México Evalúa

Incidir hoy:
Políticas Públicas en Acción

Hacia un sistema digital confiable

al servicio de la ciudadanía

México Evalúa | 15 de octubre, 2025

- *México ocupa el lugar 59 de 67 países en el Ranking de Competitividad Digital Mundial 2024 (IMD), lo que muestra rezagos en infraestructura y talento, pero también la oportunidad de acelerar la transformación digital como motor de competitividad y desarrollo.*
- *El Congreso aprobó seis reformas y cuatro nuevas leyes que son un paso importante hacia un ecosistema digital más amplio; mientras que el Paquete Económico 2026 propone que, para mejorar la fiscalización, el SAT acceda de manera permanente y en tiempo real a toda la información que obre en sus sistemas.*
- *En el marco de la expedición de la nueva CURP Biométrica, el desafío es consolidar instituciones que protejan datos y garanticen derechos digitales a ciudadanos y empresas para avanzar hacia un modelo de confianza, innovación y competitividad sin sacrificar libertades democráticas.*

Podemos imaginar la transformación digital de un país como una gran red de nodos, elementos y actores interconectados que, de forma sincrónica, logran beneficios en productividad, recaudación fiscal, competitividad y acceso a derechos básicos. El sistema, visto de forma más sencilla, se equipara a un gran rompecabezas. El que tenemos en el país, hasta ahora, tiene algunas piezas en el tablero: plataformas tecnológicas, identidad digital, transacciones bancarias cibernéticas, sistemas de pagos alternativos, y trámites en línea, entre otras. De hecho, varias de esas piezas fueron recientemente creadas o modificadas, en un paquete de seis reformas y cuatro nuevas leyes que el Congreso de la Unión aprobó durante el periodo extraordinario, celebrado del 23 de junio al 2 de julio de 2025. Sin embargo, este reciente trabajo legislativo, aunque necesario, no basta para completar el ecosistema digital que México necesita.

Según estándares internacionales, México se encuentra en una fase temprana de desarrollo digital. El *Ranking de Competitividad Digital Mundial 2024*, del Instituto para el Desarrollo Gerencial (IMD), nos ubica en el lugar 59 de 67 países. Es una posición que revela rezagos en infraestructura, conectividad y formación de talento. Atender estos desafíos para encaminarnos hacia la transformación digital no es un lujo, sino una condición indispensable para competir globalmente y cerrar brechas sociales.

Desde México Evalúa apuntamos que la digitalización es altamente deseable y necesita avanzar aceleradamente para fines productivos y de seguridad pública, pero siempre con legitimidad democrática. Es indispensable construir una estrategia nacional que reduzca brechas y promueva la modernización progresiva de una relación de confianza verdadera entre Gobierno y sociedad. En este último punto, no obstante, hay grandes ausencias. Las más evidentes son aquellas instituciones que funcionan como salvaguardas de la información sensible y privada que se maneja en las plataformas digitales. Se trata de instancias esenciales para proteger los datos personales y fortalecer los mecanismos de transparencia y rendición de cuentas. Para impulsarlas se requiere un andamiaje que ponga en el centro los derechos digitales de ciudadanos y empresas: privacidad, neutralidad de la red, acceso universal a la información y libertad de expresión.

Sin estos elementos, la digitalización en nuestro país corre el riesgo de consolidarse como un sistema desigual. Si bien podría ser un motor de productividad en todos los ámbitos económicos, no implementarla en clave democrática mermará la construcción de confianza entre ciudadanos, empresas y autoridades. Por ahora, nada limita —en la ley o en las instituciones— que ello evolucione hacia un sistema de vigilancia y control altamente efectivo, pero autoritario.

Una consecuencia de esa ausencia de límites es que, recientemente, el 23 de septiembre de 2025, el Juez Séptimo de Distrito en Materia Administrativa de la Ciudad de México, Francisco Martínez Cruz, resolvió conceder la suspensión definitiva al amparo solicitado por la organización civil Artículo 19 frente a los diversos decretos que conformaron el paquete de leyes aprobado. En su resolución, el Juez considera que la aplicación de estas leyes causaría afectaciones graves y de difícil o casi imposible reparación a los derechos humanos vulnerados. Habrá que esperar a la sentencia y el curso legal del caso hasta la última instancia judicial. No obstante, la decisión del juez da cuenta de la relevancia del tema.

El paquete normativo ya vigente en México busca, en efecto, agilizar servicios y trámites mediante el manejo de información en tiempo real. Sin embargo, genera asimetrías que expanden el acceso gubernamental a información confidencial de ciudadanos y empresas sin garantizar mecanismos de transparencia, protección y defensa ante posibles abusos. En específico, otorga facultades amplias a autoridades civiles y militares para recabar y consultar datos ciudadanos, sin establecer suficientes controles judiciales o ministeriales.

I. BENEFICIOS DE LA DIGITALIZACIÓN Y CASOS DE REFERENCIA

La digitalización como inversión estratégica para el desarrollo compartido

En las últimas décadas, diversos gobiernos han apostado por la digitalización como una estrategia para mejorar la eficiencia, reducir la burocracia, aumentar la formalidad económica, combatir el crimen, disminuir la pobreza y fortalecer la relación entre el Estado y la ciudadanía.

La digitalización aporta tres beneficios cruciales a la economía pública y general. En primer lugar, optimiza la eficiencia y reduce costos para el Gobierno y los ciudadanos, ya que la automatización de trámites y la eliminación de procesos manuales liberan recursos que pueden ser redirigidos. Segundo, mejora la transparencia y combate la corrupción al reducir la interacción personal y crear registros digitales inmutables, lo que fomenta la confianza en las instituciones. Finalmente, una economía basada en datos, al ser más ágil, impulsa la competitividad y la innovación. Esto crea un terreno fértil para el emprendimiento, el desarrollo de nuevos servicios y la atracción de capital, transformando la administración en un verdadero motor de prosperidad.

Un estudio del Banco Mundial (pág. 50), publicado en 2023, plantea que un aumento del 10% en la penetración de la banda ancha puede impulsar el crecimiento del Producto Interno Bruto (PIB) per cápita en 3.19 puntos porcentuales en las economías en desarrollo de Latinoamérica. Asimismo, una ampliación del 50% en la adopción de soluciones digitales por parte de las administraciones tributarias podría aumentar la recaudación del impuesto al valor agregado (IVA) en un 1.7% del PIB en los países en desarrollo, según el Fondo Monetario Internacional (FMI). Hay que señalar que, entre 2000 y 2010 se sentaron las bases de la modernización fiscal en México, lo que permitió un aumento del 95% en la recaudación entre 2010 y 2016. Gracias a la digitalización, la relación entre la recaudación y el PIB pasó de 12.6% a 16.2% de 2012 a 2017, ampliando la base imponible en 150% y reduciendo la evasión del 35% al 16%. Asimismo, el Servicio de Administración Tributaria (SAT) disminuyó en 57% el costo de recaudación y elevó en 117% los ingresos por auditorías, de acuerdo con el análisis realizado por Rosengard en el 2020.

Estos datos resaltan cómo la infraestructura digital no es un gasto, sino una inversión directa en el desarrollo económico. Además, según el Banco Mundial, las plataformas digitales para la prestación de servicios públicos disminuyen significativamente la incidencia de la corrupción. Por ejemplo, la digitalización de procesos de licitación y pagos de los gobiernos de los países que la han implementado, ha demostrado reducir los sobornos en un 33% en promedio, al eliminar la interacción cara a cara y crear un rastro auditable y transparente de las transacciones.

