# H. Congreso del Estado de Nuevo León

# LXXVII Legislatura

**PROMOVENTE:** C. DIP. ANA MELISA PEÑA VILLAGÓMEZ, INTEGRANTE DEL GRUPO LEGISLATIVO DE MOVIMIENTO CIUDADANO DE LA LXXVII LEGISLATURA

**ASUNTO RELACIONADO:** INICIATIVA DE REFORMA A LA FRACCIÓN III DEL ARTÍCULO 145 DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN

**INICIADO EN SESIÓN**: 20 DE AGOSTO DEL 2025

**SE TURNÓ A LA (S) COMISIÓN (ES):** LEGISLACIÓN

**Mtro. Joel Treviño Chavira**

**Oficial Mayor**

19-3

H. CONGRESO
DEL ESTADO DE
NUEVO LEÓN
LXXVII LEGISLATURA

BancadaNaranja

**H. CONGRESO DEL ESTADO DE NUEVO LEÓN**
**P R E S E N T E.-**

La suscrita **DIP. ANA MELISA PEÑA VILLAGÓMEZ** integrante del Grupo Legislativo de Movimiento Ciudadano de la Septuagésima Séptima Legislatura al Honorable Congreso del Estado de Nuevo León, en ejercicio de las atribuciones establecidas en la Constitución Política del Estado Libre y Soberano de Nuevo León, en sus artículos 87 y 88, así como los diversos 102, 103 y 104 del Reglamento para el Gobierno Interior del Congreso del Estado, acudo ante esta Soberanía a proponer, **Iniciativa que reforma la fracción III del artículo 145 de la Ley Federal de Telecomunicación y Radiodifusión** en materia de protección de datos, bajo la siguiente:

H. CONGRESO DEL ESTADO
OFICIALIA MAYOR
RECIBIDO
22 JUL 2025
DEPARTAMENTO
OFICIALIA DE PA
MONTERREY, N.L.
12:29 hrs

## EXPOSICIÓN DE MOTIVOS

Actualmente vivimos en una era en la que la conectividad digital se ha convertido en un componente esencial de la vida cotidiana. En tan solo unas décadas, la evolución de la tecnología electrónica ha transformado profundamente la manera en que las personas se comunican, acceden a la información, trabajan, estudian, participan en la vida pública o incluso acceden a servicios de salud, financieros y gubernamentales. En este contexto, el acceso a internet ha dejado de ser un lujo para convertirse en un instrumento indispensable para la inclusión social, el desarrollo económico y el ejercicio pleno de los derechos ciudadanos.

En línea con este avance, muchos gobiernos e instituciones han impulsado la habilitación de redes de acceso público a internet, como las que se encuentran en plazas, parques, sistemas de transporte, bibliotecas, hospitales y edificios oficiales. Estas redes tienen como objetivo democratizar el acceso a la conectividad, cerrar brechas digitales y permitir que cualquier persona, sin importar su condición

económica, tenga la posibilidad de conectarse, informarse y participar activamente en la sociedad digital. Son, en esencia, una herramienta de justicia digital.

No obstante, esta misma accesibilidad ha abierto una puerta a nuevas amenazas. Una parte importante de la población desconoce que, al conectarse a redes públicas de internet, sus datos personales, credenciales de acceso, historiales de navegación, ubicaciones, o incluso información bancaria pueden ser interceptados por terceros. En muchos casos, estas redes carecen de las mínimas medidas de protección, lo que las convierte en un entorno especialmente vulnerable a prácticas como el robo de identidad, el fraude digital, el espionaje informático, o la venta y uso indebido de información personal sin el consentimiento del titular.

Este tipo de vulnerabilidad no solo pone en riesgo la privacidad individual, sino que puede generar consecuencias más amplias: desde la manipulación de perfiles digitales y el acceso no autorizado a redes sociales o cuentas bancarias, hasta daños patrimoniales, hostigamiento digital, y afectaciones al ejercicio de otros derechos fundamentales como la libertad de expresión o la seguridad jurídica.

Frente a esta problemática, es necesario repensar la forma en que se concibe el acceso público a internet. No basta con garantizar conectividad; es imprescindible garantizar la conectividad segura, basada en principios de privacidad, consentimiento, integridad de la información y protección de datos personales. En ese sentido, existen soluciones técnicas ampliamente reconocidas y adoptadas en entornos más regulados, que pueden y deben trasladarse a las redes públicas abiertas para minimizar estos riesgos.

