

ANEXO 5. Línea del tiempo: Marco regulatorio internacional

1948 - Declaración Universal de Derechos Humanos

Estableció la prohibición de injerencias arbitrarias en la vida privada, sentando una base fundamental contra la vigilancia masiva.

1965 - Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial

Reforzó el derecho de igualdad ante la ley y la protección de la privacidad, con un enfoque especial en grupos vulnerables.

1966 - Pacto Internacional de Derechos Civiles y Políticos (PIDCP).

Consagra el derecho a que nadie sea objeto de injerencias arbitrarias o ilegales en su vida privada, familia, domicilio o correspondencia, y el derecho a la protección legal contra tales injerencias.

1969 - Convención Americana sobre Derechos Humanos (CADH) (Pacto de San José)

Prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, incluyendo las comunicaciones telefónicas. Establece que cualquier restricción debe estar prevista en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad

1980 - Directrices de la OCDE que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales

Fue un intento pionero por establecer principios para el uso de información digital, incluyendo la limitación de recogida, calidad de los datos, especificación de los fines, limitación de uso, salvaguarda de la seguridad, transparencia, participación individual y responsabilidad, reconociendo la privacidad como un derecho

1981 - Convenio 108 del Consejo de Europa (México es Estado parte)

Delinea principios como el consentimiento informado y la prohibición de discriminación en el tratamiento de datos, clave para la protección de las personas migrantes.

1990 - Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y sus Familiares (Artículo 14)

Establece que ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones

2002 - Informe sobre Terrorismo y Derechos Humanos (Comisión Interamericana de Derechos Humanos - CIDH)

Reconoció el papel vital del hábeas data para las víctimas de violaciones graves, permitiéndoles acceder a información gubernamental, exigir responsabilidades, y corregir, eliminar o actualizar datos sensibles, incluso cuando están en manos de entidades privadas.

2013 - Resolución 68/167 de la ONU

Reafirmó que los derechos humanos offline deben protegerse también en el ámbito digital y exigió a los Estados revisar sus prácticas de vigilancia.

2013 - Informe sobre Libertad de Expresión en Internet (Relatoría Especial para la Libertad de Expresión - CIDH)

Destaca que la libertad de expresión en internet depende de la protección de la privacidad, el anonimato y la ciberseguridad, especialmente para personas en contextos de persecución. Rechaza la Doctrina de Seguridad Nacional como justificación para el espionaje y resalta el derecho al hábeas data. Afirma que la vigilancia estatal debe estar limitada por legalidad, necesidad y proporcionalidad, y siempre bajo control judicial.

2014 - Informe de la OACNUDH: El derecho a la privacidad en la era digital (ONU)

Advierte que las tecnologías de vigilancia amenazan la dignidad humana. Subraya la necesidad de que la vigilancia se alinee con los principios de legalidad, proporcionalidad y no discriminación, evitando interferencias arbitrarias. Este informe sentó las bases para estándares globales e influyó en normativas como el GDPR, enfatizando el equilibrio entre seguridad y derechos humanos y la urgencia de salvaguardias efectivas. Exige a los Estados revisar sus leyes y establecer salvaguardias eficaces contra los abusos

Marco regulatorio en México

Constitución Política de los Estados Unidos Mexicanos

El Artículo 6o. funge como fundamento jurídico para la transparencia y el control civil sobre las actividades de vigilancia, incluyendo el acceso a la información sobre tecnologías, propósitos e impactos, bajo el principio de máxima publicidad

El Artículo 16, segundo párrafo, reconoce expresamente el derecho a la protección de datos personales, al acceso, rectificación y cancelación de los mismos, así como a la

oposición (conocidos como Derechos ARCO). Este artículo exige una orden judicial para cualquier uso indebido, acceso no autorizado o intervención de datos, afirmando la dignidad y autonomía informativa de cada individuo.

2025 Iniciativas de ley recién reformadas o en proceso de reforma, en el marco de la Estrategia Nacional de Seguridad Pública 2024-2030

Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)

Su fin es garantizar el derecho humano al acceso a la información pública y promover la transparencia y rendición de cuentas, estableciendo la obligación de las autoridades de publicar información sobre las solicitudes o acciones de vigilancia. **Desaparición del INAI.** *Esta reforma reconfigura el sistema de transparencia al desaparecer el INAI y sustituirlo por la Secretaría Anticorrupción y Buen Gobierno.*

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Consagra el conjunto esencial de facultades para que toda persona pueda proteger su información personal, conocidos como Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), garantizando su dignidad frente al tratamiento de sus datos.

Ley Federal de Protección de Datos en Posesión de los Particulares

Complementa la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, incorporando figuras como el aviso de privacidad y una noción más específica sobre el consentimiento.

Ley General en Materia de Desaparición Forzada de Personas, Sistema Nacional de Búsqueda de Personas y Ley de Población

Busca vincular el CURP con un sistema biométrico para una Plataforma Única de Identidad nacional, lo que implicaría la construcción de una base de datos centralizada con información altamente sensible, generando riesgos para la seguridad y privacidad si no se respetan los principios de proporcionalidad

Ley en Materia de Telecomunicaciones y Radiodifusión

Mantiene la identificación obligatoria de usuarios y la obligación de las operadoras de retener metadatos (geolocalización, contactos, horarios) por dos años, permitiendo el acceso a autoridades sin orden judicial y el rastreo en tiempo real. Faculta a instancias de seguridad para bloquear o anular señales.

Ley de la Guardia Nacional

Legaliza un modelo de vigilancia masiva sin controles judiciales efectivos, eliminando el requisito de autorización judicial para consultar datos conservados de comunicaciones y geolocalización en tiempo real. Reactiva facultades que la Suprema Corte había declarado inconstitucionales, como las operaciones encubiertas sin autorización judicial.

Ley de Seguridad Pública

Estas leyes buscan consolidar un sistema centralizado de vigilancia sin contrapesos, planteando la interconexión de bases de datos nacionales e internacionales, tanto públicas como privadas, sin los controles necesarios, lo que expone gravemente la privacidad de las personas.

Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública

Crea una Plataforma Central de Inteligencia operada por el Centro Nacional de Inteligencia (CNI), la cual permite la interconexión y acceso a una amplia gama de datos públicos y privados (patrimonial, fiscal, financiera, registral, comercial, de comunicaciones, biométricos, vehiculares y de salud), obligando a particulares que manejan bases de datos a suministrar información.