En la experiencia de países que han implementado la identificación biométrica de la ciudadanía, tenemos ejemplos como Estonia, India y Corea del Sur, mientras que en Latinoamérica están Uruguay y Brasil. El enfoque y resultados que han tenido es diverso, así como las condiciones en que se han desarrollado los proyectos de digitalización. A continuación, exponemos los casos de Estonia, Brasil e India.

CASO ESTONIA

Con 1.37 millones de habitantes, este país es pionero en la implementación de un sistema de gobierno digital integral. Desde inicios de los años 2000, desarrolló una plataforma que permite a sus ciudadanos realizar prácticamente todos los trámites gubernamentales en línea —desde votar hasta pagar impuestos o renovar licencias— a través de una identidad digital única respaldada por sistemas de ciberseguridad avanzados. Sobresale el desarrollo de un ecosistema basado en una blockchain que asegura tanto la trazabilidad en la consulta de datos, como la privacidad de los mismos.

Este modelo ha sido exitoso en gran parte gracias a un marco legal claro, auditorías independientes, transparencia en el uso de la información, y una fuerte inversión en educación digital. La confianza de la ciudadanía ha sido clave para su sostenibilidad, ya que el gobierno estonio ha garantizado que las personas tengan control sobre sus datos y puedan ver quién los consulta, lo que fomenta un sentido de propiedad y vigilancia compartida.

Desde el inicio del proyecto se tuvo claro que lo más importante era generar confianza en la ciudadanía sobre los beneficios del uso de sus datos personales. El gobierno de este país báltico enfoca la información recabada a la prestación de servicios de salud, trámites, pago de impuestos, y para fines estadísticos. Estonia está obligada a seguir lineamientos del derecho a la privacidad y protección de datos personales establecidos por la Unión Europea, además de tener su propia Ley de Protección de Datos Personales. Esta normativa establece que el objetivo de la digitalización no es la vigilancia de la ciudadanía con fines policiales. Por el contrario, ese uso es excepcional y las autoridades con dichas competencias deben someterse a diversos controles para poder acceder a la información.

BRASIL

Con el lanzamiento del sistema Pix en 2020, una plataforma de pagos instantáneos creada y administrada por la autoridad monetaria de Brasil, la digitalización ha tenido un fuerte impacto en la formalización de la economía, la recaudación tributaria y el combate a la corrupción al incorporar a la banca al 75% de su población y a 15 millones de empresas. Este sistema de pagos instantáneos permite transacciones de bajo costo a través de códigos QR y llaves digitales para una mayor inclusión financiera.

Al integrar a la plataforma a bancos privados e instituciones no bancarias, Brasil ha incorporado a millones de personas antes excluidas del sistema formal, lo que ha facilitado pagos electrónicos y reducido el manejo de efectivo —cuyo uso es clave en la economía informal—. Además, la obligatoriedad de participación, junto con esquemas regulatorios de seguridad y prevención de fraudes, ha fortalecido la transparencia y disminuido la evasión fiscal. Hacia 2023, de acuerdo con un análisis del Banco Central do Brasil (2023), el 80% de la población ya había usado Pix, un indicador de la transición de los hábitos de pago en todos los segmentos de ingreso.

Sin embargo, aunque Brasil cuenta con marcos normativos, institucionales y judiciales que buscan limitar excesos, la concentración de datos interoperables, la proliferación de proyectos biométricos privados y municipales, junto con un historial de incidentes de seguridad y filtraciones, evidencian debilidades operativas, afectan la confianza pública y han generado preocupación tanto entre expertos como en la Autoridad Nacional de Protección de Datos de Brasil. Este contexto, que implica un riesgo potencial de vigilancia masiva, demanda la implementación de controles más estrictos y evaluaciones de impacto en derechos humanos.

INDIA

Las autoridades de la India lanzaron el sistema Aadhaar, una de las mayores bases de datos biométricos del mundo. Aadhaar proporciona a un total de 1,438 millones de habitantes (el 94% de la población) una identificación digital única basada en huellas dactilares y escaneo de iris. Esta plataforma ha permitido conectar a sus usuarios con servicios públicos, subsidios y cuentas bancarias. Ello ha facilitado la inclusión financiera y reducido el fraude en la entrega de apoyos gubernamentales.

Sin embargo, el modelo indio también ha sido objeto de críticas y desafíos judiciales relacionados con la privacidad y la protección de datos personales, lo que ha impulsado un debate nacional sobre la necesidad de establecer controles más estrictos al uso de la información por parte del Estado y garantizar derechos fundamentales como el consentimiento informado y el acceso a mecanismos de reparación.

Una de las críticas más fuertes al sistema Aadhaar es que, al recopilar y centralizar la información biométrica y demográfica de sus habitantes, abrió la puerta a un modelo de vigilancia masiva por parte del Estado. Diversos actores, incluidos activistas, juristas y organizaciones de derechos humanos, advirtieron que, sin garantías suficientes, el sistema podría ser utilizado para rastrear y controlar a la población, especialmente a grupos vulnerables o disidentes políticos. Por ello, el Tribunal Supremo de la India reconoció, en 2017, que la privacidad es un derecho fundamental, lo que generó un debate sobre si el sistema Aadhaar violaba ese principio. Aunque en 2018 la Corte Suprema falló a favor de la constitucionalidad del sistema, también impuso restricciones: prohibió su uso obligatorio por parte de bancos, empresas privadas y compañías telefónicas, y limitó su uso a ciertos programas sociales y fiscales. Desde entonces, la India cuenta con organismos autónomos dedicados a la protección de datos personales y a la ciberseguridad.

II. DIGITALIZACIÓN SIN CONTRAPESOS: RIESGOS ESTRUCTURALES DEL NUEVO MARCO LEGAL

Digitalizar con garantías: la pieza que falta

En el ya mencionado paquete de leyes se advierte, desde la exposición de motivos, que hay un enfoque orientado a la innovación y modernización de servicios gubernamentales. El organismo a cargo de este desarrollo es la Agencia de Transformación Digital y Telecomunicaciones (ATDT). Sin embargo, no se plantean mecanismos claros para que la ciudadanía conozca cómo, cuándo y con qué fines se usarán los datos personales solicitados a la población. Esto impone, como ya se mencionó, una asimetría entre Gobierno y ciudadanía al ampliar desproporcionadamente las facultades del Estado para intervenir en la vida cotidiana de ciudadanos, residentes extranjeros y empresas. Ello vulnera derechos como la privacidad, la propiedad, la libre expresión, la libertad de asociación y movilidad, la libertad de empresa, la defensa jurídica y la presunción de inocencia.

Con la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en marzo pasado, quedamos sin una autoridad que pudiera dirimir controversias entre autoridades todo tipo de autoridades y particulares en materia de derechos a la privacidad y protección de datos. Recordemos que el

INAI era el órgano constitucional autónomo que además de garantizar a la población el acceso a la información pública, protegía los datos personales.

Ante ello, el entonces Consejo de la Judicatura Federal, hoy Órgano de Administración Judicial, emitió el Acuerdo 8/2025 del 23 de junio, por el que habilita a los Juzgados de Distrito y Tribunales Colegiados en Aguascalientes para conocer de los juicios de amparo en materia de acceso a la información pública y protección de datos personales. Con esa medida —que respondió a la urgencia del momento—, serán ahora los juzgados y tribunales de Aguascalientes, los que tendrán que resolver casos de todo el país mediante el amparo. Esto abarcará actos de autoridades desde municipales hasta federales e incluso controversias derivadas de datos en posesión de particulares.

