REPÚBLICA DE COLOMBIA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XXXIV - Nº 1229 Bogotá, D. C., viernes, 25 de julio de 2025 EDICIÓN DE 17 PÁGINAS

DIRECTORES: DIEGO ALEJANDRO GONZÁLEZ GONZÁLEZ
SECRETARIO GENERAL DEL SENADO
www.secretariasenado.gov.co

JAIME LUIS LACOUTURE PEÑALOZA
SECRETARIO GENERAL DE LA CÁMARA
www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

CÁMARA DE REPRESENTANTES

PROYECTOS DE LEY

PROYECTO DE LEY NÚMERO 038 DE 2025 CÁMARA

por medio del cual se establecen disposiciones para la personalización obligatoria de las tarjetas Sim y se implementan medidas para fortalecer la seguridad en la venta y uso de servicios de telefonía móvil en Colombia.

Bogotá, julio de 2025

Señor

PRESIDENTE

Honorable Cámara de Representantes

Congreso de la República

Ciudad

Referencia: Radicación proyecto de ley, *por medio del cual se establecen disposiciones para la personalización obligatoria de las tarjetas Sim y se implementan medidas para fortalecer la seguridad en la venta y uso de servicios de telefonía móvil en Colombia.*

Honorable Presidente,

De conformidad con lo establecido en la Ley 5ª de 1992, me permito presentar para consideración de la honorable Cámara de Representantes el siguiente proyecto de ley, *por medio del cual se establecen disposiciones para la personalización obligatoria de las tarjetas Sim y se implementan medidas para fortalecer la seguridad en la venta y uso de servicios de telefonía móvil en Colombia.*

Cordialmente,

JULIO ROBERTO SALAZAR PERDOMO
Autor
Representante a la Cámara
Departamento de Cundinamarca

EXPOSICIÓN DE MOTIVOS

por medio del cual se establecen disposiciones para la personalización obligatoria de las tarjetas Sim y se implementan medidas para fortalecer la seguridad en la venta y uso de servicios de telefonía móvil en Colombia.

1. INTRODUCCIÓN

En Colombia, el sector de Tecnologías de la Información y las Comunicaciones (TIC) ha experimentado un crecimiento sostenido, reflejado en el incremento de líneas móviles activas, que para 2023 superaron los 68,5 millones. Este fenómeno ha transformado la vida cotidiana de los ciudadanos, integrando las telecomunicaciones de manera decisiva en las dinámicas sociales, económicas y culturales del país. No obstante, este avance también ha traído consigo nuevos retos, particularmente en cuanto al uso indebido de los servicios móviles. El anonimato de las líneas telefónicas, aprovechado por delincuentes, ha sido un factor crítico en la proliferación de actividades ilícitas como la extorsión, fraude financiero, secuestro y robo de identidad.

Según datos de la Policía Nacional entre 2020 y 2023, cerca del 42% de los casos de extorsión y el 60% de los secuestros extorsivos reportados involucraron líneas móviles mal registradas o completamente anónimas. Este problema también tiene un impacto significativo en la economía del país, ya que un informe de Asobancaria estima que las pérdidas por fraude cibernético derivadas del uso no registrado de líneas móviles superan los 500.000 millones de pesos anualmente. Estos hechos subrayan la necesidad urgente de implementar un sistema de identificación más riguroso para los usuarios de telecomunicaciones, que garantice la trazabilidad de las comunicaciones.

En respuesta a estos problemas, se propone la creación de una base de datos centralizada para el registro de las tarjetas SIM. Esta base permitirá a las autoridades de seguridad y policía acceder de manera eficiente a los datos relacionados con las líneas móviles, facilitando así las investigaciones de actividades delictivas y permitiendo el rastreo de comunicaciones utilizadas con fines ilícitos. El sistema también contempla el uso de protocolos de autenticación avanzados, como la autenticación mutua entre la tarjeta SIM y el equipo móvil, lo que asegurará que solo los usuarios autorizados puedan utilizar los servicios, reduciendo de manera considerable el riesgo de fraudes y accesos no autorizados.

Además, se integrarán políticas de software con la tecnología de las tarjetas SIM para proporcionar mayores niveles de seguridad, garantizando la confidencialidad y protección de los datos en las transacciones móviles. Este enfoque garantizará la integridad de la información de los usuarios y evitará el uso indebido de sus datos. Igualmente, el empleo de procesadores y cifrado seguro en la personalización de las tarjetas SIM permitirá la protección de los datos durante su transmisión y almacenamiento, evitando posibles brechas de seguridad que comprometan la privacidad de los usuarios.

En el ámbito del comercio electrónico móvil, es fundamental lograr un equilibrio entre las medidas de seguridad y la usabilidad de los dispositivos. Plataformas como P3SIM demuestran cómo la seguridad, a través de la tarjeta SIM, se puede integrar sin comprometer la experiencia del usuario, permitiendo transacciones seguras sin dificultar el acceso o la interacción. Aunque la personalización de las tarjetas SIM incrementa la seguridad, también es necesario abordar las preocupaciones sobre privacidad y protección de datos. La recopilación y almacenamiento de información personal en bases de datos centralizadas puede suponer riesgos si no se gestionan adecuadamente, por lo que se requiere un marco legal y reglamentario sólido que asegure la protección de los derechos de los usuarios y la correcta gestión de los datos. Este enfoque debe ser equilibrado, garantizando tanto la seguridad pública como el derecho a la privacidad de los ciudadanos.

Este proyecto de ley se alinea con las mejores prácticas internacionales, adoptando medidas de seguridad y transparencia que no solo fortalecerán la confianza de los usuarios en los servicios móviles, sino que también contribuirán a la lucha contra las organizaciones criminales que abusan de las telecomunicaciones para llevar a cabo actividades ilícitas. Además, esta iniciativa proporciona un marco adecuado para la protección de los derechos de los ciudadanos, asegurando el cumplimiento con las normativas internacionales de protección de datos, como la Ley 1581 de 2012 y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, lo que garantiza la seguridad de los datos personales y la transparencia en su manejo.

2. PROBLEMÁTICA IDENTIFICADA

En Colombia, el crecimiento acelerado del mercado de telecomunicaciones ha impulsado el número de líneas móviles activas a más de 68,5 millones en 2023. Aunque este avance resalta la importancia de las tecnologías móviles en el país, también ha expuesto debilidades críticas en la regulación y seguridad del sector, relacionadas especialmente con el uso indebido de tarjetas SIM y su impacto en la seguridad pública, económica y digital.

2.1. USO DE TARJETAS SIM EN DELITOS DE ALTO IMPACTO

El anonimato en la adquisición y el uso de tarjetas SIM ha emergido como una de las principales vulnerabilidades en el sistema de telecomunicaciones de Colombia, convirtiéndose en una herramienta recurrente utilizada por organizaciones criminales para llevar a cabo diversas actividades ilícitas de alto impacto. Esta problemática se ha convertido en una de las principales fuentes de inseguridad, al facilitar la realización de delitos como la extorsión, el secuestro, el fraude financiero y el robo de identidad. La naturaleza anónima y sin control de la activación de tarjetas SIM permite que individuos y grupos delictivos operen sin ser detectados, lo que genera graves consecuencias tanto a nivel individual como social, afectando directamente la seguridad pública.

Según un informe reciente de la Policía Nacional (2023), el 42% de los casos de extorsión telefónica denunciados entre 2020 y 2023 involucraron líneas móviles adquiridas sin la debida identificación del titular, lo que evidencia la magnitud del problema. Esta cifra resalta la facilidad con la que los delincuentes pueden acceder a medios de comunicación anónimos para realizar actividades delictivas, como la extorsión, sin temor a ser rastreados o identificados por las autoridades.

El impacto de esta práctica trasciende lo individual, ya que afecta gravemente la capacidad de las autoridades para investigar y desarticular redes criminales. El uso de tarjetas SIM mal registradas representa un obstáculo significativo para la trazabilidad de las comunicaciones, dificultando la identificación de los responsables y la judicialización de los delitos. Un estudio realizado por la Fiscalía General de la Nación (2023) demostró que las tarjetas SIM mal registradas son frecuentemente utilizadas en investigaciones de delitos cibernéticos complejos, tales como fraudes financieros y el robo de identidad. Esta situación crea un entorno de impunidad, ya que la falta de trazabilidad de las comunicaciones hace que las autoridades enfrenten grandes dificultades para recopilar pruebas y rastrear a los delincuentes de manera efectiva.

La deficiencia en la trazabilidad de las tarjetas SIM no solo impacta en la capacidad de las fuerzas del orden para resolver casos de delincuencia organizada, sino que también pone en riesgo la integridad del sistema judicial, al dificultar la recopilación de pruebas y la posterior condena de los responsables. En este contexto, resulta urgente establecer un mecanismo

legal que garantice la correcta identificación de los usuarios de tarjetas SIM, lo que permitirá fortalecer la seguridad pública y mejorar la capacidad de respuesta ante los delitos cometidos a través de las telecomunicaciones.

Este panorama revela la necesidad de adoptar medidas legislativas más estrictas para regular la comercialización y activación de tarjetas SIM en Colombia. La implementación de un sistema de registro obligatorio y verificable no solo contribuirá a la lucha contra el crimen organizado, sino que también promoverá un entorno de mayor seguridad para los usuarios de telecomunicaciones, protegiendo sus derechos y garantizando la integridad de los servicios ofrecidos.

2.2. IMPACTO ECONÓMICO Y RIESGOS FINANCIEROS

El uso fraudulento de líneas móviles no solo representa un riesgo para la seguridad pública, sino que también conlleva consecuencias económicas de gran magnitud. Según un informe de la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria) de 2023, las actividades de fraude cibernético facilitadas por comunicaciones móviles anónimas generan pérdidas anuales superiores a 500.000 millones de pesos colombianos. Este tipo de fraude se ha visto favorecido por la falta de identificación y trazabilidad de las líneas móviles, lo que permite a los delincuentes operar con anonimato y cometer actos ilícitos como el fraude financiero, el robo de identidad y el lavado de dinero.

El impacto económico de estas actividades fraudulentas no solo se limita a las pérdidas directas, sino que también afecta la confianza de los usuarios en los servicios financieros digitales. La percepción de inseguridad en las transacciones electrónicas puede inhibir el crecimiento de la economía digital, un sector que es clave para el desarrollo del país. La confianza de los usuarios es un factor fundamental para el impulso de la digitalización de los servicios financieros, la cual, a su vez, se proyecta como uno de los principales motores de la economía colombiana en los próximos años. Si los usuarios no confían en la seguridad de los sistemas, la adopción de tecnologías digitales se verá limitada, afectando tanto a las empresas como a los ciudadanos que desean acceder a servicios financieros más eficientes y transparentes.

