PUEDJS
PROGRAMA UNIVERSITARIO DE ESTUDIOS SOBRE DEMOCRACIA, JUSTICIA Y SOCIEDAD

475+ UNIVERSIDAD de MÉXICO 1551 2026

#LEY OLIMPIA
defensoras digitales

BMA 100 AÑOS
BARRA MEXICANA COLEGIO DE ABOGADOS

ESTUDIO TÉCNICO

REVISIÓN DEL CAPÍTULO 19 DEL T-MEC SOBRE COMERCIO DIGITAL

Análisis crítico y propuestas de modificación
a los Artículos 19.12, 19.16 y 19.17 desde la perspectiva
de los derechos digitales

JUNIO, 2026

PUEDJS.UNAM.MX

Revisión del Capítulo 19 del T-MEC sobre Comercio Digital.

Análisis crítico y propuestas de modificación a los Artículos 19.12, 19.16 y 19.17 desde la perspectiva de los derechos digitales.

El presente estudio técnico fue elaborado por el Programa Universitario de Estudios sobre Democracia, Justicia y Sociedad (PUEDJS) de la Universidad Nacional Autónoma de México (UNAM), a través de su laboratorio digital, Tlatelolco Lab, en conjunto con el Movimiento Ley Olimpia, que conforma la Red Latinoamericana de Defensoras Digitales, Bufete Quijano y la Barra Mexicana, Colegio de Abogados, A.C. (BMA).

Primera edición, junio de 2026.

Programa Universitario de Estudios sobre Democracia, Justicia y Sociedad (PUEDJS).
Torre UNAM, Tlatelolco-Piso 13.
Ricardo Flores Magón 1, Colonia Nonoalco Tlatelolco, Alcaldía Cuauhtémoc, Código Postal, 06995, Ciudad de México.

Cómo citar:

Ackerman, J.M. y Neubauer, D.E. (coords.). (2026). *Revisión del Capítulo 19 del T-MEC sobre Comercio Digital. Análisis crítico y propuestas de modificación a los Artículos* 19.12, 19.16 y 19.17 desde la perspectiva de los derechos digitales. PUEDJS-UNAM, México, 55 páginas.

Contacto: contacto.puedjs@gmail.com
www.puedjs.unam.mx

Coordinación

John M. Ackerman
Dardo Emanuel Neubauer
PUEDJS-UNAM

Colaboradoras(es)

Olimpia Coral Melo
Marcela Hernández Oropa
Red Latinoamericana de Defensoras Digitales - Ley Olimpia

Carmen Quijano Decanini
Marina Campllonch Pollo
Bufete Quijano

Jesús Ricardo Miranda Medina
Eloy Caloca Lafont
PUEDJS-UNAM

Diseño e ilustración

Karen Ivonne Tarango Torres
Fernanda Galeana Berber
Jesús Gerardo Espinosa Reyes
PUEDJS-UNAM

Índice

Antecedentes de la iniciativa

Este análisis crítico surge de la confluencia entre el activismo, la academia y el foro jurídico, sostenido por la idea de que los mercados, el capital y la industria tienen la obligación de respetar los derechos humanos, razón por la cual los tratados comerciales deben erigirse como instrumentos de protección de las personas y sus libertades frente al poder de las empresas.

Desde 2018, el ***Movimiento Ley Olimpia***, que conforma la **Red Latinoamericana de Defensoras Digitales**, ha señalado la ineludible responsabilidad de los grandes corporativos tecnológicos, sus modelos de negocios, sus algoritmos y sus plataformas digitales en la problemática de la violencia digital contra las mujeres. A partir de 2023, estas organizaciones han impulsado, en diversos foros internacionales, propuestas para que los Estados firmen tratados o acuerdos internacionales multilaterales en los que se establezcan marcos regulatorios para las empresas, con el objetivo de garantizar la prevención, atención, investigación y sanción de todo tipo de violencia, en tanto que vulnera derechos humanos y pone en peligro los sistemas democráticos.