Aunque necesaria para el resguardo de derechos que quedaron desprotegidos, esta decisión parece insuficiente por varias razones: 1) Los costos que tendrá para la ciudadanía de todo el país que estos órganos estén concentrados en Aguascalientes. 2) La carga de trabajo de estos órganos jurisdiccionales puede aumentar considerablemente ante los efectos de la implementación del paquete de reformas que se ha aprobado a lo largo de este año —entre los que se incluye la extinción del INAI—, lo que plantea riesgos mayores para la población al haber desprotegido el derecho a la privacidad y la salvaguarda de los datos personales. 3) Además, en el contexto de la Reforma Judicial, estos jueces y magistrados habilitados, que se espera sean especialistas en la materia, serán removidos para sustituirlos por nuevos jueces a ser votados en las próximas elecciones judiciales en 2027.

Aunado a este contexto de desprotección jurídica, México se ha convertido en uno de los países más vulnerables a los ciberataques en el mundo. En 2024 registró 324 mil millones de intentos, de acuerdo con el *Global Threat Landscape Report 2025* de Fortinet. La desaparición del INAI agrava este panorama. A diferencia de la India, por ejemplo, hoy en México no existe una entidad independiente que supervise cómo se resguardan y usan nuestros datos, que esté al tanto de los avances de la industrialización del cibercrimen, y del mal uso de las herramientas de inteligencia artificial. No hay organismo en nuestro país que elabore protocolos y capacitación en ciberseguridad, que investigue en colaboración con las fiscalías sobre ciberdelitos y ponga a disposición de la población medios de defensa y de conocimiento sobre el uso de sus datos.

Cuando la digitalización vulnera derechos

En un Estado democrático, los actos que afectan la privacidad de las personas —conocidos también como actos de molestia— deben ser autorizados exclusivamente por el Poder Judicial, y nunca utilizados como medidas “preventivas” a cargo de órganos de inteligencia o cuerpos policiales, civiles o militares. Sin embargo, la nueva arquitectura jurídica abre la puerta a que las autoridades realicen investigaciones con fines de “prevención” del delito o como parte del “desarrollo de inteligencia en seguridad pública”, lo que en sí mismo vulnera el derecho a la privacidad y al debido proceso.

De acuerdo con el nuevo marco legal en materia de digitalización, una vez que el Centro Nacional de Inteligencia obtiene datos privados en tiempo real, puede legalizar su uso mediante coordinación con las fiscalías. En la práctica, esto implica que, conforme a la Ley de Inteligencia y al Código Nacional de Procedimientos Penales (CNPP), las policías y Fuerzas Armadas estarían facultadas para solicitar órdenes judiciales a posteriori —es decir, después de haber intervenido comunicaciones o realizado seguimientos en tiempo real—, lo que normaliza la invasión de la esfera privada de las personas.

Esta ampliación progresiva de las facultades legales establece incentivos para extender aún más los márgenes de intrusión de las autoridades en la vida privada de los ciudadanos. Un ejemplo reciente es la iniciativa de reforma a los artículos 30-B y 113-Bis del Código Fiscal. Fue presentada el 8 de septiembre de 2025 dentro del paquete económico 2026, y está en sintonía con el paquete de reformas aprobadas en el periodo extraordinario. La propuesta busca otorgar al SAT acceso permanente y en tiempo real a los sistemas y registros de todas las plataformas digitales, bajo la amenaza de bloqueo en caso de incumplimiento fiscal en materia de IVA. De ser aprobada sin cambios de fondo, cancelará el RFC y bloqueará temporalmente los servicios digitales de la persona física o moral vía concesionarios de telecomunicaciones. Esta medida afectaría la operación de plataformas de periodismo, comercio electrónico, streaming, teletrabajo, telemedicina, inteligencia artificial, e-learning, bancos, transporte, servicios financieros y más. Aunque pretende una mejor fiscalización, la reforma genera riesgos para derechos fundamentales como privacidad, libertad de tránsito, derecho a la movilidad, libertad de expresión y libre empresa. La medida —que sigue en discusión en el Congreso— ha encendido alertas en la sociedad civil y en el sector empresarial, que la consideran desproporcionada y riesgosa para el debido proceso y la privacidad de los usuarios y de las propias plataformas.

Desde la perspectiva del Estado de derecho, el acceso a información privada debe ser excepcional y únicamente autorizado por un juez, previa acreditación de indicios que hagan probable la comisión de un delito o una falta administrativa. La autorización judicial sólo debe proceder cuando las fiscalías presentan datos que justifiquen la investigación. Permitir que autoridades administrativas, policiales o militares accedan de manera automática y en tiempo real a información privada con fines de "prevención", inteligencia o fiscalización, erosiona el derecho a la privacidad y debilita la presunción de inocencia, principios protegidos tanto por la Constitución como por los tratados internacionales de derechos humanos suscritos por México.

Elementos clave del sistema digital aprobado en México durante el periodo extraordinario del Congreso (verano 2025)

El sistema se estructura en torno a una red interconectada de bases de datos y herramientas tecnológicas que centralizan información sensible y facilitan su acceso por parte de autoridades civiles y militares. Los elementos clave son:

- **Plataforma Única de Identidad:** Centraliza datos personales y biométricos de todos los ciudadanos, incluyendo huellas digitales, reconocimiento facial y registros de actividad relativa a cualquier registro, base o sistema de información de particulares que presten servicios financieros, de transporte, salud física y mental, telecomunicaciones, educación, asistencia privada, paquetería y servicios de entrega, registros patronales y de seguridad social, religiosos, los establecimientos residenciales de atención a las adicciones así como toda institución privada que administre registros o bases de datos de personas (i.e. historial médico, compras, empleo y uso de telecomunicaciones). Está diseñada para ser consultada en tiempo real por autoridades, lo que permite asociar la identidad de una persona con sus actividades diarias sin necesidad de una orden judicial.

- **Plataforma Central de Inteligencia:** Operada por la Subsecretaría de Inteligencia e Investigación Policial, integra datos de múltiples fuentes (públicas y privadas) para prevenir delitos y apoyar investigaciones penales. Sin embargo, la falta de controles judiciales plantea riesgos de abuso por parte de autoridades policiales civiles y militares.

- **Sistema Nacional de Información:** Interconecta bases de datos de seguridad pública, justicia y centros penitenciarios, lo que habilita el acceso a información fiscal, telefónica, migratoria e inmobiliaria. Incluye los Centros de Comando y Control (C5), que facilitan la coordinación interinstitucional y el monitoreo en tiempo real de los movimientos físicos en zonas urbanas.

- **La Clave Única de Registro Poblacional (CURP) Biométrica y la Llave MX para plataforma única de trámites y servicios públicos:** La CURP Biométrica asocia datos biométricos a la identidad de cada ciudadano, mientras que la Llave MX funciona como un mecanismo de autenticación digital para trámites y pago de servicios públicos en los tres órdenes de Gobierno. A partir del 16 de octubre, se comenzará a expedir la CURP Biométrica en todas las entidades federativas. Además del código alfanumérico de 18 dígitos que actualmente se maneja, incluirá huellas dactilares, escaneo del iris (de ambos ojos), fotografía y firma electrónica. La información será gestionada por la Secretaría de Gobernación (Segob) y el Registro Nacional de Población (Renapo)

- **Facultades del Ejército y la Guardia Nacional para tareas de vigilancia sin controles previos ni supervisión judicial:** La Guardia Nacional, bajo control de la Secretaría de la Defensa Nacional (Defensa), tiene ahora atribuciones para realizar tareas de inteligencia para fines de prevención del delito o de seguridad pública. Éstas incluyen la recolección de datos personales y de telecomunicaciones sin controles previos ni supervisión judicial.

