS TRIANA RINCÓN
CONGRESO DE LA REPÚBLICA DE COLOMBIA

Correos electrónicos: daniel.briceno@camara.gov.co ; eduar.triana@camara.gov.co ;
comision.sexta@camara.gov.co
Ciudad

REF: Observaciones al Proyecto de Ley No. 077 de 2026 Cámara «Por la cual se crea el Registro Nacional de Tarjetas SIM y eSIM, se adoptan medidas para fortalecer la seguridad en la comercialización, activación y uso de los servicios de telefonía móvil, y se dictan otras disposiciones».

Honorables Representantes:

La Comisión de Regulación de Comunicaciones (CRC) ha tenido conocimiento del proyecto de Ley de la referencia, el cual fue presentado para consideración y trámite ante el Congreso de la República. En atención a dicha solicitud y en el marco de las funciones previstas en la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, esta Comisión presenta las siguientes observaciones.

El Proyecto de Ley 077 de 2026 Cámara¹ tiene como objeto crear el Registro Nacional de Tarjetas SIM y eSIM (RNTS), así como un registro obligatorio de identificación de los usuarios finales de dichas tarjetas (el cual alimentará el RNTS, según lo señala el artículo 6 del Proyecto de Ley), de manera que se garantice la identificación de los usuarios y la trazabilidad de las operaciones de las líneas móviles, a efectos de prevenir la comisión de actividades delictivas, como la extorsión, el secuestro extorsivo, falsedad personal, entre otras, por medio de los servicios de telecomunicaciones móviles.

Al respecto, la Comisión reconoce la relevancia de las finalidades perseguidas por la iniciativa legislativa y comparte la necesidad de fortalecer las herramientas institucionales para prevenir y combatir fenómenos como la extorsión, la suplantación de identidad, el fraude y otras conductas delictivas que utilizan los servicios móviles como instrumento o medio de comisión. También destaca que el proyecto incorpora varios elementos que representan una evolución frente a iniciativas anteriores con objetivos similares. Particularmente, resulta positivo que el proyecto adopte expresamente principios orientadores (necesidad, proporcionalidad, legalidad y protección de datos personales, entre otros), y que descarte la exigencia obligatoria de mecanismos biométricos para la identificación de los usuarios finales.

¹ Gaceta del Congreso No. 909 del 31 de julio de 2026.

La Comisión considera útil distinguir entre la existencia de una problemática legítima de seguridad y la valoración de los instrumentos previstos para enfrentarla. La evidencia sobre la ocurrencia de fraude, extorsión o suplantación pone de presente la necesidad de fortalecer la respuesta institucional; al mismo tiempo, resulta conveniente profundizar en las dificultades que actualmente afectan la identificación o trazabilidad de las líneas móviles y en la contribución que las medidas propuestas podrían generar frente a dichas dificultades. Este análisis permitiría contar con mayores elementos para valorar la necesidad, proporcionalidad y eficacia de las medidas planteadas.

Por tanto, la CRC considera necesario poner de presente algunas reflexiones generales que contribuyan a enriquecer la discusión legislativa, en particular que la exposición de motivos identifique de manera expresa, y con evidencia, cuál sería el beneficio adicional esperado de la creación del RNTS, precisando su necesidad, proporcionalidad, razonabilidad y viabilidad técnica y económica, así como la relación directa de las medidas que plantea el Proyecto de Ley, con la prevención de actividades delictivas cometidas a través de los servicios de telecomunicaciones móviles.

Adicionalmente, es necesario resaltar que la CRC se ha pronunciado anteriormente sobre iniciativas legislativas de propósito similar² al presente Proyecto de Ley, lo que permite identificar la posición institucional esgrimida. Sin embargo, estos antecedentes no reemplazan el análisis particular del Proyecto de Ley No. 077 de 2026 Cámara, cuyo contenido incorpora medidas que deben ser analizadas de manera particular. Por esta razón, las observaciones que se presentan a continuación se concentran en la justificación y el articulado de la iniciativa legislativa en cuestión.

1. Comentarios generales

1.1. Identificación del problema, proporcionalidad y beneficio incremental

La exposición de motivos identifica expresamente que el Proyecto de Ley no pretende establecer cargas desproporcionadas a los usuarios o a la industria, pretende resolver, según se expone en el texto, un vacío regulatorio en tanto «hoy es posible adquirir y activar una tarjeta SIM prepago sin verificación alguna de identidad, lo que convierte a la línea móvil en un instrumento anónimo».

Sobre este punto, resulta necesario distinguir entre la comercialización o adquisición de una tarjeta SIM y la activación efectiva del servicio. La posibilidad material de adquirir una SIM no implica, por sí misma, que la línea pueda entrar en operación sin que se surtan los mecanismos de identificación y validación exigibles. En ese contexto, resultaría útil que el diagnóstico permitiera identificar en qué punto de la cadena se presentan las principales dificultades: en la comercialización, en los procesos de identificación y validación, en la activación efectiva de la línea o en el cumplimiento de las obligaciones existentes.

² Entre otros, la CRC se pronunció sobre los proyectos de Ley 165 de 2026 Cámara (Radicado 2026529119 del 29 de agosto de 2026), 535 de 2025 Cámara (Radicado 2025511445 del 14 de abril de 2025) y 038 de 2025 Cámara (Radicado 2025531068 del 24 de septiembre de 2025). También se han identificado otras iniciativas de objeto semejante, entre ellas los proyectos de Ley 269 de 2024 Senado, 381 de 2024 Cámara, 074 de 2025 Senado y 077 de 2026 Cámara.