Además de los efectos directos sobre la economía digital, la informalidad en la comercialización de tarjetas SIM tiene un impacto negativo en la recaudación fiscal del sector de telecomunicaciones. Este panorama crea una distorsión en el mercado, favoreciendo a los actores informales y dejando de lado la capacidad de generar recursos fiscales que podrían ser utilizados para fortalecer otros sectores estratégicos del país.

La falta de control en la venta de tarjetas SIM no solo representa un reto en términos de seguridad, sino también una pérdida significativa de ingresos para el Estado. La implementación de medidas que garanticen un registro adecuado y verificable de las tarjetas SIM contribuirá no solo a la reducción de actividades ilícitas, sino también a la formalización del sector, lo que permitirá mejorar la recaudación fiscal y promover el desarrollo económico sostenible en Colombia.

2.3. AUMENTO DE LA EXTORSIÓN EN COLOMBIA

La extorsión en Colombia ha experimentado un notable incremento en los últimos años, consolidándose como una de las principales formas de crimen organizado en el país. Este delito, estrechamente vinculado con organizaciones criminales y grupos armados ilegales, es utilizado como una herramienta clave para ejercer control sobre diversos territorios, especialmente en las áreas rurales y apartadas, donde las víctimas suelen estar más desprotegidas. Según las cifras del Ministerio de Defensa Nacional, el primer semestre de 2024 presentó un aumento del 27,5% en los casos de extorsión en comparación con el mismo periodo del año anterior, con Antioquia y Bogotá, D. C., destacándose entre las regiones más afectadas.

Una nueva modalidad de extorsión, conocida como “gota a gota”, ha proliferado en los últimos años. Esta forma de extorsión afecta no solo a individuos con grandes patrimonios, sino también a sectores de la población con menores recursos, garantizando un flujo constante de dinero para los delincuentes mediante pequeñas cuotas. A pesar del creciente número de denuncias, la gran mayoría de las víctimas (79,6%) no denuncia el delito, lo que refleja una falta de confianza en las autoridades y un miedo a represalias por parte de los delincuentes.

La extorsión telefónica carcelaria se ha convertido en una modalidad significativa de este crimen. Dentro de los centros penitenciarios, los reclusos utilizan teléfonos móviles y tarjetas SIM ilegales para coordinar extorsiones, lo que se ve facilitado por la ausencia de controles efectivos sobre el contrabando de dispositivos electrónicos en las cárceles. Esta situación permite a los grupos criminales seguir operando y extendiendo su actividad ilícita desde dentro de los centros de reclusión.

Para abordar esta problemática, es fundamental que los operadores de telecomunicaciones asuman un rol activo en el control de las líneas móviles, dado que tienen acceso a la información necesaria para identificar a los usuarios y bloquear los dispositivos utilizados en actividades delictivas. Sin embargo, la regulación vigente sobre la comercialización y acceso a las tarjetas SIM aún es insuficiente, lo que facilita el anonimato de los delincuentes. La cooperación de los operadores móviles se presenta como una medida esencial para prevenir y mitigar la extorsión carcelaria y otras modalidades delictivas vinculadas con el uso ilegal de las telecomunicaciones.

2.4. BRECHAS REGULATORIAS Y FALTA DE CONTROL OPERATIVO

A pesar de los avances legales alcanzados en Colombia en materia de protección de datos personales, especialmente bajo la Ley 1581 de 2012, que establece principios y normas para garantizar la

privacidad y seguridad de la información personal, persisten vacíos regulatorios significativos en relación con la venta y el registro de tarjetas SIM. Estos vacíos permiten que se continúe facilitando el anonimato en el uso de las telecomunicaciones, lo cual representa un riesgo no solo para la seguridad pública, sino también para la integridad del sistema de telecomunicaciones del país.

Una investigación realizada por la Superintendencia de Industria y Comercio (SIC) en 2022 reveló datos preocupantes que subrayan la magnitud del problema. Más del 15% de las líneas móviles activas en Colombia, lo que equivale a más de 10 millones de tarjetas SIM, no cuentan con un registro válido que permita identificar al titular. Este dato pone de manifiesto que una porción considerable de las líneas móviles operativas en el país no cumple con los requisitos legales de identificación, lo que crea una grave vulnerabilidad en el sistema de telecomunicaciones, facilitando el uso de estas líneas para actividades ilícitas.

Además, el 32% de las tarjetas SIM adquiridas en puntos de venta informales no requieren ningún tipo de identificación para su activación, lo que refuerza el entorno de impunidad y anonimato en las telecomunicaciones. Este porcentaje refleja una práctica extendida que favorece la comercialización de tarjetas SIM sin control o supervisión adecuada, permitiendo que estas sean utilizadas con fines delictivos sin la posibilidad de rastrear a los responsables.

Este panorama de falta de control y transparencia en la comercialización de tarjetas SIM genera un entorno altamente propenso para el anonimato, lo que compromete la trazabilidad de las comunicaciones. La imposibilidad de identificar a los titulares de las líneas móviles dificulta la tarea de las autoridades competentes en la prevención, investigación y resolución de delitos, como la extorsión, el secuestro, el fraude financiero y el robo de identidad. Además, la falta de un sistema robusto de registro incrementa la probabilidad de que estas líneas sean utilizadas por organizaciones criminales, que las emplean como una herramienta eficaz para ocultar su identidad y operar sin ser detectadas.

Es imperativo que se establezcan mecanismos más estrictos y efectivos para regular la venta y el registro de tarjetas SIM, garantizando así una mayor seguridad y confianza en los servicios de telecomunicaciones. La adopción de medidas de personalización obligatoria, junto con un sistema de registro centralizado y verificable, permitirá mitigar los riesgos asociados con el uso anónimo de las líneas móviles y contribuirá al fortalecimiento de la seguridad pública y la lucha contra el crimen organizado.

3. COMPARACIÓN CON MODELOS INTERNACIONALES EXITOSOS

La problemática del anonimato en las telecomunicaciones no es exclusiva de Colombia; muchos países han enfrentado desafíos similares y han implementado políticas efectivas que pueden servir como referencia para el contexto nacional. Las experiencias de países como España, México y Alemania demuestran cómo la personalización obligatoria de tarjetas SIM y la creación de registros centralizados pueden transformar el panorama de la seguridad en las telecomunicaciones, al tiempo que fortalecen la confianza de los usuarios y reducen el impacto de actividades ilícitas.

3.1. ESPAÑA: UN MODELO DE REGULACIÓN EFECTIVA

En 2007, España adoptó una medida regulatoria fundamental al implementar la obligatoriedad del registro de tarjetas SIM. Esta normativa exigió a los operadores de telecomunicaciones vincular cada tarjeta SIM a una persona identificada a través de documentos oficiales, como la tarjeta de identidad o el pasaporte. La finalidad de esta medida fue cerrar las brechas de anonimato en las telecomunicaciones, lo que permitió mejorar significativamente la seguridad del sistema móvil en el país. Entre los resultados más destacados de esta política se encuentran los siguientes:

En primer lugar, se logró una reducción del 25% en los delitos relacionados con telecomunicaciones durante los primeros cinco años de implementación de la normativa, según datos proporcionados por el Ministerio del Interior español. Esta disminución en los delitos, tales como extorsiones telefónicas, fraude, y actividades ilícitas relacionadas con el uso anónimo de las líneas móviles, demuestra la efectividad de la personalización obligatoria de tarjetas SIM en la lucha contra el crimen organizado y otros delitos complejos.

En segundo lugar, la implementación de esta normativa facilitó un incremento significativo en la colaboración entre los operadores de telecomunicaciones y las autoridades judiciales. Esta cooperación mejorada permitió una resolución más eficaz de casos relacionados con el crimen organizado y las actividades terroristas, ya que la trazabilidad de las comunicaciones se volvió mucho más efectiva. Las autoridades pudieron acceder de manera más rápida y precisa a la información necesaria para llevar a cabo investigaciones y desmantelar redes criminales.

Un tercer beneficio significativo fue la mejora de la percepción pública sobre la seguridad de las telecomunicaciones. Según datos del Instituto Nacional de Estadística (INE) de España, en 2022, el 78% de los usuarios de servicios móviles indicaron que las medidas implementadas para la personalización obligatoria de las tarjetas SIM habían aumentado su confianza en los servicios móviles. Esta mejora en la confianza no solo fortaleció el sector de las telecomunicaciones, sino que también contribuyó a un entorno más seguro para los usuarios, promoviendo una mayor adopción de servicios digitales y una participación activa en la economía digital.

Por último, España también incorporó el uso de verificaciones biométricas en ciertos procesos relacionados con las telecomunicaciones, como la portabilidad de números telefónicos. Este enfoque tecnológico adicional sirvió para garantizar un nivel de seguridad aún más alto, evitando la suplantación de identidad y brindando una capa extra de protección a los usuarios y a los operadores. La implementación de tecnologías biométricas, como el reconocimiento facial y la autenticación mediante huella dactilar, podría ser un modelo a seguir en Colombia para maximizar los resultados en términos de seguridad y trazabilidad de las comunicaciones.

3.2. MÉXICO: UN CASO DE REDUCCIÓN DEL CRIMEN ORGANIZADO

En 2009, México implementó el Registro Nacional de Usuarios de Telefonía Móvil (Renaut), una iniciativa clave diseñada para combatir el uso de líneas móviles en actividades delictivas, particularmente en extorsiones telefónicas y secuestros. Esta medida buscaba proporcionar una solución para el anonimato en las telecomunicaciones, el cual era aprovechado por organizaciones criminales para operar sin ser detectadas por las autoridades. Aunque el sistema enfrentó retos en su implementación, los primeros años de operación demostraron resultados positivos significativos:

Durante los tres primeros años de operación del Renaut, el uso de líneas móviles en actividades delictivas disminuyó en un 35%, según datos de la Procuraduría General de la República. Este descenso en los delitos demuestra la efectividad del sistema de registro obligatorio, que facilitó la trazabilidad de las comunicaciones y permitió identificar a los responsables de actividades criminales, especialmente en delitos de alto impacto como la extorsión telefónica y el secuestro.

Otro de los beneficios importantes del Renaut fue el fortalecimiento de la capacidad de las autoridades para rastrear las comunicaciones utilizadas en delitos graves. La implementación del registro permitió mejorar los índices de resolución de casos en un 20%, ya que las fuerzas de seguridad pudieron acceder con mayor rapidez y precisión a los datos necesarios para llevar a cabo investigaciones criminales. Esta mejora en la capacidad de resolución de casos fue fundamental para la efectividad del sistema judicial en el combate al crimen organizado.