Una de las principales herramientas en este esfuerzo es el cifrado de datos, concepto que podemos entender por cifrado como un proceso mediante el cual la información que se transmite a través de una red es transformada en un código

ilegible para cualquier persona no autorizada. Esto significa que, aun si un tercero logra interceptar los datos, no podrá comprender su contenido sin contar con la clave adecuada. Este mecanismo es fundamental para proteger correos electrónicos, mensajes, contraseñas, formularios o transacciones bancarias, y es una práctica estándar en el ámbito de la ciberseguridad moderna.

De la mano del cifrado, otra medida esencial es la autenticación segura, que tiene como objetivo verificar la identidad del usuario o del sistema antes de permitir el acceso a determinada información o recurso. A diferencia de mecanismos simples como una sola contraseña, la autenticación segura puede incluir múltiples capas de verificación: códigos de un solo uso, certificados digitales, tokens de seguridad o incluso sistemas biométricos. Esto reduce considerablemente el riesgo de accesos no autorizados o suplantación de identidad.

Ambas medidas, cifrado y autenticación robusta, deben considerarse no como una opción técnica, sino como estándares mínimos de seguridad para toda red de acceso público. Además, existen otras medidas complementarias como avisos visibles de riesgo, que informen a los usuarios de forma clara, previa y accesible sobre los posibles peligros al conectarse a una red pública, así como controles de seguridad automatizados que monitoreen en tiempo real el tráfico de red para detectar y bloquear comportamientos anómalos, intentos de intrusión o filtraciones de datos.

De igual forma, debe establecerse como principio rector el respeto al consentimiento informado del usuario: ninguna entidad debe recabar, procesar o compartir datos personales sin que el titular haya sido claramente advertido de ello y haya otorgado su autorización de forma libre y explícita.

Estas herramientas, tomadas en conjunto, constituyen una estrategia integral de prevención de riesgos cibernéticos. Más allá del aspecto técnico, tienen un impacto directo en la experiencia del usuario: permiten que cualquier persona, sin importar su perfil socioeconómico o nivel de conocimiento tecnológico, pueda utilizar redes públicas sin temor a que su información sea vulnerada o utilizada en su contra.

Por lo que considero que es importante el fortalecimiento de la seguridad en redes públicas, ya que esto no solo responde a una obligación legal en materia de protección de datos personales, sino que representa una oportunidad para consolidar una cultura de confianza digital.

Una red segura promueve el uso responsable de la tecnología, protege la dignidad de las personas, facilita la inclusión digital y reduce los riesgos de delitos cibernéticos. Además, impulsa una imagen institucional positiva para quienes proveen el servicio, al demostrar un compromiso real con la ciudadanía.

Para mayor comprensión de la reforma que se propone se acompaña el siguiente cuadro comparativo:

| LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN | |
|---|---|
| **Texto Vigente** | **Texto Propuesto** |
| **Artículo 145.** Los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a lo siguiente:<br>I. a II. . . | **Artículo 145. . . .**<br><br>I. a II. . . |

| LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN | |
|---|---|
| **Texto Vigente** | **Texto Propuesto** |
| III. Privacidad. Deberán preservar la privacidad de los usuarios y la seguridad de la red;<br><br>IV. a VII. . . . | **III. Privacidad.** Deberán preservar la privacidad de los usuarios y la seguridad de la red, **absteniéndose de recabar, tratar o transferir datos personales sin consentimiento previo. En caso de las redes de internet de acceso público, se deberá implementar cifrado, autenticación segura, avisos de riesgo y controles de seguridad que prevengan accesos no autorizados o vulneración de datos;**<br>IV. a VII. . . . |

Por lo anteriormente expuesto es que una vez que se siga con el trámite legislativo que corresponda, solicito se somete a la consideración del Pleno para su aprobación el siguiente proyecto de:

## DECRETO

**ARTÍCULO UNICO:** Se reforma la fracción III del artículo 145 de la **Ley Federal de Telecomunicación y Radiodifusión,** para quedar como sigue:

**Artículo 145.** ...

I. a II. ...

**III. Privacidad.** Deberán preservar la privacidad de los usuarios y la seguridad de la red, **absteniéndose de recabar, tratar o transferir datos personales sin consentimiento previo. En caso de las redes de internet**

**de acceso público, se deberá implementar cifrado, autenticación segura, avisos de riesgo y controles de seguridad que prevengan accesos no autorizados o vulneración de datos;**

IV. a VII. . . .

## TRANSITORIO

**UNICO. -** El Presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación

Monterrey, N.L., a de Julio de 2025

**DIP. ANA MELISA PEÑA VILLAGOMEZ**