

H. Congreso del Estado de Nuevo León



LXXVII Legislatura

PROMOVENTE: DIP. ESTHER BERENICE MARTÍNEZ DÍAZ, INTEGRANTE DE GLMORENA DE LA LXXVII LEGISLATURA

ASUNTO RELACIONADO: MEDIANTE EL CUAL PRESENTA INICIATIVA DE REFORMA A LA NOMENCLATURA DEL CAPÍTULO PRIMERO DEL TÍTULO TERCERO Y SE ADICIONA UN CAPÍTULO SEGUNDO AL MISMO TÍTULO, BAJO LA DENOMINACIÓN VIOLACIÓN DE SISTEMAS DIGITALES PERSONALES, QUE COMPRENDEN EL ARTÍCULO 179 BIS DEL CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN

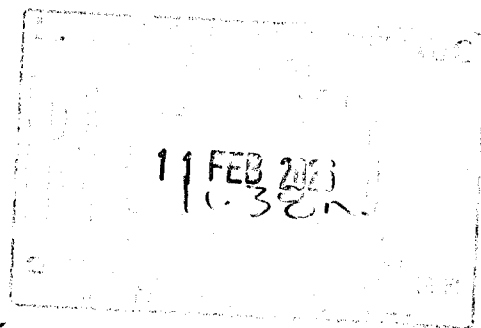
INICIADO EN SESIÓN: Lunes 16 de Febrero de 2026

SE TURNÓ A: COMISIÓN DE JUSTICIA Y SEGURIDAD PÚBLICA.

Mtro. Joel Treviño Chavira
Oficial Mayor

84

**DIPUTADA ITZEL SOLEDAD CASTILLO ALMANZA
PRESIDENTA DEL H. CONGRESO DEL
ESTADO DE NUEVO LEÓN
PRESENTE.**



La suscrita **Diputada ESTHER BERENICE MARTÍNEZ DÍAZ**, integrante del Grupo Legislativo del Partido Movimiento Regeneración Nacional perteneciente a la Septuagésima Séptima Legislatura del H. Congreso del Estado de Nuevo León, en uso de las atribuciones conferidas en los artículos 87 y 88 de la Constitución Política del Estado Libre y Soberano de Nuevo León, correlacionados con los diversos 102, 103 y 104 del Reglamento para el Gobierno Interior del Congreso del Estado de Nuevo León, someto a consideración de esta Soberanía **iniciativa con proyecto de Decreto por el que se adiciona el Código Penal para el Estado de Nuevo León, en materia de violación de sistemas digitales personales**, al tenor de la siguiente

EXPOSICIÓN DE MOTIVOS

En la última década, las tecnologías digitales se han vuelto parte integral de la vida cotidiana. Cada vez más personas en Nuevo León y en México entero trabajan, estudian, se comunican y realizan transacciones a través de dispositivos conectados a Internet. Sin embargo, este uso creciente de herramientas digitales también ha abierto la puerta a nuevos delitos informáticos, como el hackeo de cuentas personales, el robo de identidad en línea, la filtración de datos privados y otras formas de intrusión digital. Las estadísticas muestran que los ataques cibernéticos han alcanzado cifras récord: tan solo en 2024, México registró más de 324 mil millones de intentos de ciberataque, posicionándose como el país con más incidentes de este tipo en América Latina.¹

Esto refleja una realidad preocupante: los delincuentes encuentran en el mundo digital un campo fértil para vulnerar la seguridad y la privacidad de las personas,

¹ <https://www.itmastersmag.com/ciberseguridad/ciberataques-en-mexico-casos-impacto-y-respuesta/>

aprovechándose de la fragilidad de las infraestructuras de ciberseguridad actuales tanto en el ámbito público como privado.

A pesar de la gravedad de estas amenazas, existe una falta de protección jurídica específica frente a muchas conductas delictivas digitales. El Código Penal del Estado de Nuevo León solo contempla de forma general el acceso ilícito a sistemas informáticos, con penas relativamente bajas (Art. 427 del Código Penal vigente). Esta tipificación general se ha quedado rezagada frente a la sofisticación y el impacto de los delitos informáticos modernos. No se abordan explícitamente modalidades como el hackeo de dispositivos personales, la sustracción de datos privados o el phishing, ni se distinguen agravantes cuando la víctima es especialmente vulnerable (mujeres, menores, activistas) o cuando el delito causa daños significativos. En pocas palabras, nuestro marco legal local presenta vacíos legales que dejan desprotegidas a las y los ciudadanos ante la *violación de sus sistemas digitales personales*.