Para sustentar esta problemática, el Proyecto de Ley precisa que la ausencia de información sobre el usuario final de la línea móvil genera un nicho de impunidad, dado que actualmente es posible acceder a estas tarjetas sin obligación alguna de registro de los datos asociados a la línea. La exposición de motivos trae a colación cifras de la Policía Nacional y la Fiscalía General de la Nación, señalando un crecimiento sostenido de las mismas, acerca del delito de extorsión entre el 2018 y 2025, haciendo referencia al uso del teléfono móvil desde los Establecimientos de Reclusión del Orden Nacional (ERON). Precisa que la cifra de las 54.000 personas afectadas por la extorsión podría ser mayor, dado un problema de subregistro que pone de presente la Encuesta de Convivencia y Seguridad Ciudadana (ECSC) del Departamento Administrativo Nacional de Estadística (DANE).

Hace mención al fenómeno de la extorsión telefónica carcelaria, reconocido por la Corte Constitucional dentro del Estado de Cosas Inconstitucional del sistema penitenciario declarado mediante la Sentencia T-388 de 2013. Asimismo, reconoce la existencia de medidas administrativas como la que previene el Decreto 851 de 2024, por medio del cual se fortaleció los mecanismos de bloqueo de equipos terminales y líneas asociadas a extorsión carcelaria, habilitando al Instituto Nacional Penitenciario y Carcelario (INPEC) para coordinar con los operadores móviles el bloqueo de equipos usados ilegalmente desde prisión. Sin embargo, indica su Despacho que estas medidas «actúan sobre el equipo o la línea ya identificada como fuente de extorsión; no resuelven el problema de fondo, que es la posibilidad de adquirir, sin ningún control, una nueva línea anónima para reemplazar la bloqueada».

De esta manera, si bien la exposición de motivos evidencia la existencia de una problemática que se pretende atender, su análisis podría fortalecerse con una caracterización más detallada de los factores que contribuyen a ella y de la relación de estos con las medidas propuestas. Para estos efectos, pueden distinguirse, entre otros, cuatro elementos: (i) inexistencia o insuficiencia de una obligación; (ii) incumplimiento o evasión de una obligación existente; (iii) fallas en la calidad, validación o actualización de la información; y (iv) dificultades para consultar, interoperar o acceder oportunamente a información que ya existe. Estas situaciones pueden responder a causas diferentes y, por ello, admitir instrumentos de política pública también distintas.

Esta diferenciación resulta fundamental porque cada tipo de falla puede requerir una respuesta distinta. Si el problema se encuentra en el incumplimiento de obligaciones existentes, la respuesta puede estar asociada a fortalecer su aplicación y control; si se origina en los mecanismos de identificación o validación, puede requerir el mejoramiento de dichos procedimientos; y si corresponde a dificultades de acceso, fragmentación o disponibilidad de la información, pueden resultar pertinentes soluciones de interoperabilidad y mecanismos que optimicen los canales de consulta de las autoridades competentes. Estos mecanismos deberán operar, en todo caso, con observancia de las condiciones legales aplicables al acceso a la información, incluida, cuando corresponda, la orden judicial previa prevista en el artículo 244 de la Ley 906 de 2004³. La consideración conjunta de estas alternativas permitiría valorar con mayores elementos si la creación

³ «Por la cual se expide el Código de Procedimiento Penal».

de una nueva infraestructura centralizada aporta un beneficio adicional frente a ellas y en qué medida constituye una respuesta necesaria, idónea y proporcional.

En este contexto, una identificación más precisa de las causas que se pretende atender permitiría valorar con mayor fundamento si la creación del RNTS constituye una opción efectiva e idónea y si sus beneficios adicionales justifican los costos y riesgos asociados a su implementación.

Así las cosas, la Comisión respetuosamente recomienda nutrir la exposición de motivos con información asociada a: (i) la proporción de líneas activas cuyos titulares no se encuentran correctamente identificados; (ii) la calidad y actualización de los registros; (iii) los eventos de suplantación asociados a la activación de líneas; (iv) los tiempos actuales de respuesta a las autoridades, incluida la orden judicial previa; (v) las investigaciones afectadas por información fragmentada, incompleta o desactualizada; y (vi) la relación verificable entre esas deficiencias y los delitos que se pretende prevenir. Lo anterior, habitará una relación directa entre la identificación precisa del problema que pretende resolverse y la justificación del valor agregado que aportan las medidas propuestas frente al marco normativo vigente.

1.2. Marco normativo y regulatorio vigente

La Comisión considera relevante que en la exposición de motivos se tengan en cuenta los mecanismos legales, reglamentarios y regulatorios orientados a garantizar la identificación de los usuarios de servicios móviles, prevenir fraudes y apoyar las labores de investigación de las autoridades competentes, y su respectiva efectividad. De manera que, se identifiquen las medidas actualmente vigentes que resultarían insuficientes para alcanzar los objetivos perseguidos y qué beneficios adicionales generaría la iniciativa frente a dicho marco normativo.

Para tal efecto, las disposiciones aplicables se presentan en tres (3) grupos:

- (i) las obligaciones actuales de identificación y actualización de la información de los usuarios;
- (ii) las medidas complementarias de prevención del fraude y la extorsión; y
- (iii) aspectos que requieren evaluación frente al marco normativo vigente.

- Obligaciones actuales de identificación y actualización de la información de los usuarios

Tal y como lo indica la exposición de motivos, los numerales 12 y 13 del artículo 95 de la Ley 1801 de 2016⁴ establecen que constituyen comportamientos que afectan la seguridad de las personas y sus bienes, la activación de líneas telefónicas y tarjetas SIM sin que el usuario haya suministrado al prestador del servicio sus datos biográficos al momento de la activación. De esta manera, el ordenamiento jurídico ya contempla una prohibición expresa frente a la activación anónima de líneas y tarjetas SIM.