Sin embargo, a pesar de estos avances, el sistema fue descontinuado en 2012 debido a problemas administrativos y la falta de un control efectivo en su implementación. Este desmantelamiento dejó en evidencia la importancia de un diseño robusto y de una supervisión adecuada para que políticas de esta naturaleza sean realmente efectivas. El fracaso del Renaut en México subraya la necesidad de asegurar una implementación adecuada, con controles rigurosos y una infraestructura tecnológica que garantice la fiabilidad y seguridad de los datos registrados.

El caso mexicano resalta valiosas lecciones que deben ser tenidas en cuenta en la implementación de políticas similares en Colombia. Para evitar los errores que llevaron al fracaso del Renaut en México, es crucial que en el contexto colombiano se garantice una gestión eficiente del sistema de registro, con un enfoque en la protección de datos personales, la interoperabilidad entre operadores y autoridades, y el establecimiento de un marco legal que asegure el cumplimiento continuo de las disposiciones. Además, es necesario que las políticas sean sostenibles a largo plazo, con la infraestructura y los recursos adecuados para enfrentar los desafíos de seguridad y privacidad que puedan surgir.

3.3. ALEMANIA: LIDERAZGO EN SEGURIDAD Y TRAZABILIDAD

Alemania ha sido pionera en la implementación de medidas avanzadas de registro y personalización de tarjetas SIM, con la introducción de la verificación biométrica obligatoria en 2018. Estas políticas han producido resultados notables en términos de seguridad y trazabilidad de las comunicaciones:

Entre 2018 y 2022, los delitos relacionados con el uso de comunicaciones móviles disminuyeron un 30%, según la Oficina Federal de la Policía Criminal (BKA). Esta reducción destaca la efectividad de la personalización obligatoria de tarjetas SIM para frenar actividades ilícitas como la extorsión, el fraude y el terrorismo.

Además, la implementación de estas medidas mejoró la trazabilidad de las comunicaciones, facilitando las investigaciones complejas, especialmente en casos de cibercrimen y terrorismo. La capacidad de rastrear las comunicaciones en tiempo real ha sido crucial para desmantelar redes criminales y prevenir delitos de alto impacto.

Otro aspecto relevante es la adopción de estándares internacionales de protección de datos, como el Reglamento General de Protección de Datos (RGPD), que ha fortalecido la confianza de los usuarios en los servicios móviles. Esta regulación asegura el manejo ético y seguro de la información personal, protegiendo la privacidad de los ciudadanos y garantizando la integridad de los datos.

Finalmente, Alemania ha implementado sistemas de auditoría y monitoreo continuo para garantizar la integridad y seguridad de sus bases de datos, un enfoque que puede servir como modelo para la creación de la Base de Datos Nacional de Registro de Tarjetas SIM en Colombia. Estas medidas asegurarían que la información registrada se mantenga segura y que el acceso sea restringido a las autoridades competentes, garantizando la confianza del público y la eficiencia de las políticas de seguridad.

3.4. APRENDIZAJES Y APLICACIONES PARA COLOMBIA

La comparación internacional demuestra que las políticas de personalización obligatoria y registro centralizado de tarjetas SIM son herramientas efectivas para combatir el crimen, aumentar la seguridad pública y proteger los derechos de los

usuarios. No obstante, para garantizar el éxito de su implementación en Colombia, es fundamental que se consideren varios aspectos clave basados en las lecciones aprendidas de otros países con experiencia exitosa en este campo:

En primer lugar, el diseño robusto del sistema de registro es esencial para asegurar su efectividad. Aprendiendo del caso mexicano, es crucial que el sistema garantice la interoperabilidad entre los operadores de telecomunicaciones y las autoridades correspondientes. Asimismo, debe contar con controles rigurosos para evitar inconsistencias en los datos, lo cual es vital para que el sistema sea confiable y eficaz en la identificación de los usuarios de las tarjetas SIM, evitando fallos que puedan poner en riesgo su operatividad.

En segundo lugar, la incorporación de tecnologías avanzadas es un factor clave para fortalecer la seguridad del sistema. Tal como se observó en Alemania, la implementación de verificaciones biométricas para validar la identidad de los usuarios, como la huella dactilar o el reconocimiento facial, ofrecería un nivel adicional de seguridad y ayudaría a evitar la suplantación de identidad. Esto no solo contribuiría a la prevención de delitos, sino que también mejoraría la confianza de los usuarios en la integridad del sistema.

Además, el cumplimiento normativo y el respeto por la privacidad de los usuarios deben ser una prioridad en el diseño de este sistema. Siguiendo el ejemplo de España, Colombia debe asegurar que el sistema cumpla con los más altos estándares de protección de datos personales, garantizando que la información recabada se maneje de manera ética, segura y conforme con las leyes nacionales e internacionales de privacidad. Este compromiso con la protección de los datos personales fortalecería la confianza de los ciudadanos en los servicios de telecomunicaciones y fomentaría la participación activa de los usuarios en el proceso.

Finalmente, la colaboración interinstitucional es un elemento fundamental para el éxito de estas políticas. La experiencia internacional resalta la importancia de la cooperación entre las entidades regulatorias, los operadores de telecomunicaciones y las autoridades judiciales. Un esfuerzo conjunto aseguraría que las políticas se implementen de manera coherente y efectiva, maximizando su impacto en la seguridad y la justicia. Esta colaboración también facilitaría la resolución rápida de posibles conflictos y la adecuada supervisión del sistema.

En resumen, la implementación de medidas basadas en modelos internacionales exitosos tiene el potencial de transformar el entorno de las telecomunicaciones en Colombia. Al considerar estos aspectos clave y adoptando un enfoque integral, Colombia no solo mejoraría la seguridad pública y la trazabilidad de las comunicaciones, sino que también se posicionaría como un líder regional en la regulación responsable y efectiva del sector de telecomunicaciones.

4. OBJETIVOS DEL PROYECTO DE LEY

4.1. OBJETIVO GENERAL

Fortalecer la seguridad pública y la protección de datos personales en Colombia mediante la personalización obligatoria de tarjetas SIM y la creación de una Base de Datos Nacional de Registro de Tarjetas SIM, promoviendo así la trazabilidad de las telecomunicaciones y el cumplimiento de estándares internacionales en seguridad y privacidad.

4.2. OBJETIVOS ESPECÍFICOS

4.2.1. GARANTIZAR LA IDENTIFICACIÓN DE LOS USUARIOS DE TARJETAS SIM

En la actualidad, más del 15% de las líneas móviles activas en Colombia, lo que equivale a más de 10 millones de tarjetas SIM, no cuentan con un registro válido del titular, según datos proporcionados por la Superintendencia de Industria y Comercio (2022). Este vacío en la regulación ha creado una brecha significativa en la seguridad de las telecomunicaciones y ha facilitado el uso de líneas móviles en actividades ilícitas. Con el objetivo de abordar esta problemática, este proyecto de ley propone la implementación de un sistema de personalización obligatoria para todas las tarjetas SIM en el país. El propósito es garantizar que cada línea móvil esté vinculada a una persona identificada de manera inequívoca mediante documentos oficiales, eliminando así el anonimato que actualmente permite que se realicen actividades delictivas.

A través de la implementación de este sistema, se espera reducir a menos del 2% el porcentaje de líneas móviles no registradas en los primeros tres años de vigencia de la ley. Esto no solo mejorará la seguridad en el sector de las telecomunicaciones, sino que también facilitará la identificación y localización de los responsables en caso de que se utilicen las líneas para actividades ilícitas.

Uno de los objetivos primordiales de esta medida es prevenir el uso de líneas móviles en delitos como la extorsión, el secuestro y el fraude, los cuales actualmente representan más del 40% de los delitos reportados en el ámbito de las telecomunicaciones, según la Policía Nacional. Al garantizar la identificación de los usuarios, se reducirá significativamente el anonimato que facilita la comisión de estos delitos, permitiendo que las autoridades puedan rastrear las comunicaciones y actuar con mayor efectividad frente a las organizaciones criminales que utilizan las telecomunicaciones como herramienta para ejecutar sus actividades ilegales.

4.2.2. CREAR UNA BASE DE DATOS NACIONAL CENTRALIZADA

La fragmentación actual de los registros de tarjetas SIM administrados por los operadores de telecomunicaciones dificulta la trazabilidad efectiva de las líneas móviles en Colombia. Esta situación genera un entorno en el que la información se encuentra dispersa y no es fácilmente accesible

por las autoridades, lo que retrasa la capacidad de respuesta ante actividades ilícitas que utilizan líneas móviles como herramienta para operar. Con el fin de superar esta limitación y mejorar la seguridad en las telecomunicaciones, se propone el diseño y la operación de una Base de Datos Nacional de Registro de Tarjetas SIM, que centralice la información de más de 68,5 millones de líneas móviles activas en el país. Esta base de datos centralizada permitirá contar con un sistema único, que facilitará la identificación de titulares y mejorará la trazabilidad de las líneas móviles.

Una de las claves para el éxito de esta medida es garantizar la interoperabilidad entre la Base de Datos Nacional de Registro de Tarjetas SIM y las plataformas de los operadores de telecomunicaciones. Al integrar estos sistemas, se logrará reducir los tiempos de respuesta en las solicitudes de información por parte de las autoridades judiciales, pasando de semanas a solo horas. Este cambio permitirá una acción más rápida y efectiva frente a delitos como la extorsión, el secuestro y el fraude, facilitando la identificación de los responsables y mejorando la capacidad de las fuerzas de seguridad para resolver casos de manera más eficiente.

Además, se establecerán estándares avanzados de protección de datos personales, alineados con la Ley 1581 de 2012 y con los estándares internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Esta normativa garantizará que la información personal de los usuarios de telecomunicaciones se maneje de manera ética, segura y conforme a las mejores prácticas internacionales, protegiendo así los derechos de los usuarios y promoviendo la confianza en el sistema de registro. La implementación de estos estándares también contribuirá a la transparencia del proceso y a la protección contra el uso indebido de la información almacenada en la base de datos.

4.2.3. IMPLEMENTAR VERIFICACIONES BIOMÉTRICAS PARA NUEVAS ACTIVACIONES.

Según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic, 2023), más del 35% de las tarjetas SIM vendidas en puntos informales no requieren identificación del comprador. Esta práctica facilita el anonimato y contribuye al uso indebido de las líneas móviles en actividades ilícitas, lo que representa un riesgo para la seguridad pública. Para contrarrestar esta situación, el proyecto de ley propone establecer la obligatoriedad de sistemas de verificación biométrica, como el reconocimiento facial o la autenticación por huella dactilar, en el proceso de activación de nuevas tarjetas SIM.