Esta carencia de normas específicas tiene consecuencias reales: muchas víctimas de delitos cibernéticos no encuentran actualmente una figura penal adecuada para denunciar a sus agresores, o las sanciones previstas resultan insuficientes para disuadir estas conductas. El incremento en el uso malicioso de la tecnología – incluyendo herramientas de inteligencia artificial usadas para vulnerar sistemas o suplantar identidades– ha superado la capacidad de nuestras leyes actuales. En suma, enfrentamos un escenario de alta exposición a delitos informáticos con protección jurídica limitada, lo que exige una respuesta legislativa urgente y adecuada a la realidad digital del siglo XXI.

Los números confirman la magnitud del problema. En el ámbito internacional, la ciberdelincuencia se ha convertido en un “negocio” de escala gigantesca, que genera ganancias ilícitas superiores al billón de dólares anuales a nivel global, mediante fraudes, robo de identidad y apropiación de información confidencial. Organismos internacionales advierten que más del 60% de la población mundial está conectada a Internet, aumentando la superficie de riesgo, y que el costo

económico del cibercrimen sigue creciendo exponencialmente, con estimaciones de alcanzar 10.5 billones de dólares a nivel mundial en 2025.² Esto significa que ningún

país está exento: los delitos digitales trascienden fronteras y se expanden rápidamente.

En México, las cifras son igualmente alarmantes. De acuerdo con el INEGI, un 6.6% de los usuarios de Internet de 12 años o más en el país fue víctima de algún ciberdelito en el último año (periodo 2022-2023).³ En particular, 3.8% sufrieron el hackeo de sus redes sociales personales, evidenciando lo común que se ha vuelto la intrusión en cuentas privadas. Otros incidentes frecuentes incluyen el *hacking* de *correos electrónicos*, infecciones de malware y ataques de *ransomware*. Estas estadísticas se traducen en millones de personas afectadas. Por ejemplo, en 2024 más de 18.9 millones de mexicanos vivieron situaciones de acoso o violencia digital (ciberacoso) en alguna forma. Especialmente preocupante es que las mujeres jóvenes son las más expuestas: 22.2% de las usuarias de internet mexicanas sufrieron ciberacoso en 2024, lo que incluye la difusión no consentida de información o imágenes privadas y otras agresiones en línea.⁴

En cuanto al robo de identidad y fraude digital, México enfrenta un auge sin precedentes. La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) reportó que los casos de posible robo de identidad en línea aumentaron 281% al cierre de 2023 respecto al año anterior.⁵ Según el Consejo Ciudadano de Seguridad, los reportes de robo de identidad a nivel nacional crecieron 218% de 2022 a 2023 (pasando de 505 a 1,607 casos reportados). De esos casos, el 62% se originó por hackeo de información de redes sociales de la víctima (acceso indebido a sus cuentas privadas), y otro 26% por robo de información del teléfono celular. Este dato confirma que los sistemas digitales personales son un blanco principal de la delincuencia, ya sea para suplantar personas, acceder a datos sensibles o cometer fraudes financieros.

² <https://www.jornada.com.mx/2025/11/30/politica/007n2pol>

³ https://www.inegi.org.mx/contenidos/programas/mociba/2023/doc/mociba2023_resultados.pdf

⁴ Ídem

⁵ www.condusef.gob.mx

Además, México se ha posicionado desafortunadamente entre los países más afectados por ciberdelitos. Diversos análisis sitúan a nuestro país en el “top 10” mundial de las naciones con mayor tasa de cibercriminalidad, siendo la única de

Latinoamérica en ese grupo.⁶ Estudios del Banco Mundial y la ONU indican que en Latinoamérica los ciberincidentes delictivos crecieron aproximadamente 25% anual en la última década, con México entre los cinco países más golpeados de la región. En materia de ataques cibernéticos masivos, durante el primer semestre de 2025 se detectaron más de 35 mil millones de intentos de ciberataque en México⁷, lo que equivale a millones de intentos diarios de vulnerar sistemas públicos y privados. Estos números demuestran que la seguridad digital en México está en crisis, con una brecha creciente entre el avance de las amenazas y la capacidad de la ley para prevenir y sancionar efectivamente estas conductas.