Medidas en las leyes aprobadas que aumentan la incertidumbre jurídica del sector productivo

- **Se amplían las facultades de la Unidad de Inteligencia Financiera (UIF) de la Secretaría de Hacienda y Crédito Público (SHCP)** que permitirán al Gobierno federal ordenar bloqueos preventivos de cuentas bancarias sin necesidad de una orden judicial inmediata. Esto se logra mediante la reforma de 2025 a la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI) y al artículo 400 Bis del Código Penal Federal para ampliar el poder del Estado en materia de vigilancia financiera. Éste permite a la Fiscalía General de la República (FGR) investigar en todo momento, aún cuando no haya denuncia o querella de la SHCP. Aunque se mantiene como requisito de procedibilidad, la denuncia o querella podría ser posterior a la invasión de la esfera privada en aras de la investigación del Ministerio Público. Esto se añade a las facultades que refuerzan medidas cautelares como el congelamiento preventivo de activos, principalmente cuentas bancarias. En otras palabras, este nuevo marco legal permite acciones intrusivas a cuentas bancarias desde fases tempranas de investigación, y eleva el riesgo de violaciones al debido proceso, a la privacidad y a la seguridad jurídica de ciudadanos y empresas.

- **La Ley Nacional para la Eliminación de Trámites** impone el uso obligatorio de la CURP Biométrica y la Llave MX como los elementos habilitadores del expediente individual en la plataforma única de trámites y servicios. Ello representa riesgos para los datos personales de las personas físicas que funjan como representantes legales de empresas y organizaciones, pues deberán ceder su CURP Biométrica para el cumplimiento de trámites de estas corporaciones. A su vez, esto representa un riesgo para las empresas, pues dependerán de la voluntad y disponibilidad de su representante legal para ceder sus datos biométricos para que la empresa realice sus trámites.

- **La reforma a la Ley de Telecomunicaciones** también se modifica en este esquema al obligar a los operadores móviles a recabar y conservar grandes volúmenes de datos personales de los usuarios. Si bien esta ley aún exige autorización judicial o ministerial para intervenir comunicaciones privadas, la nueva Ley del Sistema Nacional de Inteligencia no contempla tales salvaguardas en sus artículos 24, 30, 36 al 38, de manera que convierten prácticamente todos los registros públicos y privados del país en fuentes obligadas de información para el sistema de inteligencia, incluyendo datos biométricos, fiscales, financieros, de salud, y de telecomunicaciones. Aunque dicho ordenamiento menciona que la interconexión con bases privadas debe respetar la ley de protección de datos, la amplitud de lo permitido representa una amenaza sistémica a la privacidad, ya que no establece límites claros ni control judicial previo para el acceso a esta información. Esto es, la legislación da poderes ilimitados al Estado para recolectar, interconectar y utilizar información personal y privada en tiempo real bajo el argumento de la seguridad pública sin garantías procesales efectivas, control judicial ex ante y mecanismos de rendición de cuentas públicos y transparentes. Esta contradicción legal abre la puerta a que las autoridades accedan, sin supervisión judicial efectiva, a información en tiempo real de prácticamente cualquier usuario del sistema telefónico.

III. ANÁLISIS Y PROPUESTAS ESPECÍFICAS AL MARCO LEGAL APROBADO

El necesario avance de la identidad digital y el uso de datos biométricos exige adoptar las mejores prácticas internacionales para proteger los derechos de las personas. Estos sistemas, al concentrar información sensible, deben operar con contrapesos institucionales, rendición de cuentas, control judicial y ministerial, y plena transparencia. Sin estos elementos, se corre el riesgo de derivar en un sistema de vigilancia del Estado hacia la población, afectando libertades fundamentales y la confianza ciudadana.

La integración de Llave MX con una CURP Biométrica es una buena idea si se alinea con estándares como los que promueve el Banco Interamericano de Desarrollo (BID). Estos incluyen principios de inclusión, seguridad y protección de datos; además, promueven identidades digitales universales pero respetuosas de derechos, con consentimiento informado, mecanismos de auditoría y accesibilidad para grupos vulnerables como adultos mayores, niños, personas con discapacidad, migrantes, etcétera. Aunque la Llave CDMX, diseñada e implementada en la Ciudad de México, ha sido reconocida como una buena práctica por el mismo BID, la iniciativa de ley actual en México no garantiza aún estos estándares internacionales. Para cumplirlos, se requiere que el marco legal asegure que la biometría sea voluntaria y que existan salvaguardas efectivas contra usos indebidos y exclusión tecnológica.

A continuación, presentamos un cuadro que contrasta el marco legal aprobado, los principales riesgos identificados y las propuestas desde la sociedad civil para construir contrapesos democráticos y tecnológicos ante el nuevo sistema de vigilancia masiva del Estado mexicano.

Ley / Reforma	Instituciones clave en el paquete de digitalización y sistema de vigilancia	Riesgos principales	Propuesta de mitigación / reconstrucción de contrapesos	Artículos de análisis
Ley General del Sistema Nacional de Seguridad Pública (LGSNSP)	Crea el Sistema Nacional de Información con acceso en tiempo real a datos fiscales, telefónicos, migratorios y de geolocalización; conecta C5, justicia y seguridad pública; centraliza decisiones en el Consejo Nacional.	Acceso a datos personales e intervención de comunicaciones **sin orden judicial**; debilitamiento del federalismo y concentración de facultades en autoridades federales (incluido el Ejército a través de la Guardia Nacional); vigilancia masiva sin controles.	**Requerir autorización judicial previa** para acceder a datos personales en investigaciones delictivas; Establecimiento legal de **auditorías ciudadanas** sobre el uso de datos personales; **Mecanismos federales de supervisión** sobre el uso de datos personales en investigaciones delictivas. **Régimen de responsabilidades y cadena de mando de las autoridades** que abusen de datos personales con fines de prevención del delito. **Socialización para medios de comunicación y sociedad civil** sobre las nuevas atribuciones y sus procedimientos.	9, f IX; 10 f V, XIII; 22 f VIII, a); 26 f VIII; 32 fVIII; 47 f XIII, XIV, XVIII, XX, XXI; 49 fI, II, III; 50 f III, IV, V; 51 III, IV; 52 f III IV; 54; 57 II, III; T 6o, 100 a 107, 113, 129 fIX 102, 106 **(Registro Nacional de Eficiencia Ministerial)**, 107
Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNISP)	Crea la Subsecretaría de Inteligencia y la Plataforma Única de Identidad con acceso a datos biométricos, fiscales, financieros, médicos y de telecomunicaciones en tiempo real y sin control judicial para fines de "prevención" del delito o de desarrollar "productos de inteligencia para la seguridad pública". Esta Ley distingue entre análisis y recopilación de datos privados para fines de "prevención" o "seguridad pública" (sin necesidad de autorización judicial), de la recopilación de información privada para fines de investigación penal con control de MP y órdenes judiciales. Pero en ambos casos, se trata de actos de molestia que deberían ser autorizados siempre por jueces, bajo la condición de que hay una causa probable de delito.	La ley da acceso a las autoridades a cualquier base de datos pública y privada de todos los sectores para fines de "prevención" o de "seguridad pública". Las Fuerzas Armadas y la Guardia Nacional están autorizadas para conducir actividades de inteligencia o vigilancia sin restricción judicial. **Vulneración del derecho a la privacidad y a la presunción de inocencia;** uso político de inteligencia; **opacidad institucional.** Posible abuso de autoridades policiales o de órganos de inteligencia sobre la información y datos personales.	**Establecer un órgano externo a la Secretaría con participación ciudadana** que en conjunto con la autoridad establezcan las políticas sobre el uso de datos personales, así como directrices de capacitación para las personas funcionarias responsables de alimentar las bases de datos **Desarrollar un código de ética para los servidores públicos que permita** identificar malas prácticas en el llenado de las bases y en el uso de la información. Establecer una **comisión permanente bicameral que audite y supervise** el actuar del cluster de instituciones que participan en la realización de acciones de inteligencia **Establecer mecanismos para atender reclamos** ciudadanos por mala praxis. **Desarrollar campañas de socialización** para medios de comunicación y sociedad civil sobre las nuevas atribuciones y sus procedimientos. **Promover reformas correctivas a la ley** que introduzcan mecanismos de control, transparencia y vigilancia a los funcionarios públicos que utilicen datos personales e información confidencial de ciudadanos y empresas.	7, 12 f III, XI; 13, 16, 19 fII, III, VI, XI, XIV, 21, 22, 23, 24, 25, 26, 27, 28, 30, 31, 32, 35, 36, 37, 39, 44, 50, 51, 55