El objetivo es garantizar que, en los primeros dos años de implementación, al menos el 90% de las activaciones de tarjetas SIM se realicen bajo este esquema de verificación biométrica. Esta medida no solo mejorará la seguridad en la activación de las líneas móviles, sino que también permitirá una mayor trazabilidad de las comunicaciones, dificultando el uso de las tarjetas SIM para actividades delictivas. Al implementar este sistema, se fortalecerá la identificación de los usuarios y se reducirá el riesgo de fraude y otros delitos relacionados con el anonimato en las telecomunicaciones.

4.2.4. PREVENIR EL USO DE TARJETAS SIM ANÓNIMAS

El uso de líneas móviles no personalizadas está estrechamente vinculado con delitos de alto impacto, como la extorsión telefónica y el fraude financiero, que generan pérdidas anuales superiores a 500.000 millones de pesos, según datos de Asobancaria (2023). Para hacer frente a esta problemática y mejorar la seguridad en las telecomunicaciones, el proyecto de ley propone medidas estrictas para erradicar el uso de tarjetas SIM no registradas. En primer lugar, se busca prohibir la comercialización y activación de tarjetas SIM sin un registro previo en la base de datos nacional, garantizando que todas las líneas móviles estén vinculadas a una persona identificada de manera verificable.

Como resultado de estas acciones, se espera reducir en un 30% las denuncias de extorsión telefónica relacionadas con líneas móviles anónimas en los primeros cinco años de implementación de la ley. Esta reducción no solo contribuiría a la disminución de delitos graves, sino también a la mejora en la confianza de los usuarios en los servicios móviles, creando un entorno más seguro y controlado para las comunicaciones en el país.

4.2.5. PROTEGER LA PRIVACIDAD Y LOS DATOS PERSONALES

La ausencia de controles estrictos en la comercialización de tarjetas SIM expone a los usuarios a riesgos graves, como el robo de identidad y el acceso no autorizado a información sensible. Esta situación resalta la necesidad de establecer medidas adicionales de seguridad para proteger los datos personales de los usuarios. Con este objetivo, el proyecto de ley propone la implementación de sistemas de cifrado avanzados y controles de acceso rigurosos para proteger los datos almacenados en la Base de Datos Nacional de Registro de Tarjetas SIM. Estos sistemas garantizarán que la información contenida en la base de datos esté protegida frente a accesos no autorizados, fortaleciendo la seguridad de los usuarios de telecomunicaciones.

Además, se establecerá que el acceso a la información almacenada en la base de datos sea restringido exclusivamente a las autoridades competentes, en cumplimiento con los principios de confidencialidad, necesidad y proporcionalidad establecidos en la Ley 1581 de 2012, que regula la protección de datos personales en Colombia. Esta medida asegurará que la información solo sea consultada y utilizada para fines específicos y legales, respetando los derechos de los usuarios y garantizando que los datos no sean utilizados de manera inapropiada o fuera de los marcos establecidos.

Finalmente, se garantizará que el 100% de las consultas realizadas a la base de datos sean rastreables y auditables. Esto permitirá que cualquier acceso a la información sea debidamente registrado, evitando posibles abusos en el manejo de los datos y asegurando que se pueda realizar un seguimiento adecuado de las consultas realizadas por las autoridades. La implementación de este sistema de auditoría y trazabilidad contribuirá a la transparencia y responsabilidad en la gestión de la información, promoviendo la confianza del público y la efectividad de las políticas de seguridad en las telecomunicaciones.

4.2.6. MEJORAR LA COOPERACIÓN ENTRE OPERADORES Y AUTORIDADES

Actualmente, las autoridades judiciales enfrentan serias dificultades para obtener información precisa y oportuna sobre las líneas móviles utilizadas en investigaciones penales, lo que retrasa el curso de las investigaciones y limita la efectividad en la resolución de delitos. Para mejorar esta situación y agilizar el acceso a la información necesaria para la lucha contra el crimen, este proyecto propone una serie de medidas orientadas a optimizar la colaboración entre los operadores de telecomunicaciones y las autoridades competentes.

En primer lugar, se propone establecer protocolos claros y específicos para la colaboración entre los operadores de telecomunicaciones y las autoridades judiciales. Estos protocolos garantizarán que los operadores estén obligados a proporcionar información relevante de manera rápida y eficiente, respetando siempre las normas legales y protegiendo los derechos de los usuarios. La creación de estos protocolos facilitará una comunicación más fluida y eficaz, reduciendo los tiempos de respuesta y mejorando la cooperación entre ambas partes.

Uno de los objetivos clave del proyecto es reducir los tiempos de entrega de la información solicitada en investigaciones judiciales en al menos un 50%. Esto se logrará mediante la implementación de sistemas tecnológicos avanzados que permitan la consulta y entrega de datos en tiempo real, eliminando los retrasos actuales en el proceso de obtención de información. Este cambio no solo mejorará la eficiencia de las investigaciones, sino que también incrementará la capacidad de las autoridades para actuar rápidamente ante delitos graves, como el secuestro, la extorsión y el fraude.

Además, se promoverá la capacitación continua de los operadores de telecomunicaciones y los funcionarios públicos en el manejo seguro de datos y en el cumplimiento de los estándares legales establecidos. Esta capacitación será esencial para asegurar que tanto los operadores como las autoridades comprendan la importancia de la protección de datos personales, así como las obligaciones legales que deben cumplir en el proceso de entrega y manejo de la información. El objetivo es garantizar que la información sensible se maneje de manera ética y conforme con la legislación vigente, evitando posibles abusos y protegiendo la privacidad de los usuarios.

4.2.7. ALINEAR A COLOMBIA CON ESTÁNDARES INTERNACIONALES

Colombia ocupa actualmente el puesto 67 de 141 países en el Índice de Adopción Digital, según el Banco Mundial (2022), lo que refleja una situación en la que, a pesar de los avances, persisten limitaciones significativas en la seguridad de las telecomunicaciones. Esta clasificación se ve afectada por el uso indebido de tarjetas SIM no personalizadas y el anonimato en las comunicaciones, lo que permite la proliferación de delitos como la extorsión, el fraude y el secuestro. Este proyecto de ley busca mejorar esta situación mediante la adopción de prácticas exitosas implementadas en países como España, México y Alemania, que han logrado reducir hasta en un 35% los delitos relacionados con el uso de tarjetas SIM tras la implementación de registros obligatorios.

5. FUNDAMENTOS NORMATIVOS

- **Ley 37 de 1993,** ***por el cual se regula la prestación del servicio de telefonía móvil celular, la celebración de contratos de sociedad y de asociación en el ámbito de las comunicaciones y se dictan otras disposiciones.***

Esta ley regula la prestación del servicio de telefonía móvil celular, su concesión y la implementación de redes de telecomunicaciones móviles, con el objetivo de garantizar la accesibilidad, transparencia y eficiencia en el uso de este servicio. Se establece que la telefonía móvil celular es un servicio público de telecomunicaciones de cobertura nacional que permite la comunicación entre usuarios móviles y entre estos y usuarios fijos, a través de la red pública conmutada. La ley dispone que la prestación del servicio estará a cargo del Estado, quien podrá delegar su operación mediante concesiones a empresas privadas o mixtas, a través de procesos de licitación pública, asegurando que las concesiones se otorguen bajo principios de igualdad y acceso democrático en audiencias públicas.

Además, se establece que las redes deben cubrir todo el territorio nacional y operar de manera interconectada, y que el espectro radioeléctrico, asignado por el Estado, será dividido en canales que se reutilizarán en diferentes áreas para asegurar el servicio. La ley también contempla la participación de la inversión extranjera en el sector de telecomunicaciones, asegurando que se regirá bajo la legislación vigente de 1991, y que las limitaciones para los servicios se regirán por las normativas pertinentes. En cuanto al control del espectro radioeléctrico, el Ministerio de Comunicaciones es responsable de asignar las frecuencias necesarias para el servicio de telefonía móvil celular, organizando su distribución y cobertura en diversas áreas geográficas. También se establece un sistema de interconexión entre redes de telefonía fija y móvil bajo condiciones de igualdad y se asegura que no se producirán prácticas monopolísticas en el mercado de telecomunicaciones. Las empresas concesionarias deberán ser sociedades anónimas, y en ciertos

casos, estas deberán transformarse en sociedades anónimas abiertas para garantizar la transparencia y participación pública. Además, las concesionarias deben presentar un plan de expansión del servicio, que incluya la cobertura de zonas rurales y de difícil acceso, con un plazo máximo de cinco años para su implementación. De esta manera, tenemos que la Ley 37 de 1993 establece un marco legal para la regulación y concesión del servicio de telefonía móvil en Colombia, con un enfoque en la expansión, transparencia, y control del espectro radioeléctrico, promoviendo la competencia y la inversión en el sector de telecomunicaciones.

Decreto número 741 de 1993, "por el cual se reglamenta la telefonía móvil celular".

El decreto regula la telefonía móvil celular en Colombia, estableciendo los lineamientos para su prestación, operación y concesión. Se aplica a las redes y servicios públicos de telefonía móvil celular y establece los procedimientos para su concesión a empresas estatales, de economía mixta o privadas. Este decreto busca garantizar el acceso al servicio de telefonía móvil en todo el territorio nacional, con especial énfasis en zonas rurales y de difícil acceso, bajo condiciones técnicas y financieras específicas.

El decreto define que la telefonía móvil celular es un servicio público de telecomunicaciones, no domiciliario, de cobertura nacional, y su prestación estará bajo el control del Ministerio de Comunicaciones. Además, se detallan las infraestructuras necesarias para la prestación del servicio, como las redes de conmutación, radiación, transmisión y localización, las cuales deben interconectarse con la red pública conmutada.

El espectro radioeléctrico es considerado un bien público, cuya asignación y uso para la telefonía móvil celular requiere autorización previa del Ministerio de Comunicaciones. Se establece también que los operadores deben cumplir con la normativa relacionada con la interconexión, el acceso al servicio, y la competencia, garantizando que no haya prácticas monopolísticas.

El proceso de concesión se realizará mediante licitación pública, y las empresas postulantes deben presentar planes de expansión y cobertura, especialmente para las áreas más necesitadas.

- Ley 1266 de 2008, "por la cual se dictan las disposiciones generales del habeas 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".