⁴ «Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana».

Por su parte, la **Resolución 912 de 2008**⁵, expedida por la Dirección de Investigación Criminal de la Policía Nacional (DIJIN), dispone que los proveedores de redes y servicios de telecomunicaciones, al activar una línea telefónica, deben registrar en sus respectivas bases de datos, entre otros, los nombres y apellidos del suscriptor o usuario, el tipo y número de documento de identificación, el número móvil o de la línea telefónica y la fecha de activación. Asimismo, contempla el registro posterior de otros datos de contacto y establece que la vigilancia del cumplimiento de estas obligaciones corresponde al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

En el ámbito regulatorio, la Resolución CRC 5111 de 2017⁶, en el marco del Régimen de Protección de los Derechos a los Usuarios, dispuso que al momento de la activación del servicio en modalidad prepago, el operador deberá registrar el nombre completo de dicho usuario, su documento de identidad y el número de su línea telefónica. Posteriormente, la **Resolución CRC 7684 de 2025**⁷ modificó los artículos 2.1.3.3 y 2.1.3.4 de la Resolución CRC 5050 de 2016, y estableció mecanismos de identificación, validación y actualización de información para usuarios prepago, incluyendo procedimientos de verificación de identidad previos a la activación de los servicios móviles.

En particular, la regulación dispone que, antes de activar el servicio, los proveedores deben recolectar y validar la información de identificación del usuario. También establece parámetros para la actualización de dicha información, define los medios de atención que deben estar disponibles para adelantar este procedimiento y prohíbe registrar como titular de una línea móvil prepago a quien adquiriera tarjetas SIM físicas o virtuales con el propósito de distribuir las o comercializarlas a terceros.

La Resolución CRC 7684 de 2025 constituye, por tanto, el antecedente regulatorio con mayor relación al objeto del Proyecto de Ley, dado que establece obligaciones específicas para la identificación, validación y actualización de los datos de los usuarios de servicios móviles en modalidad prepago. Por su parte, en los servicios pospago la información de identificación es obtenida por los proveedores en el marco de la relación contractual con el usuario.

Asimismo, la **Ley 2573 de 2026**⁸ estableció obligaciones para los operadores de telecomunicaciones, entidades financieras y establecimientos comerciales orientadas a fortalecer los procesos de validación de identidad, la seguridad en el tratamiento de datos personales y la prevención de fraudes asociados a la contratación de servicios y adquisición de obligaciones por

⁵ «Por la cual se reglamenta el suministro de información de suscriptores y usuarios autorizados para el uso de las telecomunicaciones al igual que las redes de los concesionarios y licenciarios».

⁶ «Por la cual se establece el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, se modifica el Capítulo 1 del Título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones»

⁷ «Por la cual se adoptan medidas para la promoción de la competencia, se modifican algunas disposiciones de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones». Disponible en: <https://www.crcm.gov.co/sites/default/files/normatividad/00007684.pdf>.

⁸ «Por medio del cual se establecen medidas para proteger a las personas del reporte negativo ante operadores de información y el cobro de obligaciones en casos de suplantación de identidad ante los operadores de telecomunicaciones, las entidades financieras - crediticias y demás establecimientos comerciales con esta competencia y se dictan otras disposiciones». Su entrada se tiene prevista 6 meses siguientes a la promulgación (19 de noviembre de 2026), a excepción de los párrafos primero y segundo del artículo 5 de la Ley, que entraron en vigencia con la promulgación de la Ley.

terceros que actúan de manera fraudulenta. Asimismo, la ley reforzó los principios de seguridad, veracidad de la información y carga dinámica de la prueba, trasladando a las entidades la responsabilidad de demostrar la adecuada verificación de identidad de sus usuarios y clientes cuando se presenten controversias por presuntos eventos de suplantación.

Estas medidas consolidan un marco regulatorio que facilita el cumplimiento de las distintas normas antes señaladas encaminadas a garantizar que se cuente con la información de los usuarios de los servicios móviles y, en la misma línea, propende por la efectividad de los procesos de registro de los datos de los usuarios ante los operadores.

Desde esta perspectiva, la CRC considera importante que durante el trámite legislativo se profundice en la proporcionalidad y razonabilidad de las medidas propuestas, identificando qué aspectos del régimen actualmente vigente podrían requerir fortalecimiento y cuál es el beneficio agregado que aportaría la creación de nuevas obligaciones legales de identificación y registro frente a los instrumentos regulatorios ya existentes. Lo anterior resulta particularmente relevante en atención al principio de proporcionalidad y al deber de evitar duplicidades normativas que puedan generar cargas adicionales sin una evidencia clara sobre su efectividad, de cara, de una parte, a los principios constitucionales de la función administrativa, en particular el principio de eficiencia contenido en el artículo 209 de la Constitución Política y, de otra, a las obligaciones de verificación de identidad y seguridad digital contenidas en la Ley 2573 de 2026, lo cual refuerza la necesidad de identificar el beneficio incremental de imponer medidas adicionales como una base de datos nacional centralizada e interoperable.

- Medidas complementarias de prevención en la comisión de actividades delictivas

Además de las obligaciones directamente relacionadas con la identificación de los usuarios, el ordenamiento jurídico y la regulación sectorial contienen medidas complementarias dirigidas a prevenir el fraude, la extorsión y otras conductas ilícitas realizadas mediante servicios móviles.

En este sentido, el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016 establece que los proveedores tienen la obligación de utilizar herramientas tecnológicas adecuadas para prevenir la comisión de fraudes al interior de sus redes y realizar controles periódicos sobre la efectividad de dichos mecanismos. También les impone el deber de investigar las causas de las PQR relacionadas con posibles eventos de fraude y de demostrar al usuario las razones de su decisión cuando concluyan que el fraude no existió.

