La ampliación de la vigilancia estatal: GNI alerta sobre las leyes de telecomunicaciones y seguridad en México

En julio del 2025, el gobierno mexicano aprobó, de forma acelerada, un paquete de leyes que incrementan significativamente los poderes de vigilancia por parte del Estado e imponen al sector privado la obligación de retener y divulgar información sensible de la ciudadanía. Estas leyes incluyen reformas a la Ley de Telecomunicaciones, la Ley General de Población, la Ley de Inteligencia, la Ley de Personas Desaparecidas, la Ley de la Guardia Nacional y la Ley Orgánica de la Administración Pública Federal.

En conjunto, estas reformas crean una infraestructura de vigilancia masiva interconectada que exige la identificación biométrica, establece un registro centralizado para una amplia gama de datos sensibles, permite el acceso en tiempo real a bases de datos públicas y privadas, obliga a las empresas a obedecer a estos cambios, sin las salvaguardas adecuadas, y permite la vigilancia militar sin una supervisión autónoma y suficiente. Esto plantea preguntas incómodas sobre el compromiso y la capacidad de México para cumplir con sus obligaciones en virtud del derecho internacional de los derechos humanos y las garantías constitucionales.

La Global Network Initiative está profundamente preocupada por este paquete de reformas legislativas y exhorta al gobierno, así como al Congreso y al sector judicial, a reconsiderar los enfoques dados por estas leyes dando prioridad a la protección de los derechos humanos.

Cambios clave en las reformas de ley:

- Las empresas de telecomunicaciones están obligadas a retener, por dos años, los metadatos de usuarios de telefonía móvil y proporcionar los datos de geolocalización a las autoridades competentes.
- Todas las líneas telefónicas deben estar conectadas a una identificación biométrica o serán bloqueadas en Mayo de 2026.
- Creación de un nuevo registro de usuarios de telefonía móvil que obliga a las empresas de telecomunicaciones a conservar y almacenar datos de comunicaciones pormenorizados, lo que se asemeja al PANAUT, que fue anulado anteriormente por la Suprema Corte de Justicia de México.
- Todas las personas deben obtener una CURP biométrica, que incluirá escaneo de iris y huellas dactilares, para acceder a servicios públicos y privados.
- Creación de la Plataforma Única de Identidad que centralizará todos los datos biométricos y facilitará el acceso, en tiempo real, a las fuerzas del orden.

- La ley de inteligencia da acceso a las autoridades a cualquier base de datos pública y privada, incluyendo empresas de todos los sectores, en aras de mantener "la seguridad pública", término que aún no ha sido definido claramente.
- Las Fuerzas Armadas y la Guardia Nacional ahora tienen el poder de conducir actividades de inteligencia o vigilancia sin ninguna restricción judicial.

La reestructuración normativa socava la independencia y la supervisión

El paquete de leyes introduce colectivamente una importante reforma institucional del marco regulatorio de las telecomunicaciones en México. Las reformas sustituyen al Instituto Federal de Telecomunicaciones (un organismo autónomo conocido por su experiencia técnica, su toma de decisiones pluralista y su relativa independencia del control por parte del Ejecutivo).

En su lugar, la ley establece dos entidades nuevas: La Agencia de Transformación Digital y Telecomunicaciones, una agencia ejecutiva a nivel ministerial encargada de formular la política digital y supervisar la infraestructura, y la Comisión Reguladora de Telecomunicaciones (CRT), una figura técnica autónoma, pero subordinada, que operará bajo el ATDT.

Mientras la CRT aparentemente es responsable de la asignación del espectro, la concesión de licencias y los derechos de los usuarios, no será institucionalmente independiente. Por lo que el poder ejecutivo ahora controlará tanto la dirección de las políticas como la aplicación de la normativa, lo que crea un conflicto de intereses estructural, dado que el Estado mexicano también actúa como proveedor de servicios de telecomunicaciones en algunos contextos. En un contexto con amplio poder para una vigilancia exhaustiva, una retención de datos onerosa y la obligación por parte de empresas privadas de acatar las reformas, la pérdida de un regulador independiente es especialmente alarmante ya que elimina un mecanismo institucional crucial que, de otro modo, podría haber cuestionado los abusos, mediado en las disputas o defendido el debido proceso y la protección de los usuarios.