Ley / Reforma	Instituciones clave en el paquete de digitalización y sistema de vigilancia	Riesgos principales	Propuesta de mitigación / reconstrucción de contrapesos	Artículos de análisis
Ley de la Guardia Nacional (LGN) Ley de Disciplina del Ejército, Fuerza Aérea y Guardia Nacional (LDEFGN)	Autoriza al Ejército a recabar y procesar datos personales y de telecomunicaciones; refuerza tareas de inteligencia **sin contrapesos civiles y sin rendición de cuentas.** Las facultades otorgadas permiten a la Guardia Nacional realizar tareas de vigilancia e inteligencia bajo el argumento de prevención. **No hay responsabilidades ni consecuencias disciplinarias** específicas por violación de derechos o abuso en el uso de datos personales.	Vulneración de los principios constitucionales de legalidad, necesidad y proporcionalidad en la intervención de comunicaciones privadas (Art. 16 de la Constitución). Militarización de la seguridad pública y de la investigación delictiva; riesgos de abuso y opacidad y falta de rendición de cuentas Cualquier ciudadano puede ser monitoreado sin justificación específica, lo que contraviene la presunción de inocencia. Sin lineamientos públicos ni mecanismos de supervisión externa, este tipo de análisis masivo **podría derivar en sesgos discriminatorios** o persecución arbitraria	**Crear un observatorio independiente** con facultades de fiscalización de las autoridades de seguridad pública que tienen estas facultades. **Crear y difundir campañas de sensibilización** para la ciudadanía sobre los riesgos de la militarización y la urgente necesidad de exigir mecanismos de control y revisión y desempeño de la Guardia Nacional. **Transparentar los procesos de responsabilidad militar, administrativa y penal** de autoridades que estén involucradas en el abuso de datos personales **Impulsar amparos y acciones de inconstitucionalidad** cuando se usen tecnologías de vigilancia sin orden judicial o se cometan detenciones arbitrarias. **Acompañar casos emblemáticos** de comunidades afectadas (por ejemplo, en zonas con militarización de facto). **Documentar la falta de controles civiles** y presionar al Poder Judicial a revisar criterios sobre proporcionalidad y legalidad. **Dar seguimiento a los casos de autoridades que abusen** de los sistemas de información para que no queden impunes. **Impartir talleres de socialización** para medios de comunicación y sociedad civil sobre las nuevas atribuciones y sus procedimientos. **Legislar para incluir en la LDEFGN** consecuencias por violar derechos digitales o por abuso en el uso de datos personales.	Ley de la Guardia Nacional: 9 f XXVI, XXXVII, fXXXVIII, fXXIX

Ley / Reforma	Instituciones clave en el paquete de digitalización y sistema de vigilancia	Riesgos principales	Propuesta de mitigación / reconstrucción de contrapesos	Artículos de análisis
Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas (LGMDF)	**Crea la Plataforma Única de Identidad (PUI)** para centralizar datos biométricos y personales que incluye: **I.** El Registro Nacional de Personas Desaparecidas y No Localizadas; **II.** La Base Nacional de Carpetas de Investigación de Personas Desaparecidas y No Localizadas; **III.** El Banco Nacional de Datos Forenses; **IV.** Registros Administrativos, y **V. Cualquier registro, base o sistema de información de particulares** que presten servicios financieros, de transporte, salud física y mental, telecomunicaciones, educación, asistencia privada, paquetería y servicios de entrega, registros patronales y de seguridad social, religiosos, los establecimientos residenciales de atención a las adicciones así como toda institución privada que administre registros o bases de datos de personas, cuya consulta sea necesaria para la investigación, búsqueda, localización e identificación de personas desaparecidas o no localizadas. El sistema permite el monitoreo continuo, por parte de la Fiscalía General de la República, las fiscalías locales y las comisiones de búsqueda, de la CURP de personas desaparecidas, para generar alertas automáticas cuando se detecta actividad en registros públicos o privados. La Secretaría de Gobernación es la entidad competente para dar acceso a la PUI sin necesidad de orden judicial, siempre que se utilice para la investigación, búsqueda, localización e identificación de personas desaparecidas o no localizadas	La ley no sanciona el uso indebido de la PUI ni exige trazabilidad ni controles externos. Limita la base nacional a Personas Desaparecidas y No Localizadas, dejando fuera carpetas con otros delitos vinculados. La ley no prevé que las Unidades de Investigación Especializadas en Desaparición puedan atraer y perseguir los delitos relacionados con las desapariciones, cuestión que es fundamental para realizar investigaciones integrales que pongan en contexto el origen de la desaparición de personas. Se mantiene intacta la fracción XIII del artículo 70 que dice que las Fiscalías Especializadas deben “remitir a las autoridades competentes las investigaciones y actuaciones” que tengan relación con otros delitos. Esto mantiene la práctica de fragmentar los casos de desaparición, aunado a que la Base Nacional de Carpetas se restringe a Personas Desaparecidas y No Localizadas, dejando fuera carpetas en las que se investigan otros delitos relacionados con este fenómeno criminal. La ley no regula responsabilidades administrativas o penales por consultas indebidas, uso excesivo o desvío de propósito en el acceso a la PUI. La ley no establece un mecanismo de trazabilidad obligatoria, ni se prevé la intervención de órganos garantes de derechos humanos en la supervisión del uso de esta plataforma. La ley no contempla controles ex ante ni ex post sobre la proporcionalidad o legalidad de las consultas.	**Crear un órgano de seguimiento** para la integración y tratamiento del padrón de personas desaparecidas y no localizadas con esquemas de trazabilidad y auditorías externas. Generar esquemas de **colaboración ágil y oportuna entre autoridades investigadoras, jueces y empresas de telecomunicaciones** para la localización de personas, con rendición de cuentas e implicaciones procesales en investigaciones penales (nulidad de pruebas obtenidas ilícitamente). **Armonizar la ley** con un marco jurídico actualizado en materia de protección de datos personales que constituya un nuevo órgano que concentre estas responsabilidades a nivel nacional según las mejores prácticas internacionales. **Perfeccionar la ley** para establecer un régimen sancionador con multas, inhabilitación y responsabilidad directa por uso indebido de la PUI; y para complementar con incentivos positivos como certificaciones éticas. Incorporar en la ley mecanismos de consentimiento informado, análisis de proporcionalidad de la información para las consultas, y de exclusión temporal de datos sensibles a solicitud de familiares, especialmente en contextos de riesgo.	12 Bis, f V; 12 Quinquies; 12 Sexies– 12 Nonies; 119; 12 Bis V; 43 Bis y 114 Bis