De otra parte, el **Decreto 4768 de 2011**⁹ adoptó medidas para restringir la utilización de dispositivos de telecomunicaciones en establecimientos penitenciarios y carcelarios. En desarrollo de estas medidas, MinTIC puede autorizar la inhibición o el bloqueo de señales, o requerir a los proveedores la restricción o eliminación de estas, cuando existan motivos fundados para considerar que desde dichos establecimientos se realizan amenazas, estafas, extorsiones u otros hechos delictivos mediante dispositivos de telecomunicaciones.

⁹ «Por medio del cual se adoptan medidas para restringir la utilización de dispositivos de telecomunicaciones en los establecimientos penitenciarios y carcelarios y se dictan otras disposiciones».

En la misma línea, y tal y como se anuncia en la exposición de motivos, el **Decreto 851 de 2024**¹⁰ estableció mecanismos de articulación entre el sector justicia, MinTIC y los proveedores de redes y servicios de telecomunicaciones móviles para fortalecer las estrategias de prevención de la extorsión originada desde establecimientos de reclusión. Entre otras medidas, contempla la posibilidad de solicitar el bloqueo del IMEI de los equipos terminales móviles y del IMSI asociado a las tarjetas SIM identificadas en comunicaciones no autorizadas.

Adicionalmente, mediante la **Resolución CRC 8308 de 2026**¹¹, la Comisión estableció nuevas medidas para detectar comunicaciones atípicas o sospechosas y suministrar a los usuarios más información antes de contestar, responder o compartir sus datos. Estas medidas actuarán en distintos puntos de la cadena, desde el uso de la numeración y el envío de mensajes, hasta la información que aparece en la pantalla del usuario. La implementación de las mismas será gradual.

Dentro de las medidas definidas por la Resolución CRC 8308 de 2026, los PRST deberán analizar en tiempo real las llamadas que presenten señales sospechosas y, cuando detecten comportamientos atípicos, advertir al usuario mediante la etiqueta «Alerta de llamada sospechosa»; asimismo, deberán impedir llamadas originadas desde números no asignados o habilitados únicamente para recibir comunicaciones, y bloquear aquellas llamadas internacionales que pretendan presentarse como provenientes de numeración colombiana, salvo los casos legítimos de roaming internacional.¹² La Resolución también prevé medidas para que los mensajes automáticos enviados por bancos, comercios, entidades públicas o plataformas identifiquen al remitente, utilicen códigos cortos autorizados y correspondan a formatos previamente aprobados, para lo cual se creará un sistema central de verificación que deberá ser consultado por los operadores antes de entregar el mensaje. Esta última medida entrará en vigencia 12 meses después de la expedición del acto administrativo que defina la remuneración del ecosistema.

Finalmente, dicha Resolución creó el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles, liderado por la CRC, espacio para compartir alertas, analizar nuevas modalidades de fraude y coordinar acciones entre operadores, empresas de mensajería y autoridades.

Las medidas descritas atienden manifestaciones específicas del fraude, la extorsión y otras actividades ilícitas en diferentes puntos de la cadena. Por tanto, complementan las obligaciones de identificación de los usuarios, pero no equivalen a la creación de un Registro Nacional de tarjetas SIM y eSIM ni permiten concluir, por sí solas, que exista una duplicidad con el RNTS propuesto por el Proyecto de Ley.

¹⁰ «Por el cual se dictan disposiciones relacionadas con la restricción de comunicaciones no autorizadas al interior de Establecimientos de Reclusión del Orden Nacional (ERON), se adicionan unos artículos al Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1069 de 2015, y se modifican y derogan algunas disposiciones del Título 11 de la Parte 2 del Libro 2 del Decreto 1078 de 2015».

¹¹ «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones». Disponible en: <https://www.crcm.gov.co/sites/default/files/normatividad/00008308.pdf>

¹² Servicio adicional que permite a los usuarios tener servicios de voz, mensajes de texto (SMS) y datos en el exterior, con el mismo número celular que utiliza en Colombia

- Aspectos que requieren evaluación frente al marco normativo vigente

A partir del marco normativo y regulatorio expuesto, se observa que actualmente existen obligaciones dirigidas a (i) identificar a los usuarios de los servicios móviles, (ii) mantener actualizada su información y (iii) prevenir la utilización de las redes para la comisión de fraudes y otras conductas ilícitas. No obstante, para determinar si se requiere una intervención legislativa adicional, resulta necesario establecer, a partir de evidencia verificable, cuáles aspectos de la problemática permanecen sin ser atendidos suficientemente por las medidas vigentes.

En particular, como se expuso previamente, la exposición de motivos debería presentar información que permita determinar si las dificultades identificadas obedecen al incumplimiento de las obligaciones existentes, a problemas en la calidad o actualización de la información suministrada por los usuarios, a eventos de suplantación durante los procesos de activación, a la dispersión de los registros entre los diferentes proveedores, a los tiempos requeridos para atender las solicitudes de las autoridades o a una combinación de estos factores.

Esta precisión resulta especialmente relevante frente a la Resolución CRC 7684 de 2025, por ser el antecedente regulatorio que se relaciona con la identificación y actualización de los datos de los usuarios de servicios móviles prepago. Teniendo en cuenta su reciente expedición e implementación, resulta necesario considerar la información disponible sobre su aplicación y, en la medida en que transcurra un periodo suficiente para su evaluación, los resultados obtenidos con las obligaciones de identificación, validación previa y actualización de datos allí establecidas.

En ese contexto, y a criterio de la Comisión no es posible concluir, con fundamento en la información contenida en la exposición de motivos, que el régimen vigente haya solucionado integralmente la problemática; como tampoco puede concluirse de la exposición de motivos que la creación del RNTS constituya la alternativa más adecuada para atenderla.