Obligaciones generales para las empresas sin salvaguardas

Las leyes transfieren las responsabilidades de vigilancia a las empresas privadas, incluidos los proveedores de telecomunicaciones, bancos, proveedores de servicios sanitarios y las plataformas digitales. Estas empresas están obligadas a recopilar, conservar y entregar datos sensibles de las personas usuarias, interconectar sus bases de datos con los sistemas gubernamentales y aceptar CURP biométrica y la Llave MX para su autenticación.

Estas obligaciones están pobremente definidas, dejando a las empresas expuestas a una incertidumbre legal y potenciales sanciones, incluyendo responsabilidades penales. Estas obligaciones también hacen más difícil para las compañías cumplir de forma adecuada con sus responsabilidades y compromisos en materia de derechos humanos, lo que crea tensión entre la legislación nacional y los estándares internacionales en materia de empresas y derechos humanos.

Militarización de la vigilancia

La ley permite que autoridades militares tengan acceso a sistemas y bases de datos con información de la ciudadanía con fines de inteligencia. Con la Guardia Nacional ahora bajo control militar y con las facultades para realizar actividades de vigilancia en tiempo real sin ningún control judicial, México está en riesgo de normalizar la vigilancia militar en contextos no militarizados.

En contextos donde se entrelazan la aplicación de la ley, la recopilación de información y la vigilancia durante protestas, aumenta la confusión y el riesgo de que la vigilancia se utilice para reprimir la disidencia o intimidar a la sociedad civil. Sin límites legales claros, obligaciones en términos de transparencia o garantías judiciales, la presencia de actores militares en los ecosistemas de vigilancia digital socava el estado de derecho y crea un desequilibrio de poder que puede ser difícil de revertir. Estos riesgos son especialmente graves en un país donde los periodistas, las personas defensoras de derechos humanos y las comunidades indígenas se han enfrentado históricamente a persecuciones e intimidaciones.

Vinculación biométrica obligatoria y un sistema de vigilancia centralizado

El paquete legislativo recrea una disposición que refleja fielmente el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT), el cual fue declarado inconstitucional por la Suprema Corte de Justicia de la Nación en 2022. El PANAUT ordenaba que todas las personas usuarias de telefonía móvil vincularan su tarjeta SIM a sus datos biométricos, incluyendo fotografía y huellas dactilares, obligando a las empresas de telecomunicaciones a recolectar y almacenar esta información en una base de datos gubernamental totalmente centralizada. La Suprema Corte encontró que el PANAUT era una medida desproporcionada que violaba el derecho a la privacidad de todas las personas usuarias, la protección de sus datos, y el acceso a la comunicación, enfatizando que la ley no contaba con salvaguardas suficientes, tal como: una supervisión independiente, limitaciones estrictas para el propósito de la consulta y una autorización judicial para el acceso a esa información.

A pesar de esta sentencia, el reciente paquete legislativo reintroduce un registro similar que debe contener todas las líneas telefónicas posibles, junto con la obligación de identificar a

cada propietario con una identificación biométrica. Esta estructura reproduce las características fundamentales que llevaron a la Corte a anular la PANAUT: vinculación biométrica obligatoria, falta de control por parte de las personas usuarias, mecanismos de acceso poco claros e intervención desproporcionada a la privacidad y la libertad de expresión.

Además, al vincular el acceso a los servicios básicos con el registro de la CURP biométrica y exigir que el servicio telefónico esté vinculado a una identificación biométrica, la ley condiciona las actividades privadas y la participación ciudadana al cumplimiento de sistemas que pueden ser utilizados indebidamente para la vigilancia. Actualmente no existen disposiciones de exclusión voluntaria, lo que significa que el incumplimiento probablemente conduzca a una marginación económica, social y política significativa.

Centralizar vastas cantidades de información personal sensible sin las salvaguardas adecuadas también crea potencialmente la posibilidad de filtraciones de datos, robo de identidad y otros usos ilegítimos, como cuando los datos recopilados para un fin se usan para investigaciones o perfilamientos no relacionados. Con la ausencia de una supervisión independiente, mecanismos de compensación claros, y minimización de estándares para esos datos, esta infraestructura debilita tanto la confianza en instituciones públicas como en los principios de proporcionalidad.