Tlatelolco Lab, laboratorio digital para la democracia del **Programa Universitario de Estudios sobre Democracia, Justicia y Sociedad (PUEDJS)** de la **Universidad Nacional Autónoma de México (UNAM)**, trabaja desde 2021 para articular diferentes perspectivas teóricas, metodologías y herramientas, a favor de la democracia en redes sociodigitales y de la protección de las y los usuarios, proponiendo la construcción de rutas críticas para generar contextos más plurales y transparentes en la Red, y empoderar la participación ciudadana (Ackerman y Escamilla, 2023). Con este propósito, el laboratorio ha publicado el *Decálogo de Derechos Digitales en Redes Sociales* (Ackerman, Atilano, Aguilar, Ardissom et al., 2023) e impulsado una serie de iniciativas de reforma para la regulación de los entornos y servicios digitales en México, además de coordinar una **Clínica de Litigio Estratégico** para brindar asesoría, respaldo y seguimiento en casos de violaciones de la integridad o seguridad personal, por parte de plataformas y empresas tecnológicas (Ackerman, Ardissom, Miranda y Neubauer, 2026).

Por su parte, las abogadas Carmen Quijano y Marina Campllonch, de **Bufete Quijano**, se han posicionado públicamente desde 2021 en diversos espacios, así como en el libro *Derecho a la Privacidad en Internet* (Quijano, 2022) sobre la responsabilidad que deben asumir las plataformas tecnológicas en la rendición de cuentas, la protección de las garantías

constitucionales y los datos personales en el espacio digital. Recientemente, han sumado esfuerzos con la **Barra Mexicana, Colegio de Abogados, A.C**. en la salvaguarda de los derechos fundamentales en Internet.

La alianza entre el PUEDJS-UNAM (por medio de Tlatelolco Lab), Defensoras Digitales y la Barra Mexicana, Colegio de Abogados, A.C., nace en 2026 para defender los derechos de las personas frente a los intereses corporativos de mercado en el marco de la revisión del Tratado entre México, Estados Unidos y Canadá (T-MEC), considerando, sobre todo, el Capítulo 19 de dicho acuerdo regional, correspondiente al "Comercio Digital".

Resumen Ejecutivo

El presente estudio técnico analiza los artículos 19.12, 19.16 y 19.17 del Capítulo 19 sobre "Comercio Digital" del Tratado entre México, Estados Unidos y Canadá (T-MEC), de cara a la Revisión Conjunta por sus gobiernos firmantes, prevista para 2026. Tras un análisis crítico de las omisiones y restricciones de cada artículo, el estudio sugiere introducir ciertas modificaciones, a favor de la protección de las y los usuarios de Internet, y hace un llamado a ampliar los espacios de consulta pública y renegociación del Tratado para aumentar la participación directa de la ciudadanía a través de organizaciones civiles, investigadoras e investigadores académicos, personas expertas de todo tipo y representantes de los intereses colectivos. El argumento central es que el Capítulo 19 del T-MEC otorga inmunidad a las plataformas y defiende sus intereses comerciales por encima de los derechos de las personas usuarias, lo cual va en detrimento del acceso inmediato a la justicia en caso de violencia, la no discriminación algorítmica, y una vida libre de agresiones en entornos digitales.

Por lo anterior, las modificaciones que aquí se proponen parten de que las medidas del T-MEC se supeditan, ante todo, a marcos regulatorios estadounidenses y a leyes que corresponden a modelos obsoletos de diseño web (como la Sección 230 de la *Communications Decency Act*), por lo que desprotegen a la o el usuario digital a través de: a) la falta de una disposición expresa que indique o reitere que las empresas propietarias y gestoras de las plataformas tecnológicas se sometan a la jurisdicción de aquellos países en los que hacen negocios y donde residen sus consumidores, creadores de contenido, representantes e inversionistas; b) la dificultad para que las instituciones de impartición de justicia de diferentes Estados soliciten y accedan ágilmente a materiales multimedia o bases de datos que puedan servir como evidencia para perseguir delitos y salvaguardar a víctimas de violencia; y c) que el

acuerdo comercial deslinda a las plataformas de responsabilidad por los contenidos que se exhiben y circulan en sus interfaces, señalando que estas publicaciones reflejan las ideas de terceros, y minimizando el papel que juegan los efectos de la tecnología en la vida de las personas, a través de algoritmos y pautas publicitarias que promueven y amplifican discursos de actores o grupos antagónicos a la pluralidad, el diálogo y el bienestar común.