Esta ley regula el manejo y tratamiento de los datos personales en Colombia, en particular, la información financiera, crediticia, comercial y de servicios. Su principal objetivo es proteger el derecho constitucional de las personas a conocer, actualizar y rectificar los datos que se encuentran en bancos de datos, garantizando la privacidad y la protección de la información personal. La ley establece principios claros sobre cómo deben ser recolectados, gestionados y circulados estos datos, con énfasis en la calidad, veracidad, y seguridad de la información.

Esta ley se aplica a todas las bases de datos, tanto públicas como privadas, que contienen datos personales, exceptuando aquellos relacionados con inteligencia de Estado y ciertos registros públicos. Asimismo, otorga derechos a los titulares de la información, como el acceso a los datos que se almacenan sobre ellos, la corrección de datos erróneos y la consulta sobre el uso que se da a su información.

En cuanto a las entidades que manejan estos datos (operadores, fuentes y usuarios), la ley establece deberes específicos, tales como garantizar la seguridad de los datos, actualizar la información periódicamente, y asegurar que el acceso esté restringido a personas autorizadas. También prohíbe la circulación de datos personales sin la debida autorización o sin cumplir con las condiciones establecidas.

Los bancos de datos financieros, crediticios y comerciales, así como aquellos provenientes de terceros países, deben ser administrados de manera que favorezcan la expansión del crédito y no afecten injustamente a los titulares. Además, se establece la obligación de reportar información negativa sobre las deudas de los titulares únicamente después de un proceso previo de comunicación, para que estos puedan demostrar el pago o rectificar la información.

La ley también regula las sanciones que pueden imponer las autoridades competentes, como la Superintendencia de Industria y Comercio, por el incumplimiento de las disposiciones relacionadas con el manejo de datos. Las sanciones incluyen multas y la suspensión de actividades de los bancos de datos, y las empresas deben demostrar que están cumpliendo con las obligaciones de la ley a través de medidas de seguridad y políticas internas adecuadas. De acuerdo con la Resolución número 0912 de 2008 del Ministerio de Defensa, el artículo 3° establece lo siguiente:

"Al momento de activar una línea telefónica, los concesionarios y licenciatarios deberán registrar inmediatamente en sus respectivas bases de datos los siguientes datos: el nombre completo del suscriptor o usuario, el número de identificación, el tipo de documento de identificación (CC, CE, Pasaporte, NIT, TI), el número de la línea telefónica fija o móvil, el número de identificación (ID) y, en su caso, la Flota. Este registro se realizará independientemente de la legalización posterior de los otros datos solicitados en el Anexo Uno (1)".

- La Ley 1341 de 2009, por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las Comunicaciones (TIC), se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Se establece el marco general para el desarrollo y regulación del sector de Tecnologías de la Información

y las Comunicaciones (TIC) en Colombia, con el objetivo de promover el acceso universal a las TIC y asegurar su integración eficiente en los procesos sociales, económicos y culturales del país. Esta ley busca garantizar el acceso a la información, promover la competitividad, fortalecer la infraestructura tecnológica, y asegurar el cumplimiento de los derechos de los usuarios. Define las políticas públicas para la gestión y administración de las redes y servicios de telecomunicaciones, buscando un equilibrio entre el desarrollo tecnológico y la protección de los derechos de los usuarios. En términos de acceso universal, prioriza el acceso a las TIC, especialmente en zonas rurales y para poblaciones vulnerables, promoviendo la inclusión digital como una estrategia para reducir la brecha digital. La ley también fomenta la competencia, estableciendo principios para asegurar una competencia leal y abierta en el sector, protegiendo al usuario final de prácticas monopólicas. Además, refuerza la protección de los derechos de los usuarios de servicios TIC, garantizando la calidad, la transparencia en la información y precios justos para los servicios de telecomunicaciones.

En cuanto a la infraestructura y el espectro radioeléctrico, regula la asignación del espectro, promoviendo su uso eficiente para el desarrollo de las TIC en Colombia y asegurando la cobertura a nivel nacional, con especial atención a las zonas de difícil acceso. La ley también incentiva la creación de contenidos y aplicaciones que promuevan la educación, la cultura y el desarrollo productivo, especialmente en sectores rurales y vulnerables. Otro aspecto relevante es el fomento de la digitalización del gobierno y la oferta de servicios públicos a través de plataformas en línea, contribuyendo a la eficiencia y transparencia en la administración pública. Finalmente, la ley define las funciones de la Comisión de Regulación de Comunicaciones (CRC), encargada de promover la competencia en el sector, garantizar la calidad de los servicios y regular el uso de las infraestructuras tecnológicas.

- A su vez, ***el Decreto número 1630 de 2011, por medio del cual se adoptan medidas para restringir la operación de equipos terminales hurtados que son utilizados para la prestación de servicios de telecomunicaciones móviles.***

El decreto tiene como objetivo principal establecer medidas para restringir el uso de equipos terminales móviles que hayan sido reportados como hurtados o extraviados, en la prestación de servicios de telecomunicaciones móviles en Colombia. A través de la creación de bases de datos positivas y negativas, se garantiza que estos dispositivos no sean utilizados en redes de telecomunicaciones móviles, promoviendo así la seguridad y protección de los usuarios.

El decreto define términos clave como IMEI (código único de identificación para cada dispositivo móvil), y establece la obligación para los proveedores de redes y servicios de telecomunicaciones móviles (PRSTM) de implementar, mantener y operar un sistema centralizado de bases de datos donde se registren los IMEI de los equipos móviles. Estos deben ser verificados al momento de la activación de los dispositivos. La base de datos negativa contiene los IMEI de los dispositivos reportados como hurtados, mientras que la base de datos positiva alberga los dispositivos que ingresan legalmente al país, registrando el IMEI junto con la información del propietario.

El decreto regula también la venta de equipos móviles, indicando que sólo las personas autorizadas pueden realizarla, y establece que cualquier dispositivo vendido debe estar homologado conforme a las normas establecidas por la Comisión de Regulación de Comunicaciones (CRC). Los PRSTM deben verificar los IMEI al momento de la venta y activación de los equipos, asegurando que no estén en la base de datos negativa.

Los importadores y fabricantes de equipos móviles tienen la responsabilidad de registrar los IMEI de los dispositivos que ingresan al país o se fabrican localmente, garantizando que los equipos sean legales y seguros para su comercialización y uso. Además, se establece un sistema de actualización de las bases de datos y un procedimiento para la reactivación de dispositivos que hayan sido recuperados y estén en la base de datos negativa.

- **La Ley 1801 de 2016, también conocida como el Código Nacional de Seguridad y Convivencia Ciudadana**

Tiene como objetivo principal establecer un marco normativo que regule el comportamiento de los ciudadanos, así como las obligaciones y responsabilidades de los operadores de servicios públicos, con el fin de garantizar la convivencia pacífica y la seguridad en el ámbito nacional. En su artículo 95, esta ley subraya la responsabilidad que tienen los operadores de telecomunicaciones de mantener la información actualizada de los titulares de las líneas móviles activas, independientemente de la modalidad del servicio que se preste, es decir, ya sea prepago o postpago. Esta disposición busca asegurar que las autoridades tengan acceso a información verídica y actualizada sobre los usuarios de los servicios de telecomunicaciones, lo que resulta crucial para la implementación de medidas de seguridad y control en el sector. La ley también establece que ciertos comportamientos relacionados con el uso de los equipos móviles afectan directamente la seguridad de las personas y sus bienes, en particular aquellos comportamientos vinculados con la activación de las líneas telefónicas. Entre las infracciones mencionadas, destacan las siguientes:

1. Activar líneas telefónicas sin que el usuario haya suministrado los datos biográficos al prestador del servicio en el momento de la activación. Esta práctica pone en riesgo la seguridad de las personas, ya que facilita el uso de líneas móviles sin una debida identificación del titular, lo que puede ser aprovechado por individuos con fines

delictivos. La activación de líneas sin verificar la identidad del usuario es una violación a las normas de seguridad establecidas, ya que impide rastrear a los responsables en caso de actividades ilícitas que involucren esas líneas.

2. Activación de tarjetas SIM (IMSI) sin que el usuario haya proporcionado al prestador del servicio los datos biográficos al momento de la activación. Esta situación también representa un riesgo considerable para la seguridad, ya que la tarjeta SIM, que es fundamental para el funcionamiento de la línea móvil, puede ser utilizada sin que se haya validado la identidad del propietario de la línea. La falta de esta validación permite que las tarjetas SIM sean utilizadas con fines ilícitos, como fraudes, extorsiones o el uso anónimo de los servicios móviles en actividades delictivas.

- **La Resolución CRC 5050 de 2016,** en su artículo 2.1.10.8.

Establece la obligatoriedad para los proveedores de servicios de telefonía fija de ofrecer a sus usuarios, sin costo adicional, el servicio de identificación de llamadas. Además, el artículo 2.1.10.7 detalla las condiciones para la implementación del servicio de código secreto, especificando que debe ser proporcionado a los usuarios como un servicio suplementario, con el objetivo de prevenir la generación de llamadas no consentidas que pudieran ocasionar cargos adicionales fuera de las llamadas locales.

En el caso de nuevas líneas, los proveedores deben entregar automáticamente el código secreto al usuario que suscribe el contrato, junto con el contrato correspondiente, sin que el usuario necesite solicitarlo. También se debe proporcionar información clara sobre cómo acceder al servicio, cómo utilizarlo adecuadamente y las ventajas que ofrece en términos de seguridad.

Adicionalmente, la resolución establece que la información sobre el uso y los beneficios del servicio de código secreto debe ser entregada a los usuarios trimestralmente, utilizando procedimientos idóneos y verificables, para garantizar que los usuarios estén debidamente informados y puedan aprovechar las ventajas de este servicio de manera efectiva.

- ***La Ley 1908 de 2018, por medio de la cual se fortalecen la investigación y judicialización de organizaciones criminales, se adoptan medidas para su sujeción a la justicia y se dictan otras disposiciones.***

Establece en su artículo 11 una regulación específica sobre el manejo de las llamadas telefónicas realizadas desde los centros de reclusión. Este artículo dispone que, cuando se generen comunicaciones provenientes de dispositivos de telecomunicaciones ubicados en centros penitenciarios y carcelarios, los operadores de redes y servicios de telecomunicaciones tienen la obligación de implementar los mecanismos necesarios para informar al destinatario de la llamada sobre el origen de la comunicación, especificando tanto el lugar como el nombre del establecimiento desde el cual se efectúa la llamada.