Ley / Reforma	Instituciones clave en el paquete de digitalización y sistema de vigilancia	Riesgos principales	Propuesta de mitigación / reconstrucción de contrapesos	Artículos de análisis
Ley General de Población	Impone CURP Biométrica como requisito obligatorio para trámites.	La capacidad de acceder a datos biométricos y geolocalización en tiempo real sin orden judicial vulnera principios constitucionales como la privacidad y la presunción de inocencia. Impone **sanciones de 10,000 a 20,000 UMAs, equivalentes a 1.1 a 2.2 millones de pesos, a privados que no entreguen datos o no integren datos biométricos.** Esto genera presión para que instituciones y ciudadanos faciliten acceso a la información sin garantía judicial. La reforma a la ley no prevé en los artículos transitorios los mecanismos y presupuestos que se requerirán para empadronar en la CURP Biométrica a mexicanos residentes en el extranjero.	**Crear observatorios ciudadanos** que vigilen interoperabilidad entre bases de datos, y protocolos de acceso de autoridades. **Impulsar que existan autoridades responsables focalizadas en la protección ciudadana digital** que den asesoría y acompañamiento legal y técnico a víctimas, personas investigadas o vigiladas y ciudadanos afectados por el uso indebido de las herramientas de vigilancia de la ley. **Promover reformas correctivas a la ley**, con cinco ejes: • *Obligación expresa de autorización judicial* para cualquier acceso a datos sensibles. • *Reducción de sanciones coercitivas a privados* por no colaborar con vigilancia estatal. • *Cláusulas de protección reforzada a derechos humanos* y exclusión de pruebas obtenidas sin control legal. • *Separar fines forenses* de vigilancia general; • *Garantizar derechos de consentimiento* y acceso sin medidas de protección de datos personales biométricos. **Armonizar la ley** con un marco jurídico actualizado en materia de protección de datos personales que constituya un nuevo órgano que concentre estas responsabilidades a nivel nacional según las mejores prácticas internacionales. **Impartir talleres de socialización** para medios de comunicación y sociedad civil sobre las nuevas atribuciones y sus procedimientos.	**Ley General de Población:** 91 bis; 91 Sexies; 114 bis.

Ley / Reforma	Instituciones clave en el paquete de digitalización y sistema de vigilancia	Riesgos principales	Propuesta de mitigación / reconstrucción de contrapesos	Artículos de análisis
Ley Nacional para Eliminar Trámites Burocráticos (LNETB)	Establece la Llave MX como sistema de autenticación digital obligatoria ligada a la CURP Biométrica.	Expansión de vigilancia al ámbito cotidiano y digital; discriminación digital. **Posibles violaciones al TMEC:** **Capítulo 27 Anticorrupción.** (Artículo 27.3) **Capítulo 28 Buenas prácticas** regulatorias (Artículo 28.3, 28.11) Obligación para las personas morales de uso de CURP Biométrica de representante legal para el cumplimiento de obligaciones de la persona moral. Riesgo de incumplimiento	**Promover reformas correctivas a la ley** para habilitar el Registro Federal de Contribuyentes (RFC) como mecanismo de acceso a la plataforma para que personas morales puedan cumplir sus trámites en la plataforma Llave Mx sin necesidad del uso de la CURP Biométrica. **Crear consejos tripartitas de mejora regulatoria** para habilitar mecanismos de participación ciudadana para la simplificación y la digitalización según las buenas prácticas regulatorias.	Sección II; 13 f XVI; 16 f VIII; 31, 36 f I al VIII; 49; 62, 63, 91, 92, 95, 96; 102; 113 y 114; Tr.12°.
Reforma a la Ley Federal de Telecomunicaciones y Radiodifusión (reformada) (LFTR)	Obliga a operadores de telecomunicaciones a conservar datos de geolocalización de dispositivos, y registros telefónicos y datos sin orden judicial y sin definir claramente qué autoridades acceden o bajo qué criterios. Conservación obligatoria por dos años de información sensible como llamadas, mensajes, ubicación y patrones de uso de todos los usuarios. Identificación obligatoria del usuario con la CURP Biométrica para contratar líneas telefónicas y servicios de internet móviles y fijos. La Comisión Reguladora de Telecomunicaciones podrá suspender líneas no asociadas a usuarios con CURP Biométrica.	No obstante que la LFTR mantiene el principio de inviolabilidad de las comunicaciones privadas salvo que exista autorización judicial o del titular del Ministerio Público estatal, la LSNISP autoriza el acceso a dichos datos sin previa orden judicial o del Ministerio Público. La Agencia de Transformación Digital y Telecomunicaciones (ATDT) y la Comisión Nacional de Telecomunicaciones (CNT) podrán suspender transmisiones bajo criterios que ellas mismas determinen como “derechos de las audiencias”. La ATDT y la CNT no tienen contrapesos. • Los operadores de telecomunicaciones están obligados 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 los operadores de telecomunicaciones	**Convocar una plataforma multisectorial** (académicos, periodistas, OSCs, empresas tecnológicas y usuarios) para redactar una propuesta ciudadana que exija: • Que la ATDT y la CNT convoquen a la creación de un Comité Técnico Nacional de Gobernanza Digital con participación de una representación por cada orden de gobierno, más los sectores privado, académico y social para **el diseño de lineamientos** que equilibren el ejercicio de los derechos de audiencias, los límites de actuación del ombudsman de las audiencias en cada medio, y la libertad creativa y empresarial de creadores de contenidos, empresas de medios y audiencias. • **Que dicho comité desarrolle un Plan Nacional de Derechos Digitales** que vigile la neutralidad de la red. Es decir, que no pueda ordenar a concesionarios ralentizar, bloquear o despriorizar contenido en función de “seguridad nacional”, “orden público” o “protección de derechos de audiencias” sin una orden judicial estricta y con control constitucional posterior .	10 f XLIII; 64 f III;103, 183 f I a XII; 232

Ley / Reforma	Instituciones clave en el paquete de digitalización y sistema de vigilancia	Riesgos principales	Propuesta de mitigación / reconstrucción de contrapesos	Artículos de análisis
		deberán conservar y almacenar de manera pormenorizada. **Posibles violaciones al TMEC:** **Capítulo 18 Telecomunicaciones:** Artículo 18.4: Protección de secretos empresariales; Artículo 18.17: Imparcialidad del regulador, independiente del Ejecutivo Federal. **Capítulo 19 Comercio Digital:** Artículo 19.16: Código Fuente; Seguridad de la red;	• **La inclusión de mecanismos concretos de transparencia y rendición de cuentas** en la elaboración del reglamento de la Comisión Nacional de Telecomunicaciones. **Promover hackatones** a jóvenes con talentos digitales —programación, diseño, análisis de datos— que propongan soluciones a causas públicas ante este nuevo sistema de vigilancia.	
Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI) Reforma al artículo 400 Bis del Código Penal Federal	Amplía facultades del Estado para fiscalizar operaciones financieras de personas físicas y morales; facilita uso de información financiera en investigaciones sin requerimientos judiciales previos; tipifica operaciones ilícitas con mayor amplitud.	Se amplían las facultades de la UIF, facilitando bloqueos preventivos de cuentas bancarias sin garantía de recursos judiciales inmediatos Las personas físicas y MiPyMEs enfrentan nuevas cargas administrativas y regulatorias (Registro de información detallada en los sistemas electrónicos) con costos elevados y riesgo de penalización por incumplimiento. La reforma penal (400 Bis) permite a la FGR investigar en todo momento, aún cuando no haya denuncia o querella de la SHCP. Aunque se mantiene como requisito de procedibilidad la denuncia o querella de la SHCP, esta podría ser posterior a la invasión de la esfera privada en aras de la investigación del MP. Riesgo de criminalización preventiva; uso indebido de información financiera contra opositores o críticos; eliminación de garantías procesales. **Posibles violaciones al TMEC:** **Capítulo 14 Inversión:** Artículo 14.3 Trato Nacional; Artículo 14.4: Trato de Nación Más Favorecida; Artículo 14.6: Expropiación indirecta.	**Vigilar el uso de facultades discrecionales de la UIF** (como congelamiento de cuentas), promover la transparencia y garantizar el respeto al debido proceso. **Presionar para que la Auditoría Superior de la Federación** audite anualmente el desempeño de la UIF. **Crear una red de asesoría legal** gratuita o accesible con apoyo de colegios de abogados. **Difundir guías ciudadanas** explicativas sobre obligaciones reales y riesgos. **Impulsar un programa de cumplimiento** proporcional y progresivo. **Promover reformas correctivas a la ley** para: • Limitar los bloqueos preventivos a resoluciones judiciales firmes. • Establecer mecanismos de apelación inmediatos. • Reducir cargas regulatorias injustificadas para MiPYMEs y personas físicas. • Evitar la criminalización excesiva de omisiones formales o administrativas. Esto es, las omisiones sin dolo no son delitos. • Incluir excepciones explícitas para actividades de bajo riesgo económico o sin intención fraudulenta.	**LFPIORPI** 18, f VI **Código Penal Federal** 400 Bis