Otra poderosa razón para legislar es la protección de derechos fundamentales. La Constitución Política de los Estados Unidos Mexicanos garantiza el *derecho a la privacidad y a la protección de datos personales* en su artículo 16. Asimismo, establece la inviolabilidad de las comunicaciones privadas. Estos preceptos constitucionales reconocen que la intimidad de las personas abarca sus datos digitales, comunicaciones electrónicas y contenidos almacenados en la nube o dispositivos. Cada vez que un agresor accede sin autorización a la información privada de alguien, está vulnerando no solo un archivo electrónico sino un derecho humano básico. Del mismo modo, instrumentos internacionales suscritos por México –como la Declaración Universal de los Derechos Humanos (art. 12) y la Convención Americana sobre Derechos Humanos (art. 11)– consagran la protección contra injerencias arbitrarias en la vida privada y la correspondencia. Legislar contra la violación de sistemas digitales personales es entonces cumplir con estas obligaciones nacionales e internacionales, actualizando la tutela jurídica de la privacidad al entorno tecnológico actual.

⁶ www.buzos.com.mx

⁷ Ídem nota 2.

Con esta iniciativa de reforma al Código Penal de Nuevo León, se persiguen seis objetivos principales, encaminados a prevenir, sancionar y disminuir la violación de sistemas digitales personales:

1. Tipificar claramente la intrusión digital no autorizada: Crear un delito específico que sancione a quien *acceda, sin consentimiento y por cualquier medio, a un sistema digital o dispositivo ajeno* (computadora, teléfono, cuenta en la nube, correo electrónico, redes sociales, etc.). Esto abarca tanto el acceso inicial como el mantenerse dentro del sistema contra la voluntad del legítimo usuario, equiparándolo legalmente a invadir un espacio privado. La claridad en la tipificación dará certeza jurídica a víctimas y autoridades.
3. Incorporar agravantes según la conducta y el daño: Prever penas más severas cuando la intrusión conlleve actos adicionales particularmente dañinos. Por ejemplo, si el delincuente *copia, difunde o utiliza la información obtenida* para perjudicar al titular (robo de datos personales, publicaciones sin consentimiento, fraude con información robada), o si *se comete con ciertos medios peligrosos* (uso de malware, violación de medidas de seguridad sofisticadas). Asimismo, establecer agravantes especiales cuando la víctima sea menor de edad, persona con discapacidad, adulto mayor, o cuando la intrusión se realice con el fin de violentar a una mujer por razones de género o de silenciar a un periodista/activista. Esto asegurará que las sanciones sean proporcionales al impacto real del delito.
4. Aumentar los rangos de pena y multas: Elevar significativamente las penas carcelarias y económicas respecto a las actualmente previstas para el simple “acceso ilícito” genérico. La reforma buscará que la violación de sistemas digitales personales deje de considerarse un delito menor. Penalidades más altas (por ejemplo, de 3 a 8 años de prisión en casos básicos, y superiores en casos agravados) servirán como efecto disuasorio frente a quienes hoy ven en estas conductas “de cuello blanco” un bajo riesgo. Con penas robustas, también se evita que delitos graves queden impunes mediante salidas alternas.
5. Cerrar lagunas legales y evitar la impunidad técnica: Detallar en la ley las diversas formas en que se puede cometer el delito (mediante *engaños*

6. *phishing*, aprovechando vulnerabilidades técnicas, sustrayendo credenciales, etc.) para que ninguna variante quede fuera de castigo. Incluir definiciones de términos técnicos clave (por ejemplo “sistema informático”, “datos personales”, “dispositivo de almacenamiento”) para facilitar la aplicación judicial. La meta es que los operadores de justicia cuenten con herramientas normativas explícitas para procesar cualquier incidente de hackeo o acceso indebido, sin depender de analogías forzadas.
7. Protección de grupos vulnerables y víctimas: La reforma tiene un enfoque de derechos humanos y perspectiva de género. Sus objetivos incluyen proteger
8. la privacidad e integridad de las mujeres en entornos digitales, atendiendo compromisos de combatir la violencia digital de género. Igualmente, salvaguardar a niños, niñas y adolescentes en sus espacios virtuales (redes, juegos en línea, aulas virtuales), a activistas y periodistas cuyo trabajo se ha trasladado en buena medida a plataformas digitales, y en general a cualquier ciudadano cuya vida privada ahora está entrelazada con dispositivos inteligentes. El objetivo es brindarles un amparo legal efectivo para que puedan desarrollar sus actividades digitales sin miedo constante a ser vulnerados.
9. Fomentar la cultura de la ciberseguridad y la denuncia: Aunque es una reforma penal, lleva implícito el objetivo pedagógico de sensibilizar sobre la importancia de la seguridad digital. Al elevar el perfil de estas conductas a delitos explícitos, se envía un mensaje a la sociedad sobre la seriedad de proteger contraseñas, datos personales y respetar la privacidad ajena en línea. Así, se espera incentivar a las víctimas a denunciar (sabiendo que la ley ahora sí las ampara) y a potenciales infractores a abstenerse por el riesgo real de sanción. En conjunto con campañas de educación digital, la reforma busca propiciar un entorno online más seguro y responsable para todos.