Este control tiene como objetivo garantizar la transparencia y el monitoreo adecuado de las comunicaciones realizadas desde los centros de reclusión, especialmente para evitar que las organizaciones criminales utilicen estos medios para coordinar actividades ilícitas desde el interior de las cárceles. Además, el incumplimiento de esta disposición por parte de los operadores de telecomunicaciones dará lugar a sanciones, conforme a las multas establecidas en el artículo 65 de la Ley 1341 de 2009, bajo el régimen previsto en dicha normativa.

Con el **artículo 11** de la **Ley 1908 de 2018**, se refuerzan las estrategias para regular y supervisar el uso de las telecomunicaciones dentro de los centros penitenciarios, a fin de evitar que estos dispositivos sean utilizados para coordinar actividades delictivas por parte de organizaciones criminales. Esta disposición establece que, cuando se generen llamadas telefónicas desde dispositivos ubicados en los centros de reclusión, los operadores de redes y servicios de telecomunicaciones deben tomar las medidas necesarias para informar al destinatario de la llamada sobre el origen de la comunicación. Específicamente, se debe identificar el lugar y el nombre del establecimiento desde el cual se realiza la llamada. Este control tiene como objetivo permitir una supervisión adecuada y garantizar que las comunicaciones no sean utilizadas para fines ilícitos. En caso de que los operadores no cumplan con esta obligación, se establecerán sanciones, que incluyen la imposición de multas de acuerdo con lo previsto en el **artículo 65 de la Ley 1341 de 2009**. De esta manera, la Ley 1908 de 2018 proporciona a las autoridades un mecanismo adicional para controlar y supervisar las comunicaciones dentro de las cárceles, contribuyendo de manera efectiva en la lucha contra las organizaciones criminales.

Por su parte, la **Ley 1978 de 2019,** conocida como la "Ley de Modernización del Sector de las Tecnologías de la Información y las Comunicaciones (TIC)", introduce importantes reformas en el ámbito de las telecomunicaciones. Esta ley no solo modifica el **Registro Único de TIC,** sino que también amplía la cobertura de este registro al incluir a los proveedores de redes y servicios de telecomunicaciones, entre otros actores clave en el sector. La ley establece nuevas disposiciones para la asignación del espectro, asegurando un uso más eficiente y organizado de los recursos tecnológicos en el país. Además, introduce un marco normativo que regula las actividades de estos proveedores, con el objetivo de fomentar la competitividad en el sector, asegurar un servicio de calidad para los usuarios y promover una mayor cobertura y accesibilidad en todo el territorio nacional. La creación de un regulador único para el sector TIC refuerza la supervisión y control de las políticas públicas en este campo, permitiendo una gestión más eficiente de los recursos y una mejor coordinación entre los diferentes actores del sector.

6. ANÁLISIS DE IMPACTO FISCAL

Dando cumplimiento al artículo 7° de la Ley 819 de 2003 [1] *"Análisis del impacto fiscal de las normas"*. Debemos señalar que, los gastos que se generen de la presente iniciativa legislativa se deben entender como incluidos en los presupuestos y en el Plan Operativo Anual de Inversión al cual haya lugar. Así las cosas, posterior a la promulgación del presente proyecto de ley, el Gobierno nacional deberá promover y realizar acciones tendientes a su ejercicio y cumplimiento, lo anterior con observancia de la regla fiscal y el marco fiscal de mediano plazo.

De conformidad con lo anterior, resulta importante citar un pronunciamiento de la Corte Constitucional acerca del tema, el cual quedó plasmado en la Sentencia C-490 del año 2011, en la cual señala a renglón seguido.

"El mandato de adecuación entre la justificación de los proyectos de ley y la planeación de la política económica, empero, no puede comprenderse como un requisito de trámite para la aprobación de las iniciativas legislativas, *cuyo cumplimiento recaiga exclusivamente en el Congreso. Ello en tanto (i) el Congreso carece de las instancias de evaluación técnica para determinar el impacto fiscal de cada proyecto, la determinación de las fuentes adicionales de financiación y la compatibilidad con el marco fiscal de mediano plazo; y (ii) aceptar una interpretación de esta naturaleza constituiría una carga irrazonable para el Legislador y otorgaría un poder correlativo de veto al Ejecutivo, a través del Ministerio de Hacienda, respecto de la competencia del Congreso para hacer las leyes. Un poder de este carácter, que involucra una barrera en la función constitucional de producción normativa, se muestra incompatible con el balance entre los poderes públicos y el principio democrático."* (Negrillas propias)[2].

En el mismo sentido resulta importante citar el pronunciamiento de la Corte Constitucional en la Sentencia C-502/2007, en el cual se puntualizó que el impacto fiscal de las normas, no puede convertirse en una barrera, para que las corporaciones públicas (congreso, asambleas y concejos) ejerzan su función legislativa y normativa:

"En la realidad, aceptar que las condiciones establecidas en el artículo 7° de la Ley 819 de 2003 constituyen un requisito de trámite que le incumbe cumplir única y exclusivamente al Congreso reduce desproporcionadamente la capacidad de iniciativa legislativa que reside en el Congreso de la República, con lo cual se vulnera el principio de separación de las Ramas del Poder Público, en la medida en que se lesiona seriamente la autonomía del Legislativo.

Precisamente, los obstáculos casi insuperables que se generarían para la actividad legislativa del Congreso de la República conducirán a concederle una forma de poder de veto al Ministerio de Hacienda sobre las iniciativas de ley en el Parlamento"[3].

De conformidad con lo anterior, y como lo ha resaltado la Corte Constitucional, el análisis del impacto fiscal de las iniciativas parlamentarias que se presenten no puede ser una barrera para establecer disposiciones normativas que requieran gastos fiscales. Mencionando además que si bien compete a los congresistas y a ambas cámaras del Congreso de la República la inexorable responsabilidad de estimar y tomar en cuenta el esfuerzo fiscal que el proyecto bajo estudio puede ocasionarle al erario, es claro que es el Gobierno nacional a través del Ministerio de Hacienda, el que dispone de los elementos técnicos necesarios para valorar correctamente ese impacto, y a partir de ello, llegado el caso, demostrar a los miembros de la Rama Legislativa la inviabilidad financiera del proyecto de ley que en su momento se estudie, en este caso el que nos ocupa.

Con base en lo expuesto anteriormente, pongo a disposición de la Honorable Cámara de Representantes de la República de Colombia, la discusión y aprobación del presente proyecto de ley.

7. RELACIÓN DE POSIBLES CONFLICTOS DE INTERÉS

De conformidad con lo establecido en el artículo 3° de la Ley 2003 del 19 de noviembre de 2019, que modifica el artículo 291 de la Ley 5ª de 1992 y remite al **artículo 286 de la ley**, se establece que el ponente del proyecto de ley debe presentar una descripción detallada de las posibles circunstancias o eventos que pudieran generar un conflicto de interés durante la discusión y votación del proyecto. En el caso de este proyecto de ley relacionado con la personalización obligatoria de tarjetas SIM, no se identifica un conflicto de interés para los congresistas ponentes. Esto se debe a que la iniciativa tiene como objetivo mejorar la seguridad pública, la trazabilidad de las telecomunicaciones y la lucha contra el crimen organizado, sin beneficiar directamente a ningún sector específico o generar ventajas para los ponentes. La propuesta busca crear un entorno más seguro en las telecomunicaciones y proteger los derechos de los usuarios, lo que es una medida de interés general y no está vinculado a intereses particulares que pudieran comprometer la imparcialidad de los congresistas.

Conforme a lo anterior, se considera que en los términos en que está planteado el presente proyecto de ley, salvo circunstancias específicas y particulares, no se configuran causales de conflicto de interés para los congresistas ponentes y sobre los congresistas que participen en la discusión y votación del articulado podrán presentar su impedimento si lo consideran pertinente.

---

[1] **ARTÍCULO 7°. ANÁLISIS DEL IMPACTO FISCAL DE LAS NORMAS.** En todo momento, el impacto fiscal de cualquier proyecto de ley, ordenanza o acuerdo, que ordene gasto o que otorgue beneficios tributarios, deberá hacerse explícito y deberá ser compatible con el Marco Fiscal de Mediano Plazo, Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0819_2003.html.

[2] Corte Constitucional Colombia, M. P. Luis Ernesto Vargas Silva, C-490 del año 2011, disponible en línea en, https://www.corteconstitucional.gov.co/RELATORIA/2011/C-490-11.htm e

[3] Corte Constitucional Colombiana, M. P. Manuel José Cepeda Espinosa, C-502 del año 2007, disponible en, https://www.corteconstitucional.gov.co/RELATORIA/2007/C-502-07.htm.

1. CONCLUSIONES

El proyecto de ley se presenta como una solución para enfrentar las crecientes amenazas relacionadas con el uso ilícito de las telecomunicaciones. Esta medida busca erradicar el anonimato en el uso de líneas móviles, que actualmente favorece la comisión de delitos como la extorsión, el secuestro y el fraude financiero, proporcionando a las autoridades herramientas más efectivas para la identificación y persecución de los responsables. Al implementar un sistema centralizado de registro, donde cada tarjeta SIM esté vinculada a una persona identificada, se prevé una mejora significativa en la trazabilidad de las comunicaciones, lo que dificultará el accionar de organizaciones criminales que operan desde el anonimato de las líneas móviles.

Este proyecto tiene un impacto directo en la seguridad nacional, especialmente en la lucha contra la extorsión telefónica carcelaria, un fenómeno que ha crecido en las últimas décadas. Al asegurar que las líneas móviles estén correctamente registradas, se reducirá la posibilidad de que los delincuentes, operando desde centros penitenciarios, continúen utilizando dispositivos ilegales para llevar a cabo extorsiones. De igual manera, la colaboración entre operadores de telecomunicaciones y las autoridades judiciales se fortalecerá, permitiendo un acceso más rápido a los datos necesarios para la investigación de delitos, reduciendo los tiempos de respuesta y mejorando la eficiencia del sistema judicial.

El proyecto también tiene un fuerte componente económico, ya que se espera que al eliminar la comercialización de tarjetas SIM no registradas, se reduzcan las pérdidas anuales por fraude cibernético y delitos relacionados, que superan los 500.000 millones de pesos. Además, la formalización del mercado de telecomunicaciones permitirá incrementar la recaudación fiscal, lo que contribuirá a la estabilidad y sostenibilidad del sector. La protección de datos personales se garantiza mediante la implementación de tecnologías de verificación biométrica, alineándose con las mejores prácticas internacionales en cuanto a seguridad de la información.

La legislación también se adapta a la infraestructura ya existente en Colombia, aprovechando el sistema de registro de documentos de identidad que maneja la Registraduría Nacional del Estado Civil, lo que facilita el proceso de verificación y asegura la fiabilidad del sistema. En este sentido, el proyecto no solo se inspira en ejemplos internacionales exitosos, sino que también tiene en cuenta las particularidades del país, como la informalidad en la comercialización de SIM cards y las dinámicas específicas de la criminalidad.