IV. CONCLUSIONES Y RECOMENDACIONES

Para balancear y completar un sistema de digitalización democrático, incluyente y seguro, se necesitan establecer límites claros —en la normatividad y en el entramado institucional del Gobierno en sus tres niveles—, respecto del actuar de las autoridades respecto de sus facultades para recabar y usar información de manera masiva en función de los derechos humanos vigentes en nuestra Constitución Política. La participación ciudadana y el papel de la sociedad civil y la iniciativa privada a través de sus órganos de representación y vigilancia como cámaras industriales y sindicatos, permitirían visibilizar abusos, exigir límites legales y promover mecanismos de control democrático.

Estas son nuestras recomendaciones en orden de prioridad:

Desde el Congreso:

- **Establecer una comisión permanente bicameral** que audite y supervise el actuar del cluster de instituciones que participan en la realización de acciones de inteligencia e investigación penal.

- **Legislar la creación de un organismo de protección a los datos personales** que vigile, sancione y dote a los ciudadanos de mecanismos de defensa ante abusos por parte de las autoridades o de las empresas que hagan mal uso de los datos personales.

- **Legislar y armonizar mecanismos de control para funcionarios públicos y personal de las fuerzas armadas** que violen derechos digitales o abusen del uso de datos personales de la población.

- **Promover una Ley de Ciberseguridad**. Debe garantizar no sólo la protección del Estado, sino la privacidad, integridad y autonomía digital de las personas según las mejores prácticas internacionales.

- **Ratificar el Convenio de Budapest en Ciberseguridad** para modernizar y armonizar el marco jurídico de México, y fortalecer la cooperación internacional en la materia.

- **Promover que la normatividad para la implementación de la CURP Biométrica como documento de identidad** cumpla con las mejores prácticas internacionales y distinga tratamientos diferentes y adecuados para empresas y grupos vulnerables como: adultos mayores, infancias y adolescentes, migrantes, personas con discapacidades, etcétera.

- **Reformar la Ley de Eliminación de Trámites** para reducir los espacios de discrecionalidad para las autoridades, ampliar los espacios de participación ciudadana y habilitar el Registro Federal de Contribuyentes como mecanismo de validación al sistema de cumplimiento de trámites para las empresas.

- **Reformar la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI) y el artículo 400 Bis del Código Penal** Federal para limitar los bloqueos preventivos a resoluciones judiciales firmes, establecer mecanismos de apelación inmediatos, reducir cargas regulatorias injustificadas para MiPYMEs y personas físicas, evitar la criminalización excesiva de omisiones formales o administrativas e incluir excepciones explícitas para actividades de bajo riesgo económico o sin intención fraudulenta.

- **Reformar las leyes de Inteligencia y de Seguridad Pública** para aclarar que el uso de datos personales e intervención de comunicaciones sólo se podrá utilizar en investigaciones criminales previa orden judicial, y revisar la redacción de los artículos que habilitan a los cuerpos de seguridad sobre este uso para fines de "prevención del delito" e "inteligencia" sin orden judicial.

Desde el Ejecutivo:

- **Definir un plan de implementación de la CURP Biométrica** para priorizar y gradualmente poner a prueba su uso en diferentes servicios públicos. Que dicho plan y sus resultados sean públicos y sometidos a escrutinio ciudadano.

- **Transparentar medidas de ciberseguridad** de los sistemas en los que se alojen los datos personales

- **Emitir un Código de Ética de todas las autoridades** que intervienen en el registro y uso de datos personales, y fortalecer el sistema de responsabilidades administrativas, civiles y penales por abuso de información privada.

- **Establecer auditorías externas** que permitan verificar el diseño del sistema de digitalización de datos y su uso para la prestación de servicios públicos.

- **Desarrollar y cumplir códigos de conducta** para que desde las instituciones de seguridad pública (con énfasis en Guardia Nacional y personal militar) eviten el uso de facultades de intervención de comunicaciones bajo la justificación de prevención.

- **Establecer protocolos que permitan identificar la cadena de mando** cuando se autoriza el acceso a datos personales al personal de instituciones de seguridad pública.

- **Definir la autoridad responsable de proteger derechos digitales y a la privacidad de datos personales**.

- **Establecer protocolos de investigación criminal** que impliquen actos de molestia que requieren autorización judicial, cuyo diseño sea colaborativo entre cuerpos de seguridad, fiscalía, poder judicial federal y organizaciones civiles especializadas en materia penal. En estos protocolos será clave seguir estándares internacionales.

- **Establecer indicadores que permitan dar seguimiento a la implementación de las políticas de digitalización** en materia de prestación de servicios y de respeto a derechos.

Desde el Poder Judicial:

- **Avanzar hacia la digitalización de trámites judiciales para mejorar el acceso a la justicia**, cuidando los derechos al debido proceso, privacidad y libertad.

- **Proteger derechos de debido proceso y privacidad de datos,** en el sentido de los precedentes relevantes en materia judicial cuando la Suprema Corte declaró inconstitucionales el Padrón Nacional de Usuarios de Telefonía Móvil y las operaciones encubiertas de la Guardia Nacional en las acciones de inconstitucionalidad 82/2021 y 62/2019, respectivamente.

- **Seguir estándares internacionales en materia de protección de derechos digitales**.

Desde sociedad civil

- **Capacitar al personal judicial en materia de protección de derechos digitales**.
- **Dar seguimiento a los casos de autoridades que abusen de los sistemas de información** para que no queden impunes los responsables de espionaje (como en el caso Pegasus).
- **Crear plataformas de monitoreo ciudadano**, como observatorios, auditorías ciudadanas, impulsar el periodismo de investigación, las defensorías públicas, y el acompañamiento a víctimas que puedan visibilizar y documentar abusos.
- **Impartir talleres de socialización** para medios de comunicación y sociedad civil sobre las nuevas atribuciones y sus procedimientos que permitan su puntual monitoreo
- **Impulsar —desde los medios masivos y redes sociales— la creación de campañas de sensibilización pública** sobre los riesgos de la vigilancia masiva en materia de derechos humanos y principios democráticos. Estos esfuerzos contarían con el apoyo de las organizaciones de la sociedad civil y el sector académico.
- **Generar programas de alfabetización digital** para que la población de todas las edades aprenda a usar herramientas informáticas, cierre la brecha tecnológica y adquiera capacidades para fortalecer su propia ciberseguridad. Es importante que los políticos y/o legisladores del futuro aprendan sobre protección de datos en clave democrática.
- **Exigir desde todos los frentes ciudadanos transparencia y rendición de cuentas** al Gobierno con respecto al uso de datos personales.
- **Crear contrapesos ciudadanos** que participen en ejercicios de Parlamento Abierto que sean incorporados en las piezas legislativas, para provocar reformas correctivas que garanticen controles judiciales y seguridad en el manejo de la información personal y derechos de privacidad.
- **Establecer un órgano ciudadano** que ofrezca a las autoridades la oportunidad de trabajar en conjunto para establecer las directrices de capacitación para las personas funcionarias responsables de alimentar las bases de datos, así como un código de ética para identificar malas prácticas en el llenado de las bases y en el uso indebido de la información.
- **Dotar al órgano mencionado de la facultad de involucrarse** en el establecimiento de sanciones ante malas prácticas en el llenado de bases y abuso de la información.
- **Promover amparos contra leyes invasivas**. Esta medida encarece políticamente su implementación ya que es una manera de forzar al Gobierno a dar explicaciones en público para legitimar su actuar.
- **Denunciar las violaciones a la privacidad ante instancias internacionales** como la Comisión Interamericana de Derechos Humanos (CIDH) o la Organización de las Naciones Unidas (ONU). La presión internacional y la formación de alianzas con organismos de derechos humanos son clave para encarecer la vigilancia masiva y fortalecer la impugnación ciudadana.