En consecuencia, se recomienda complementar la justificación de la iniciativa con información que permita determinar: (i) qué componentes de la problemática son atendidos por las obligaciones vigentes; (ii) cuáles dificultades persisten en su aplicación; (iii) cuál es su magnitud; y (iv) de qué manera las nuevas medidas producirían un beneficio adicional y verificable frente al régimen actual. Este análisis permitiría valorar si los beneficios esperados del RNTS justifican sus costos, riesgos y cargas de implementación, así como comparar estas medidas con otras opciones que permitan alcanzar la misma finalidad.

1.3. Creación del Registro Nacional de Tarjetas SIM y eSIM (RNTS)

Una de las medidas centrales del proyecto consiste en la creación del RNTS como sistema de información centralizado interoperable con las autoridades de investigación, administrado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con el acompañamiento técnico de la CRC. Este Registro, indica la exposición de motivos, no se limita a la verificación de información en el punto de venta sino que dota a las autoridades de una herramienta permanente de consulta y trazabilidad histórica.

Aunque esta herramienta se presenta como un mecanismo para fortalecer la trazabilidad de las líneas móviles y facilitar el acceso a la información por parte de las autoridades, la Comisión considera que su conveniencia debe ser analizada de manera integral desde la perspectiva técnica, regulatoria, económica y de protección de datos personales.

Actualmente, los proveedores de redes y servicios de telecomunicaciones móviles (PRSTM) ya cuentan con obligaciones de identificación, custodia, actualización y conservación de información de sus usuarios. En este contexto, resulta necesario determinar el valor agregado efectivo que produciría una base nacional centralizada frente a los mecanismos existentes, así como los costos de implementación, operación, interoperabilidad y mantenimiento asociados a su puesta en marcha. De igual forma, la concentración de grandes volúmenes de información personal en una única plataforma incrementa los retos en materia de ciberseguridad, gestión de riesgos y protección de datos personales.

La necesidad de mejorar el acceso oportuno y confiable a la información no implica necesariamente la necesidad de concentrarla en un único repositorio. En este contexto, podría resultar útil comparar la creación de un repositorio centralizado con otras alternativas que también permitan mejorar el acceso oportuno, confiable y seguro a la información, como mecanismos de interoperabilidad entre las bases existentes, esquemas descentralizados de consulta o pasarelas seguras de acceso. Esta comparación permitiría valorar las ventajas, costos y riesgos de cada alternativa, incluida la posible duplicación de información.

De igual manera, resulta pertinente considerar que la centralización de la información podría no resolver por sí sola eventuales dificultades originadas en los procesos de identificación, validación o actualización de los datos. En esos casos, la información incorporada al nuevo repositorio podría conservar algunas de las dificultades presentes en las fuentes originales. Este elemento puede contribuir a valorar el beneficio incremental del RNTS frente a otras alternativas disponibles.

Adicionalmente, la exposición de motivos debería presentar un diagnóstico que permita establecer si la creación del RNTS responde a fallas verificadas del modelo actual, en particular deficiencias en la calidad y actualización de los registros existentes, incremento en los tiempos de respuesta a las autoridades, o a investigaciones afectadas por la fragmentación de información. De igual modo, la exigencia de que la base de datos permita la interconexión y el intercambio de información con las entidades públicas del orden nacional con competencias en la prevención e investigación del fraude en servicios móviles y canales digitales, debe consultar lo previsto en el artículo 244 del Código de Procedimiento Penal, en relación con la exigencia de orden judicial previa cuando la consulta implique el acceso a información confidencial referida al indiciado o imputado. Adicionalmente, debe evaluarse si campos como correo electrónico e historial de cambios son estrictamente necesarios para las finalidades de la ley.

De esta manera, y considerando lo expuesto en los numerales precedentes, la Comisión estima conveniente fortalecer en la exposición de motivos el sustento técnico y empírico asociado a la creación de un registro centralizado, particularmente en relación con el beneficio adicional que aportaría frente a las medidas legales, reglamentarias y regulatorias actualmente vigentes y a las obligaciones existentes de identificación, custodia, actualización y conservación de la información

de los usuarios.

El proyecto de ley incorpora salvaguardas relevantes: exige mecanismos de cifrado, protocolos de acceso controlado y auditorías periódicas. Estas garantías contribuyen a mitigar algunos de los riesgos identificados y podrían complementarse con una mayor fundamentación sobre la necesidad y proporcionalidad de centralizar la información.

1.4. Protección de datos personales y enfoque de minimización de datos

La CRC destaca positivamente que el proyecto incorpore expresamente los principios de legalidad, necesidad, proporcionalidad, finalidad, seguridad de la información y habeas data. De igual manera, se considera favorable que la iniciativa descarte la captura obligatoria de datos biométricos como requisito para la identificación de los usuarios finales, circunstancia que atiende observaciones que la Entidad había formulado previamente¹³ frente a iniciativas legislativas de objeto similar.

Sin perjuicio de lo anterior, la Comisión considera conveniente fortalecer el marco de gobernanza del Registro Nacional de Tarjetas SIM y eSIM (RNTS), particularmente mediante la incorporación de criterios generales relacionados con las finalidades de acceso a la información, la trazabilidad y auditoría de las consultas realizadas sobre la base de datos, los principios aplicables a la conservación y eliminación de registros, y las responsabilidades de los distintos actores que intervienen en el tratamiento de la información. Lo anterior resulta especialmente relevante considerando que el proyecto propone la creación de un sistema nacional centralizado que almacenará información personal de usuarios de servicios móviles.