Qué hace la ley: En resúmen

- Permite la exclusión y vigilancia basadas en la identidad. Crea registros de datos para la vida cotidiana.
- Ley General de Población: Obliga el uso de la identificación biométrica para cualquier transacción, pública y privada.
- Ley de Telecomunicaciones: Compañías de telecomunicaciones retendrán metadatos de todas las personas usuarias por más de 2 años + autoridades podrán acceder a los datos de geolocalización en tiempo real sin una orden judicial.
- Facilita la vigilancia por parte del Estado y obliga a las empresas a actuar como autoridades encargadas de hacer cumplir la ley.
- Nuevo paquete legislativo en México amenaza la privacidad y la libertad de expresión.
- Ley de la Guardia Nacional y de la Administración Pública: La Secretaría de la Defensa Nacional está autorizada para acceder a todas las bases de datos centralizadas para dirigir actividades de inteligencia sin la necesidad de una orden judicial
- Militariza la vigilancia sin supervisión y faculta a las fuerzas armadas con seguimiento de vigilancia en tiempo real.
- Posibilidad de uso indebido para normalizar la vigilancia indiscriminada.

- Ley de Personas desaparecidas: Crea la Plataforma Única de Identidad y centraliza las actividades biométricas en todos los sectores.
- Ley de Inteligencia: Permite el acceso en tiempo real a todas las bases de datos de autoridades y obliga a empresas financieras, de telecomunicaciones, de salud, inmobiliarias y otras corporaciones comerciales a compartir sus registros.
- No hay mecanismos de transparencia. Responsabilidad penal para empresas por incumplimiento.

Llamado a la acción por parte del GNI

El GNI insta al Gobierno de México a reconsiderar y revisar este paquete legislativo de acuerdo con las normas internacionales de derechos humanos. En particular, pedimos lo siguiente:

- Definiciones claras y precisas de las obligaciones de acceso y retención de datos, con una supervisión judicial independiente y adecuada, incluido el requisito de aprobación judicial (órdenes judiciales) para las solicitudes por parte del Gobierno para acceder a los datos de las personas usuarias en poder de intermediarios.
- Establecer una supervisión judicial sólida, que exija órdenes judiciales independientes para cualquier acceso a los datos de las personas usuarias.
- Proporcionar claridad y protección jurídica a las empresas que se enfrentan a solicitudes de datos por parte del Gobierno.
- Garantías sólidas para proteger los datos personales sensibles, especialmente los que se refieren a datos biométricos.
- Mecanismos significativos de transparencia y rendición de cuentas para las operaciones de inteligencia y aplicación de la ley.
- Un proceso inclusivo y multilateral para evaluar el impacto de estas leyes en los derechos humanos que garantice que el sector privado no se vea obligado a actuar como instrumento de vigilancia sin el debido proceso.
- Involucrar a la sociedad civil, la industria y los expertos en derechos humanos en una revisión participativa de estas leyes.

GNI se compromete a promover marcos legales y políticos que respeten la libertad de expresión y la privacidad, y hacemos un llamado a las autoridades mexicanas para que garanticen que la gobernanza digital promueva derechos fundamentales. Seguimos disponibles para interactuar y trabajar junto con el Gobierno mexicano para seguir colaborando en el tema.

Acerca del GNI

GNI reúne a más de 100 destacados académicos, organizaciones de la sociedad civil, empresas de tecnología de la información y la comunicación (TIC's) e inversores de todo el mundo. Durante los últimos años, GNI ha revisado, comentado y ayudado a dar forma a una serie de proyectos de ley sobre "seguridad en línea" en varias jurisdicciones. Nuestro análisis de los derechos humanos y nuestras recomendaciones para los responsables políticos se pueden encontrar en el informe Content Regulation & Human Rights Policy Brief, que utiliza los principios internacionales de derechos humanos para analizar una amplia gama de iniciativas legislativas y ofrece orientación proactiva sobre cómo abordar la seguridad en línea de una manera que proteja nuestros derechos. Estas recomendaciones se basan en dicho informe y se remite a los lectores al mismo para un análisis más detallado.