REFERENCIAS

- Agencia Digital de Innovación Pública (ADIP). (2022). Reconoce Banco Interamericano de Desarrollo a la Ciudad de México por los avances de Llave CDMX. Recuperado de https://www.adip.cdmx.gob.mx/comunicacion/nota/reconoce-banco-interamericano-de-desarrollo-la-ciudad-de-mexico-por-los-avances-de-llave-cdmx

- Artículo 19 México y Centroamérica (2025). Juez otorga suspensión definitiva a ARTICLE 19 contra normas de vigilancia. https://articulo19.org/juez-otorga-suspension-definitiva-a-article-19-contra-normas-de-vigilancia/#_ftn1

- Banco Central do Brasil. (2023). Relatório de Economia Bancária e Pix. Brasília: BCB. relatorio_gestao_pix_2023.pdf

- Banco Interamericano de Desarrollo (BID). (2025). Data and Digital Government. Recuperado de https://www.iadb.org/en/who-we-are/topics/modernization-state/data-and-digital-government

- Banco Mundial. (2016). World Development Report: Digital Dividends (Capítulo sobre conectividad y crecimiento). Recuperado de https://openknowledge.worldbank.org/server/api/core/bitstreams/12e40c3f-5e54-440e-8f0f-982edcb156c9/content

- Cámara de Diputados. (2025). Ley de Disciplina del Ejército, Fuerza Aérea y Guardia Nacional (LDEFAM). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LDEFAM.pdf

- Cámara de Diputados. (2025). Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI.pdf

- Cámara de Diputados. (2025). Ley de la Guardia Nacional (LGN). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf

- Cámara de Diputados. (2025). Ley General de Población (LGP). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGP.pdf

- Cámara de Diputados. (2025). Ley General del Sistema Nacional de Seguridad Pública (LGSNSP). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf

- Cámara de Diputados. (2025). Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas (LGMDFP). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGMDFP.pdf

- Cámara de Diputados. (2025). Ley de Modernización de Trámites y Regulaciones (LMTR). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LMTR.pdf

- Cámara de Diputados. (2025). Ley Nacional para Eliminar Trámites Burocráticos (LNETB). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LNETB.pdf

- Cámara de Diputados. (2025). Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (LSNIIMSP). Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LSNIIMSP.pdf

- Centro i. (2025). Conéctamex. Recuperado de https://centroi.org/conectamex/ Check Point. (2025). Security Report 2025. Recuperado de https://engage.checkpoint.com/security-report-2025

- Consumo TIC (2025). Riesgos legales ante eventual bloqueo de plataformas digitales. https://consumotic.mx/telecom/riesgos-legales-ante-eventual-bloqueo-de-plataformas-digitales-alai/

- Diario Oficial de la Federación (DOF). (2025, 16 de julio). DECRETO por el que se reforman y adicionan diversas disposiciones de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, y se reforma el artículo 400 Bis del Código Penal Federal. Decreto publicado en el DOF. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5763161&fecha=16/07/2025#gsc.tab=0

- Digital Policy Alert (2025). Brazil: National Data Protection Authority announced an investigation into Tools for Humanity over biometric data processing for World ID project. https://digitalpolicyalert.org/change/12675

- Government of India Press Information Bureau (2024). Aadhaar: A Unique Identity For The People. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2067940

- International Association of Privacy Professionals (IAPP) (2018). Blockchain: Practical use cases for the privacy pro — Learning from Estonia. https://iapp.org/news/a/blockchain-practical-use-cases-for-the-privacy-pro-learning-from-estonia/?utm_source=chatgpt.com

- International Institute for Management Development (IMD). (2025). World Digital Competitiveness Ranking 2025. Recuperado de https://www-imd-org.translate.goog/centers/wcc/world-competitiveness-center/rankings/world-competitiveness-ranking/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wa

- JCSC Global digital risk management solutions (2025). La revolución fintech de Brasil construyó acceso a gran escala. Ahora enfrenta el costo de la velocidad. https://juicyscore.ai/es/blog/brazil-fintech-revolution-pix-digital-payments-fraud

- Mathos Filho (2025). Law and technology in Brazil: trends, challenges, and opportunities for 2025. https://www.mattosfilho.com.br/en/unico/technology-brazil-trends-2025/

- Riquelme Rodrigo (2025). La Alai rechaza que plataformas digitales se conecten al SAT. El Economista. https://www.eleconomista.com.mx/tecnologia/alai-rechaza-plataformas-digitales-conecten-sat-20250922-778212.html

- Red en Defensa de Derechos Digitales (R3D) (2025). Reforma al Código Fiscal Pretende Acceso Permanente a Datos de Plataformas Digitales. https://r3d.mx/2025/09/23/reforma-al-codigo-fiscal-pretende-acceso-permanente-a-datos-de-plataformas-digitales/

- Republic of Estonia E-Residency (2025). Do Business Securely. https://www.e-resident.gov.ee/do-business-securely/

- Suprema Corte de Justicia de la Nación (SCJN). (2019). Acción de inconstitucionalidad 62/2019. Recuperado de https://www2.scjn.gob.mx/juridica/engroses/cerrados/Publico/Proyecto/AI62-2019PL-Ver230217.pdf

- Suprema Corte de Justicia de la Nación (SCJN). (2021). Acción de inconstitucionalidad 82/2021. Recuperado de https://transparencia-ciudadana.scjn.gob.mx/resoluciones-relevantes-de-la-SCJN/derechos-digitales/AI-82-2021

Incidir Hoy | Construyamos un sistema digital confiable para todos los mexicanos, es resultado del esfuerzo de los integrantes de México Evalúa, Centro de Análisis de Políticas Públicas. La investigación, el análisis y la redacción no hubieran sido posibles sin la participación de cada miembro del equipo:

Mariana Campos
Directora General de México Evalúa

Ana Lilia Moreno
Coordinadora del Programa de Regulación y Competencia

Susana Camacho
Coordinadora del Programa de Justicia

Felipe Soto
Edición

Miguel Cedillo
Edición gráfica

Priscila García
Coordinadora de Comunicación

Mariana Villalobos, Kenia Chávez y Cinthia Galán
Equipo de comunicación

El contenido de este artículo es responsabilidad de México Evalúa D.R. 2025, México Evalúa, Centro de Análisis de Políticas Públicas Jaime Balmes No. 11, Edificio D, 2o. piso, Col. Los Morales Polanco, 11510, Ciudad de México T. +52 (55) 5985