En este marco, la incorporación al RNTS de información sobre líneas presuntamente asociadas con actividades delictivas haría conveniente delimitar con mayor precisión las condiciones para su reporte, consulta, permanencia, actualización y retiro, así como de las autoridades habilitadas para acceder a dicha información y de los mecanismos que permitan auditar su utilización.

En criterio de la Comisión, estos elementos corresponden al núcleo esencial de las garantías asociadas al tratamiento de datos personales y permiten delimitar claramente los derechos de los ciudadanos, las obligaciones de las entidades involucradas y los controles mínimos que deben existir sobre el uso de la información. En consecuencia, resulta pertinente que la ley defina estos lineamientos generales, sin perjuicio de que su implementación concreta sea posteriormente desarrollada mediante los instrumentos reglamentarios correspondientes.

1.5. Competencias institucionales

Las funciones legalmente asignadas a la CRC se concentran en la regulación técnica y económica del sector de comunicaciones, la protección de los usuarios y la promoción de la competencia. Esta delimitación también responde a criterios de eficiencia institucional, puesto que una adecuada

¹³ Ver nota al pie No. 2 del presente documento.

separación entre las funciones de regulación, ejecución y vigilancia permite preservar la especialización de las entidades, facilitar la rendición de cuentas y evitar que una misma autoridad participe simultáneamente en el diseño regulatorio y en la operación de los mecanismos sobre los cuales posteriormente debe adoptar decisiones técnicas. En ese contexto, sería conveniente que la participación de la CRC en el desarrollo de la iniciativa se mantenga en el ámbito de las competencias previstas en la Ley 1341 de 2009 y la Ley 1978 de 2019, sin extenderse a funciones de inspección, vigilancia y control, administración de bases de datos o ejecución operativa de políticas públicas que correspondan a otras autoridades.

2. Comentarios específicos

Sobre las definiciones – Artículo 3

Se sugiere armonizar las definiciones con la terminología prevista en la Ley 1341 de 2009, la Ley 2573 de 2026 y en el Título I de la Resolución CRC 5050 de 2016, a efectos de emplear conceptos técnicos sectoriales actualmente vigentes.

Así mismo, considerar que dentro de la definición de Proveedor de Redes y Servicios de Telecomunicaciones (PRST) se encuentra el Operador Móvil Virtual (OMV) y el Operador Móvil de Red (OMR), por expresa disposición regulatoria.

Particularmente, la definición de usuario ya cuenta con una descripción legal, en el numeral 3 del artículo 5 de la Ley 1480 de 2011.

Sobre Registro obligatorio de usuarios- Artículo 5

La Comisión observa que el artículo 5 regula materias relacionadas con la identificación de los usuarios, la recolección de información para la activación de líneas y la conservación de los registros asociados a los usuarios finales. No obstante, y como se expuso de manera precedente, estas materias ya han sido objeto de desarrollo regulatorio, particularmente a través de las disposiciones contenidas en la Resolución CRC 7684 de 2025 compilada en la Resolución CRC 5050 de 2016, la cual establece procedimientos específicos para la identificación, validación y actualización de la información de los usuarios de servicios móviles, especialmente en modalidad prepago.

En este contexto, se recomienda evaluar el alcance de la disposición a efectos de evitar duplicidades regulatorias y preservar la coherencia entre el marco legal y el regulatorio. Particularmente, podría considerarse que la ley se limite a establecer la obligación general de identificación y registro de los usuarios finales, así como los principios y objetivos que orientan dicha actividad, mientras que los procedimientos específicos para su implementación sean desarrollados posteriormente mediante regulación técnica sectorial a cargo de la CRC.

En este sentido, podría resultar conveniente que la ley concentre la definición de las obligaciones, finalidades y garantías generales, preservando la posibilidad de que la regulación técnica determine y actualice los mecanismos mediante los cuales estas se cumplen.

Lo anterior permitiría que aspectos tales como los mecanismos de validación documental de identidad, los procedimientos de actualización de registros, las condiciones de consistencia y calidad de la información, los canales habilitados para realizar el registro, los mecanismos de verificación en tiempo real, los requisitos aplicables a los procesos de actualización por cambio de titularidad, así como las condiciones operativas que deben observar los PRST, puedan ajustarse de manera flexible a la evolución tecnológica, a las dinámicas de fraude observadas en el sector y a las necesidades operativas de los agentes involucrados.

Asimismo, este enfoque resulta consistente con el principio de neutralidad tecnológica y con la práctica regulatoria del sector de comunicaciones, permitiendo que la regulación pueda incorporar de manera ágil nuevos mecanismos de autenticación, validación y seguridad cuando estos demuestren ser eficaces, sin requerir modificaciones legislativas para cada ajuste técnico que resulte necesario.

En consecuencia, la CRC considera que la ley debería concentrarse en definir las obligaciones generales de identificación, trazabilidad y conservación de información, mientras que los aspectos procedimentales y operativos asociados a la validación de identidad y administración de registros deberían ser objeto de desarrollo regulatorio posterior por parte de la CRC.

Registro Nacional de Tarjetas SIM y eSIM (RNTS) - Artículo 6

La CRC recomienda evaluar la necesidad de la creación del RNTS a partir de una valoración detallada de sus beneficios esperados, costos de implementación, riesgos de tratamiento masivo de datos personales y alternativas regulatorias posibles.

Se reitera que los PRSTM ya poseen información de usuarios, por lo que resulta necesario justificar la necesidad del registro centralizado, los beneficios esperados, el análisis costo-beneficio, y los riesgos de tratamiento masivo de datos y su forma de mitigación.