Se considera adecuado y coherente ubicar la nueva figura de “*Violación de Sistemas Digitales Personales*” dentro del Título Tercero del Código Penal de Nuevo León, como capítulo relativo a delitos contra la inviolabilidad de la privacidad. Con base en las siguientes razones:

A) Protección del Bien Jurídico Primordial: El núcleo de este delito es *invadir la esfera privada digital de una persona* – equivalente funcional de allanar su domicilio virtual o hurgar en su correspondencia electrónica. Ubicarlo en el título de privacidad reafirma que el bien jurídico tutelado es la intimidad personal y la inviolabilidad del entorno privado, aunque el medio sea digital. Esto lo alinea con el tratamiento ya dado a la violación de correspondencia, reflejando que tanto abrir una carta ajena como hackear una cuenta personal constituyen violaciones a la privacidad del individuo. Desde una perspectiva de derechos, esto refuerza el mensaje de que la *dignidad, intimidad y vida privada digital* gozan de igual protección que los espacios físicos tradicionales.

B) Sistemática interna y especialidad: La creación de un capítulo propio en Título III permitirá especializar la descripción típica a los supuestos personales. De este modo, se evita tocar o desnaturalizar el Título XXII (que seguiría regulando accesos ilícitos a sistemas *no personales*, ataques a bases de datos empresariales, etc.), y a la par se dota de una *herramienta penal más gravosa* cuando la víctima sea un ciudadano común cuya información privada fue vulnerada. En otras palabras, habría una norma especial (179 Bis) para el hacking contra personas, coexistiendo con la norma general (427) para el hacking contra sistemas informáticos en general.

Por lo anteriormente expuesto y fundado, someto a la consideración de esta H. Soberanía el siguiente proyecto de

DECRETO

ÚNICO. Se reforma la nomenclatura del Capítulo Primero del Título Tercero y se adiciona un Capítulo Segundo al mismo Título, bajo la denominación VIOLACIÓN DE SISTEMAS DIGITALES PERSONALES, que comprende el artículo 179 Bis, del Código Penal para el Estado de Nuevo León, en los siguientes términos:

CAPÍTULO PRIMERO

...

ARTÍCULO 178. ...

ARTÍCULO 179. ...

CAPÍTULO SEGUNDO

VIOLACIÓN DE SISTEMAS DIGITALES PERSONALES

ARTÍCULO 179 BIS. - Se impondrá una sanción de prisión de dos a cuatro años y de quinientos a mil días multa, a quien, mediante el uso de cualquier medio digital o tecnológico:

I. Acceda sin autorización a cuentas de correo electrónico, redes sociales, plataformas digitales, servicios de mensajería electrónica o cualquier otro sistema de comunicación o almacenamiento de datos personales, con la intención de obtener, modificar, utilizar, divulgar o eliminar información contenida en dichas cuentas, dañar la privacidad o los intereses de su titular;

II. Inserte, altere o elimine información en cuentas digitales o sistemas mencionados en la fracción que antecede, sin el consentimiento de su titular, generando perjuicio o riesgo a la integridad, la privacidad o derechos de su titular; y

III. Utilice indebidamente información obtenida sin autorización, con el propósito de causar daño, lucro indebido o afectar la reputación, seguridad o privacidad del titular de la cuenta.

Cuando la conducta sea cometida por un servidor público, o quien tenga acceso privilegiado a sistemas o información en virtud de su empleo, cargo o

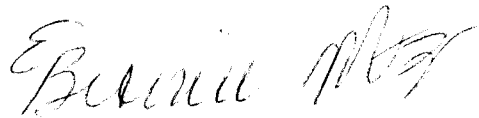
función, la pena se aumentará en una mitad, sin perjuicio de las sanciones administrativas o disciplinarias aplicables.

TRANSITORIOS

ÚNICO. El presente Decreto entrará en vigor al día siguiente al de su publicación en el Periódico Oficial.

Monterrey, Nuevo León a los 11 del mes de febrero de 2026

Atentamente,



Dip. Esther Berenice Martínez Díaz