Este proyecto de ley no solo aborda de manera efectiva la problemática de la extorsión y otros delitos facilitados por las telecomunicaciones, sino que también promueve la seguridad pública, la transparencia fiscal, y la protección de datos personales. Al crear un sistema de registro centralizado y obligatorio, se potenciará la confianza en los servicios de telecomunicaciones, se reforzará la lucha contra el crimen organizado, y se contribuirá al desarrollo de la economía digital en Colombia.

BIBLIOGRAFÍA

- **Asuntos Legales**. (2021). La radiografía de los delitos más comunes que terminan con sentencia de prisión. Recuperado de https://www.asuntoslegales.com.co/actualidad/la-radiografia-de-los-delitos-mas-comunes-que-terminan-con-sentencia-de-prision-3213631.

- **Decreto número 741 de 1993**, por el cual se reglamenta la telefonía móvil celular.

- **Decreto número 1630 de 2011**, por medio del cual se adoptan medidas para restringir la operación de equipos terminales hurtados que son utilizados para la prestación de servicios de telecomunicaciones móviles.

- **DANE**. (2023). Boletín técnico. Encuesta de convivencia y seguridad ciudadana (ECSC). Periodo de referencia año 2021. Bogotá, D. C.: Recuperado de https://www.dane.gov.co/files/investigaciones/poblacion/convivencia/2021/Bol_ECSC_2021.pdf.

- **Ley 1266 de 2008**, por la cual se dictan las disposiciones generales del habeas 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.

- **Ley 1341 de 2009**, por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- **Ley 37 de 1993**, por el cual se regula la prestación del servicio de telefonía móvil celular, la celebración de contratos de sociedad y de asociación en el ámbito de las comunicaciones y se dictan otras disposiciones.

- **Ley 1801 de 2016**, Código Nacional de Seguridad y Convivencia Ciudadana.

- **Ley 1908 de 2018**, por medio de la cual se fortalecen la investigación y judicialización de organizaciones criminales, se adoptan medidas para su sujeción a la justicia y se dictan otras disposiciones.

- **Ley 1978 de 2019**, por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.

- **Paksoy, E., Shankar, N., & Redin, S.-I.** (2005). Methods, apparatus, and systems for securing SIM (subscriber identity module) personalization and other data on a first processor and secure communication of the SIM data to a second processor. Recuperado de https://patents.google.com/patent/US20060129848A1/en.

- **Policía Nacional**. (2024). Resultados operativos. Delito - Extorsión ART 244 del C. P. Recuperado de https://www.policia.gov.co/resultados-operativos.

- **Procuraduría General de la Nación**. (2024). Procuraduría raja al gobierno por extorsión carcelaria. Recuperado de https://www.procuraduria.gov.co/Pages/procuraduria-raja-al-gobierno-por-extorsion-carcelaria.aspx.

- **Rankl, W., Müller, B., Stöhr, V., Vedder, K., Otte, G., Richter, O., & Garbers, C.** (2007). Method for personalising a safety module of a telecommunications terminal. Recuperado de https://patents.google.com/patent/EP1860840A2/en.

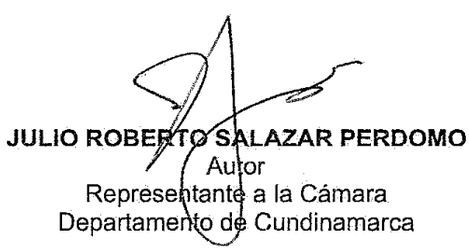
- **Sutherland, E.** (2010). El registro obligatorio de las tarjetas SIM. Red de Investigación de Ciencias Sociales. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=1566769.

- **Zidouni, N., Chitroub, S., Chebout, H., & Boukais, N.** (2018). New safety measure to protect the 3G/4G SIM cards against cloning. 1–8. https://doi.org/10.1109/MOWNET.2018.8428876.

- **Verma, S., Burakovsky, L., Shu, J. C., & Chang, L.** (2017). Mobile user identity and/or SIM-based IoT identity and application identity-based security enforcement in service provider networks. Recuperado de https://patents.google.com/patent/US20180367571A1/en.

- **Martínez Pabón, F. O., Caicedo Guerrero, J., Hernández Cuenca, R., Rendón, C., & Hurtado Guaca, J. A.** (2007). Seguridad basada en parámetros SIM para entornos de comercio electrónico móvil. Recuperado de http://www.redalyc.org/pdf/643/64327209.pdf.

Cordialmente



JULIO ROBERTO SALAZAR PERDOMO
Autor
Representante a la Cámara
Departamento de Cundinamarca

PROYECTO DE LEY NÚMERO 038 DE 2025 CÁMARA

por medio del cual se establecen disposiciones para la personalización obligatoria de las tarjetas Sim y se implementan medidas para fortalecer la seguridad en la venta y uso de servicios de telefonía móvil en Colombia.

El Congreso de Colombia

DECRETA:

Artículo 1º. *Objeto de la ley.* La presente ley tiene como finalidad establecer la obligación para todos los usuarios de telefonía móvil de personalizar las tarjetas SIM, así como la creación y regulación de la Base de Datos Nacional de Registro de Tarjetas SIM. El propósito de esta ley es asegurar la correcta identificación, autenticación y trazabilidad de las tarjetas SIM en circulación en el país, combatir el uso fraudulento de las tarjetas SIM y prevenir actividades ilícitas relacionadas con las telecomunicaciones, proteger la privacidad y seguridad de los usuarios de los servicios de telecomunicaciones y garantizar el cumplimiento de las normativas relacionadas con la protección de datos personales y privacidad.

Artículo 2º. *Definiciones.* Para los efectos de la presente ley, se entenderá por:

- **Tarjeta SIM**: Dispositivo electrónico utilizado para autenticar a los usuarios en las redes móviles. Está asociado a un número telefónico y posee un identificador único (ICCID). Puede ser de tipo físico o electrónico (E-SIM). Su función principal es habilitar el acceso a servicios de telecomunicaciones móviles y garantizar la autenticación del usuario ante el operador.

- **Base de Datos Nacional de Registro de Tarjetas SIM (BDNSC)**: Sistema centralizado y seguro administrado por las autoridades competentes, encargado de almacenar la información detallada de las tarjetas SIM activas en el país, incluyendo datos personales de los usuarios a quienes están asociadas.

- **Operadores de Telecomunicaciones**: Entidades o empresas autorizadas por el Estado para prestar servicios de telefonía móvil en Colombia. Estas entidades tienen la responsabilidad de la comercialización, activación, registro y actualización de las tarjetas SIM, asegurando que las mismas estén debidamente registradas en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNSC) y que se cumpla con los requisitos legales establecidos para su uso.

Usuario: Persona natural o jurídica titular de una tarjeta SIM, cuya información personal será registrada y almacenada en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNSC).

- **Autenticación Biométrica**: Proceso de verificación de identidad que utiliza características biométricas únicas del individuo, como huellas dactilares, reconocimiento facial, iris o voz, con el fin de autenticar al usuario de manera confiable.

- **Fraude telefónico**: Actividad ilegal que involucra el uso no autorizado de una tarjeta SIM, con el objetivo de cometer delitos como extorsión, fraude financiero, secuestro, robo de identidad o cualquier otro tipo de actividad ilícita.

- **Interoperabilidad**: Capacidad de los sistemas de telecomunicaciones, la Base de Datos Nacional de Registro de Tarjetas SIM (BDNSC) y las autoridades competentes para intercambiar, verificar y acceder a la información registrada en tiempo real, de manera eficiente, para permitir la supervisión, control y ejecución de medidas de seguridad y judiciales en el marco de la ley.

- **Protección de datos personales**: Conjunto de medidas jurídicas, técnicas y organizativas que tienen como fin garantizar la privacidad, integridad y seguridad de la información personal registrada en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNSC).

- **Suplantación de identidad**: Acción delictiva que consiste en la falsificación o manipulación de la identidad de una persona, con el fin de acceder de manera fraudulenta a servicios o recursos. En el contexto de esta ley, la suplantación de identidad se refiere al uso de tarjetas SIM registradas a nombre de un individuo distinto, con fines delictivos como el fraude, extorsión, o actividades ilícitas que afectan la seguridad pública.

- **Número IMEI**: Identificador único de cada dispositivo móvil, que permite su registro y seguimiento dentro de las redes de telecomunicaciones. Este número es utilizado para verificar la legalidad del dispositivo al momento de su activación en la red y se almacena en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNSC) para asegurar su trazabilidad y evitar el uso de equipos ilícitos.

Artículo 3º. ***Obligatoriedad de la identificación del titular de la tarjeta SIM.*** Todo operador de servicios de telefonía móvil deberá registrar obligatoriamente, en una plataforma digital segura, la identidad del usuario final al momento de la adquisición de una tarjeta SIM. Este registro deberá incluir, como mínimo, el nombre completo, el tipo y número de identificación del titular (Cédula de Ciudadanía, Cédula de Extranjería, Pasaporte, o Tarjeta de Identidad), así como cualquier otro dato adicional que permita verificar la identidad del usuario según lo establecido en la normativa vigente.

Parágrafo 1º. Queda expresamente prohibida la venta de tarjetas SIM que no hayan sido debidamente personalizadas con los datos completos y correctos del adquirente, conforme a los requisitos establecidos por esta ley. Los operadores serán responsables de asegurar que todas las tarjetas SIM activadas y en circulación estén correctamente registradas, y podrán enfrentar sanciones en caso de incumplimiento de estas disposiciones.

Parágrafo 2º. Los operadores deberán garantizar que el proceso de personalización e identificación sea transparente y accesible, y que los usuarios sean informados sobre el uso adecuado de sus datos personales, garantizando así la protección de la privacidad y el cumplimiento de las normativas nacionales e internacionales sobre datos personales.

Artículo 4°. ***Creación de la base de datos nacional de registro de tarjetas SIM.*** Créase la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS), que estará bajo la administración conjunta de la Comisión de Regulación de Comunicaciones (CRC) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic). Esta base de datos centralizada almacenará la información de las tarjetas SIM activas en el país, incluyendo los datos personales de los usuarios a quienes están asignadas, como nombre, identificación, dirección, así como la información de la tarjeta SIM, incluyendo su ICCID, IMEI, tipo de tarjeta (física o electrónica), y el estatus de la misma. Además, se almacenará el historial de activación de cada tarjeta, detallando fechas, ubicaciones y modificaciones relevantes.