En este punto, conviene delimitar el alcance de la trazabilidad que se pretende obtener mediante el RNTS. La inscripción de una línea a nombre de una persona permite establecer su titularidad o registro, pero no permite equiparar automáticamente al titular registrado con la persona que materialmente utilizó la línea en un momento determinado. Por ello, este elemento podría ser considerado al valorar el beneficio adicional que la información aportaría para los fines de prevención e investigación perseguidos por la iniciativa.

En cuanto al esquema de administración del RNTS, resultaría pertinente valorar una distribución de responsabilidades que aproveche las capacidades de cada entidad y preserve claridad sobre las funciones de diseño técnico, operación, custodia de la información y vigilancia. En este marco, el acompañamiento de la CRC podría concentrarse en los aspectos propios de sus competencias regulatorias, mientras que las responsabilidades operativas y de administración del sistema podrían asignarse conforme a las competencias institucionales que correspondan.

Comercialización y activación - Artículo 7

La CRC comparte el propósito del artículo orientado a evitar la circulación y utilización de líneas móviles anónimas o no identificadas y reconoce la importancia de asegurar que la activación de tarjetas SIM y eSIM se encuentre asociada a un usuario previamente identificado, en línea con los objetivos de trazabilidad y prevención de conductas delictivas previstos en el proyecto de ley.

No obstante, la Comisión considera conveniente revisar el alcance de la prohibición propuesta, particularmente respecto de los conceptos de comercialización, activación y uso, dado que se trata de actividades que poseen naturaleza y responsables diferentes dentro de la cadena de provisión de los servicios móviles.

En primer lugar, debe tenerse en cuenta que la comercialización de tarjetas SIM puede ser realizada por distintos agentes del mercado, incluidos distribuidores y comercializadores autorizados, quienes no necesariamente cuentan con las capacidades técnicas ni con los sistemas de información requeridos para verificar en tiempo real el cumplimiento de todos los requisitos asociados al registro de usuarios o la integración con el RNTS. En contraste, la activación de la línea constituye una actuación que se realiza bajo control directo del PRSTM o del OMV responsable de la prestación del servicio y de la gestión de la información asociada al usuario.

En este sentido, la activación constituye un punto de control especialmente relevante para impedir que una línea entre en operación sin que previamente se haya realizado el proceso de identificación y registro exigido. Por ello, podría resultar conveniente concentrar la obligación principal sobre la activación efectiva de la línea, garantizando que ninguna tarjeta SIM o eSIM pueda entrar en operación sin que previamente se haya realizado el proceso de identificación y registro exigido por la ley. Lo anterior resulta consistente con el enfoque actualmente contenido en la regulación, la cual, como ya se vio, establece obligaciones específicas de identificación, validación y registro previas a la activación de los servicios móviles, especialmente en modalidad prepago.

De igual forma, se considera pertinente revisar el alcance de la expresión relacionada con la prohibición del uso de tarjetas SIM o eSIM no registradas. Si bien la finalidad perseguida por la norma es legítima, la aplicación práctica de una prohibición de esta naturaleza requiere precisar mecanismos de verificación, procedimientos de suspensión o desactivación y responsabilidades de los distintos actores involucrados. En este punto, podría resultar más adecuado asociar la consecuencia jurídica al mantenimiento de líneas activas sin el cumplimiento de los requisitos de identificación y registro exigidos por la ley, en lugar de formular una prohibición general sobre el uso, cuyo control material resulta más complejo desde una perspectiva operativa.

Adicionalmente, la Comisión considera conveniente que el proyecto incorpore expresamente medidas para impedir el registro de líneas a nombre de distribuidores o comercializadores cuando estos actúan únicamente como intermediarios en la cadena de venta. Al respecto, la regulación vigente¹⁴ ya contiene disposiciones dirigidas a evitar que las tarjetas SIM sean registradas a nombre

¹⁴ «Artículo 2.1.3.3.7 de la Resolución CRC 5050 de 2016 Prohibición de registro de líneas móviles en la modalidad prepago a nombre de distribuidores y comercializadores. El operador no podrá registrar como titular de la línea móvil en la modalidad prepago a quien adquiera sus SIM físicas o SIM virtuales con el fin de distribuirlas o comercializarlas a terceros». (Subrayado fuera del texto)

de terceros comercializadores en lugar del usuario final que efectivamente utilizará el servicio, medida que contribuye de manera directa a los objetivos de identificación y trazabilidad perseguidos por la iniciativa legislativa.

Finalmente, la CRC estima que los procedimientos específicos asociados a la verificación de identidad durante la activación, las validaciones en tiempo real, los controles operativos sobre distribuidores y comercializadores, así como los mecanismos de suspensión o desactivación por incumplimiento de las obligaciones de registro, deberían desarrollarse posteriormente mediante regulación o reglamentación sectorial, lo que permitiría atender las particularidades operativas del mercado, preservar la neutralidad tecnológica y adaptar dichos mecanismos a la evolución de las tecnologías y modalidades de comercialización de los servicios móviles.

Límites a líneas prepago - Artículo 8

La CRC considera que la restricción prevista en el artículo 8, según la cual ninguna persona natural podrá tener más de cinco (5) líneas móviles prepago activas con un mismo proveedor, podría beneficiarse de una justificación técnica y económica más amplia dentro de la exposición de motivos. Si bien la finalidad de prevenir activaciones masivas asociadas a posibles actividades fraudulentas o delictivas resulta legítima, el proyecto debería incorporar evidencia empírica y sustento técnico que permita concluir que el umbral de cinco líneas constituye una medida necesaria, adecuada o proporcional para alcanzar dicho objetivo.

Debe considerarse, además, que el límite propuesto opera respecto de un mismo proveedor, por lo que no equivale necesariamente a un límite nacional sobre el número de líneas prepago que pueden estar asociadas a una misma persona.