Parágrafo 1º. La BDNTS deberá ser actualizada de manera continua y los operadores de telecomunicaciones tendrán la responsabilidad de integrar sus sistemas de gestión de datos con la base, garantizando que toda tarjeta SIM activada en el país esté registrada en la base de datos antes de ser utilizada. Los operadores deberán notificar de inmediato cualquier modificación en el estado de las tarjetas SIM, como la desactivación o pérdida, y colaborar con las autoridades en caso de investigaciones de actividades delictivas.

Parágrafo 2º. La seguridad de la información almacenada en la BDNTS será supervisada de acuerdo con los estándares nacionales e internacionales de protección de datos. Se implementarán medidas de encriptación y protocolos de acceso controlado para evitar el acceso no autorizado a los datos personales. Además, se establecerán mecanismos para garantizar la transparencia en el manejo de la base, con auditorías periódicas y la participación de organismos de control independientes.

Artículo 5º. ***Estructura y Contenidos de la Base de Datos Nacional de Registro de Tarjetas*** **SIM.** La Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS) será un sistema centralizado y seguro que almacenará la siguiente información esencial para garantizar la trazabilidad, la seguridad y el control de las tarjetas SIM en circulación:

1. **Datos de la tarjeta SIM:**

- ICCID (Identificador único de la tarjeta SIM).
- Número de teléfono asociado.
- Estado de la tarjeta SIM (activada, bloqueada, cancelada, etc.).
- Fecha de activación y desactivación.

2. **Datos del usuario:**

- Nombre completo.
- Tipo y número de identificación (Cédula de Ciudadanía, Cédula de Extranjería, Pasaporte o Tarjeta de Identidad)
- Dirección de residencia.
- Correo electrónico.
- Otros datos relevantes según la normativa vigente.

3. **Historial de la tarjeta SIM:**

- Registro de cambios de estado (activaciones, bloqueos, transferencias de titularidad).
- Información de operadores de telecomunicaciones que gestionaron la tarjeta SIM.

Artículo 6º. ***Actualización de la información.*** Los usuarios deberán actualizar su información personal en caso de cualquier cambio relevante, incluyendo, pero no limitado a, modificaciones en su dirección de residencia, datos de contacto o tipo de identificación. Los operadores de telecomunicaciones estarán obligados a realizar campañas periódicas de actualización de datos, asegurando que las líneas activas estén siempre asociadas a usuarios plenamente identificados. Estas actualizaciones deben garantizar la precisión de la información registrada en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS) y cumplir con los plazos establecidos para la verificación y actualización de los datos.

Parágrafo 1º. Los operadores deberán implementar mecanismos eficientes de notificación para que los usuarios sean informados sobre la necesidad de actualizar sus datos. En el caso de que el usuario no realice la actualización dentro del tiempo estipulado, el operador podrá suspender temporalmente el servicio hasta que la información sea actualizada y validada. Las autoridades competentes podrán intervenir en casos donde se detecten inconsistencias o irregularidades en la actualización de los datos, con el fin de garantizar la trazabilidad y seguridad de las comunicaciones móviles

Artículo 7º. ***Acceso a la base de datos nacional de registro de tarjetas*** **SIM.** El acceso a la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS) estará restringido exclusivamente a las autoridades competentes, incluidas las autoridades judiciales y la fuerza pública únicamente en el marco de investigaciones judiciales. Dicho acceso se otorgará bajo los principios de necesidad, proporcionalidad y respeto a los derechos fundamentales de los ciudadanos, asegurando que la utilización de la información sea estrictamente limitada al cumplimiento de fines legales específicos. La consulta de los datos almacenados en la BDNTS deberá adherirse de manera rigurosa a las disposiciones de la Ley 1581 de 2012 sobre protección de datos personales, garantizando la confidencialidad y la integridad de la información.

Artículo 8º. ***Responsabilidad de los operadores de telecomunicaciones.*** Los operadores de telecomunicaciones serán responsables de garantizar que todas las tarjetas SIM activadas y en circulación estén correctamente registradas y personalizadas conforme a lo establecido en la presente ley. Asimismo, deberán colaborar con las autoridades competentes en la verificación de los datos de los usuarios y la lucha contra el uso indebido de las tarjetas SIM. Los operadores serán sujetos a sanciones por el incumplimiento de estas disposiciones.

Artículo 9º. ***Protección de la privacidad.*** Los datos personales almacenados en la Base de Datos Nacional de Registro de Tarjetas SIM estarán sujetos a la legislación vigente en materia de protección de datos personales, en especial a lo dispuesto en la Ley 1581 de 2012 y demás normas aplicables. Estos datos deberán ser tratados de manera confidencial, segura y con altos estándares de protección, garantizando la privacidad de los usuarios. Ningún dato personal podrá ser divulgado, compartido o utilizado para fines distintos a los establecidos por la ley, salvo en los casos en que se cuente con el consentimiento expreso del titular o cuando así lo dispongan las autoridades competentes en el marco de una investigación legalmente autorizada.

Parágrafo. La protección de los datos personales será supervisada por las autoridades competentes, y las medidas de seguridad adoptadas serán auditadas periódicamente para garantizar el cumplimiento de las disposiciones legales en materia de privacidad y protección de datos.

Artículo 10. ***Verificación biométrica.*** Los operadores de servicios de telefonía móvil deberán implementar mecanismos de verificación biométrica al momento de la activación de nuevas tarjetas SIM, con el fin de garantizar que el titular registrado sea efectivamente quien adquiere la tarjeta. Dichos mecanismos de verificación deberán ser aplicados de manera rigurosa y eficiente, asegurando que la identidad del usuario sea comprobada de forma fehaciente antes de la activación del servicio.

La verificación biométrica podrá incluir tecnologías como reconocimiento facial, huellas dactilares, o cualquier otra tecnología biométrica que, de acuerdo con la normativa vigente, garantice un alto nivel de seguridad y confiabilidad en el proceso de identificación del titular.

Los operadores serán responsables de asegurar que el proceso de verificación se lleve a cabo de forma adecuada, eficiente y transparente, y de que se mantenga un registro de las activaciones realizadas mediante estos mecanismos, con el fin de permitir la trazabilidad de las acciones realizadas y prevenir el uso fraudulento de las tarjetas SIM.

Artículo 11. ***Prohibición de la Venta y uso de Tarjetas Sim no Registradas en la Base de Datos Nacional de Registro de Tarjetas*** **SIM.** Se prohíbe la venta y el uso de tarjetas SIM que no estén debidamente registradas en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS). Todo punto de venta de tarjetas SIM, ya sea físico o digital, deberá verificar que la identidad del comprador esté registrada en la base de datos antes de realizar la activación o entrega del dispositivo.

Las tarjetas SIM solo podrán ser comercializadas una vez se haya validado correctamente la identidad del usuario mediante los mecanismos establecidos por la ley, incluyendo la verificación de datos personales y la autenticación biométrica, cuando corresponda. La venta o uso de tarjetas SIM sin el cumplimiento de este registro será considerado una infracción grave.

Los puntos de venta que incurran en la venta de tarjetas SIM no registradas o que permitan la activación de tarjetas de forma anónima serán sancionados de acuerdo con lo dispuesto en la presente ley, con medidas que podrán incluir multas, la suspensión de la licencia de operación, y otras

sanciones conforme a la normativa aplicable. La implementación y cumplimiento de estas medidas será supervisada por la autoridad competente, con el fin de asegurar la correcta regulación del mercado y la protección de los usuarios.

Artículo 12. ***Sanciones.*** Los operadores de telecomunicaciones que infrinjan las disposiciones establecidas en la presente ley estarán sujetos a sanciones económicas, las cuales serán impuestas por la Superintendencia de Industria y Comercio (SIC). Estas sanciones podrán incluir multas de hasta quinientos (500) salarios mínimos legales mensuales vigentes, dependiendo de la gravedad de la infracción y de la reincidencia en la misma.

Asimismo, los puntos de venta que no cumplan con las obligaciones de identificación y registro completo de los usuarios de tarjetas SIM en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS) serán responsables solidarios de las infracciones cometidas. La sanción podrá incluir multas adicionales, suspensión temporal o definitiva de su licencia de operación, y otras medidas correctivas que aseguren el cumplimiento de la ley.

La imposición de las sanciones se realizará con base en los principios de proporcionalidad y necesidad, garantizando un debido proceso y la oportunidad para que los infractores presenten su defensa. La Superintendencia de Industria y Comercio ejercerá la supervisión y control de estos procedimientos, contribuyendo a la implementación efectiva de la ley.

Artículo 13. ***Vigilancia y control.*** La Comisión de Regulación de Comunicaciones (CRC), en conjunto con la Superintendencia de Industria y Comercio (SIC), será la encargada de vigilar y asegurar el cumplimiento de las disposiciones establecidas en la presente ley. Ambas entidades trabajarán de manera coordinada para garantizar que los operadores de telecomunicaciones y los puntos de venta cumplan con las obligaciones relacionadas con la personalización de las tarjetas SIM, el registro adecuado de los usuarios en la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS) y las demás medidas establecidas en este marco normativo.

La CRC y la SIC tendrán la autoridad para realizar inspecciones, auditorías y verificaciones a los operadores y puntos de venta, con el fin de verificar el cumplimiento de la ley. Asimismo, estas entidades podrán aplicar las sanciones correspondientes en caso de incumplimiento, asegurando que las medidas correctivas sean proporcionales a la gravedad de la infracción y favoreciendo el cumplimiento de los objetivos de seguridad, trazabilidad y protección de la privacidad de los usuarios.

Artículo 14. ***Reglamentación.*** El Gobierno nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic), en coordinación con la Comisión de Regulación de Comunicaciones (CRC) y la Superintendencia de Industria y Comercio (SIC), tendrá un plazo de seis (6) meses contados a partir de la promulgación de la presente ley, para expedir la reglamentación correspondiente. Esta reglamentación deberá incluir los procedimientos detallados y los mecanismos necesarios para la implementación de las disposiciones establecidas, así como los estándares técnicos, de seguridad y de protección de datos personales.

La reglamentación también deberá contemplar las medidas para garantizar la interoperabilidad entre los sistemas de los operadores de telecomunicaciones y la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS), así como los protocolos para la verificación biométrica, la actualización de datos, la vigilancia, el control y la aplicación de sanciones.

Artículo 15. ***Entrada en vigencia.*** La presente ley regirá a partir de su promulgación y derogará todas las disposiciones que le sean contrarias.

Cordialmente

JULIO ROBERTO SALAZAR PERDOMO
Autor
Representante a la Cámara
Departamento de Cundinamarca