En particular, sería útil incorporar estudios, estadísticas sectoriales, análisis comparados o evaluaciones de impacto regulatorio que expliquen la elección de dicho límite, ni se valoran los posibles efectos sobre usuarios legítimos que, por razones familiares, empresariales, comerciales o de otra índole, puedan requerir un número superior de líneas móviles prepago.

Por lo anterior, además de profundizar en la justificación técnica del umbral escogido, podría resultar útil valorar, de manera complementaria, mecanismos basados en riesgo que permitan identificar patrones atípicos de activación, concentración temporal, reiteración de identidades u otras señales asociadas a posibles usos fraudulentos. Este enfoque permitiría ajustar los umbrales y mecanismos de alerta en función de la evidencia y de la evolución de los riesgos identificados.

Vigilancia, control y competencias institucionales – Artículo 11

La propuesta de funciones de vigilancia y control conjunta entre MinTIC, la SIC y la CRC requiere una delimitación clara de las responsabilidades de cada entidad. Las funciones legalmente asignadas a la CRC se concentran en la regulación técnica y económica del sector de comunicaciones, la promoción de la competencia y la protección de los usuarios, de conformidad con la Ley 1341 de 2009 y la Ley 1978 de 2019.

Esta delimitación también responde a criterios de eficiencia institucional. La diferenciación entre las funciones de regulación, ejecución y vigilancia favorece la especialización de las entidades, facilita la rendición de cuentas y contribuye a una asignación clara de responsabilidades. En este contexto, podría resultar conveniente que la participación de la CRC se concentre en las actividades propias de su función regulatoria y de acompañamiento técnico, de conformidad con su marco legal de competencias.

Reglamentación — artículo 12

Respecto del artículo 12, sería conveniente distinguir la potestad reglamentaria del Gobierno Nacional de las competencias regulatorias asignadas a la CRC, de manera que la coordinación institucional prevista en la iniciativa preserve las responsabilidades propias de cada autoridad. De igual manera, los espacios de coordinación y participación con los operadores y demás actores involucrados pueden aportar elementos relevantes para identificar las condiciones técnicas y operativas necesarias para la implementación de las medidas, sin alterar la competencia decisoria de la autoridad correspondiente. La ley puede establecer los elementos esenciales, mientras que cada autoridad desarrollaría los asuntos comprendidos dentro de sus competencias mediante el instrumento jurídico aplicable. Asimismo, convendría preservar el principio según el cual la reglamentación no puede crear conductas sancionables, sujetos responsables o sanciones que no hayan sido definidos por el legislador.

3. Consideraciones finales

La CRC reconoce la relevancia de la finalidad perseguida por el Proyecto de Ley 077 de 2026 Cámara y los avances que incorpora frente a iniciativas anteriores. En ese marco, considera conveniente que durante el trámite legislativo se profundice en algunos elementos que permitan fortalecer la justificación y el diseño de las medidas propuestas. En particular, resulta importante profundizar en tres aspectos que permitirían fortalecer la justificación y el diseño de la iniciativa:

- (i) Contar con mayor evidencia sobre las dificultades que persisten en materia de identificación y trazabilidad de las líneas móviles. Un análisis más detallado permitiría identificar si las principales dificultades se encuentran en el cumplimiento de las obligaciones existentes, en los procesos de identificación y validación de los usuarios, en la calidad o actualización de la información, en la dispersión de los registros o en el acceso oportuno a estos por parte de las autoridades. Lo anterior, considerado que cada una de estas situaciones puede requerir respuestas distintas.
- (ii) Valorar el beneficio adicional que podrían generar el RNTS y las demás obligaciones previstas frente a los instrumentos actualmente vigentes. Más allá de la utilidad potencial de contar con mayores capacidades de identificación y consulta, resultaría útil profundizar en qué dificultades adicionales podrían atender las nuevas medidas, cuál sería su contribución concreta a los objetivos de prevención e investigación y en qué medida dicho beneficio justificaría los costos, riesgos y cargas asociados a su implementación.
- (iii) Evaluar las alternativas técnicas e institucionales disponibles para alcanzar los objetivos

propuestos. La creación de un registro nacional centralizado constituye una de las opciones posibles, pero resulta pertinente compararla con otros mecanismos de interoperabilidad, consulta y acceso a la información, así como valorar la distribución de responsabilidades entre las entidades involucradas. Este análisis permitiría identificar una solución técnicamente viable, proporcional, segura y suficientemente flexible para adaptarse a la evolución tecnológica y a las nuevas modalidades de fraude.

Este análisis contribuiría a que las medidas finalmente adoptadas respondan de manera proporcional a las problemáticas identificadas, se articulen adecuadamente con el marco regulatorio vigente y conserven la flexibilidad necesaria para adaptarse a la evolución tecnológica y a las nuevas modalidades de fraude.

En estos términos, la CRC reitera su disposición para brindar el acompañamiento técnico necesario durante el trámite legislativo y contribuir a la construcción de un marco normativo que fortalezca la seguridad de los usuarios, proteja los datos personales y preserve la eficiencia regulatoria del sector de comunicaciones

Cordial saludo,

DIAZ SUAZA Firmado digitalmente
por DIAZ SUAZA
FELIPE FELIPE AUGUSTO
AUGUSTO Fecha: 2026.09.21
10:03:02 -05'00'

FELIPE AUGUSTO DÍAZ SUAZA
Director Ejecutivo

Proyectado por: Amparo Cubillos Vargas
Revisado por: Víctor Bladrich
Aprobado por: Zoila Vargas



Calle 59A BIS No. 5-53, Edificio Link Siete Sesenta, piso 9 Bogotá, D.C.
Código postal 110231 - Teléfono +57 601 319 8300
Línea gratuita nacional 018000 919278