Con el fin de hacer valer que se respeten los **derechos digitales**, compartimos las siguientes propuestas de modificación a aquellos artículos que ponen en riesgo a la o el usuario:

Artículo 19.12: Jurisdicción de las plataformas

Problema: El T-MEC establece que los países no pueden obligar a las empresas digitales a establecer instalaciones informáticas en los territorios donde ofrecen sus servicios o hacen negocios, y tampoco establece la posibilidad para que los gobiernos tengan acceso a datos alojados en *data centers* privados, incluyendo aquellos que son útiles o necesarios en casos de violaciones a normas de orden público. Esto: a) inhibe la rendición de cuentas de las plataformas, al no obligarlas a respetar las leyes de orden público de los diferentes países donde extraen y almacenan información, o donde obtienen ganancias por venta de publicidad; b) supone dificultades para que las y los ciudadanos mexicanos puedan proteger su propia información; y c) obstaculiza que las instituciones judiciales de nuestro país puedan solicitar auditorías especiales a las empresas para revisar información útil para la procuración de justicia, agilizar los debidos procesos, resguardar los derechos humanos y combatir la violencia digital.

Propuesta: Que cada corporación se sujete a la legislación y jurisdicción de cada país donde opera, respecto de controversias derivadas de violaciones a normas de orden público y protección de derechos fundamentales. De igual forma, se solicita obligar a las plataformas a atender requisitos de solicitud de información y atención a las y los ciudadanos de los territorios donde operan, cuando estas peticiones sirvan para: a) proteger datos personales sensibles, conforme a la legislación nacional; b) garantizar el acceso oportuno y efectivo de las autoridades nacionales competentes a evidencia digital en investigaciones penales, particularmente en casos de violencia contra las mujeres y niñas, explotación sexual y trata de personas; c) proteger datos relativos a la seguridad nacional o a infraestructuras críticas; y d) proteger derechos humanos y cumplir obligaciones internacionales en esa materia.

Artículo 19.16: Acceso a información

Problema: No existen, ni en el T-MEC ni en otros instrumentos regionales, políticas claras de rendición de cuentas que lleven a las plataformas a transparentar sus códigos ni algoritmos, pero tampoco a explicar, de mínimo, cómo funcionan sus esquemas de capitalización de contenidos y datos, sus políticas de moderación de publicaciones, ni las operaciones de sus mecanismos de obtención y analítica de información. Lo que es evidente, como antes hemos establecido, es que abundan los sesgos discriminatorios, las violencias y la desinformación en las plataformas, sin que exista la capacidad de combatir estas agravantes desde el propio diseño tecnológico.

Propuesta: Políticas claras y expeditas para el acceso a códigos fuente o, al menos, a informes claros del funcionamiento de diseños técnicos y algoritmos por parte de las empresas, con el fin de darle obligatoriedad a que las plataformas rindan cuentas ante instituciones públicas. Así, consideramos que se pueden hacer solicitudes de información en los siguientes supuestos: a) investigaciones, inspecciones, exámenes, acciones de cumplimiento o procedimientos judiciales específicos; b) verificaciones al cumplimiento de normas aplicables en los Estados del T-MEC para la protección de las ciudadanías o el cumplimiento de normas de orden público; c) prevención y protección de derechos humanos; d) rendición de cuentas sobre las afectaciones a derechos; y e) verificaciones de cumplimiento de obligaciones de transparencia algorítmica.

Artículo 19.17: Responsabilidades de las plataformas sobre contenido sensible

Problema: Las plataformas están protegidas de toda responsabilidad legal por el contenido generado por usuarias o usuarios, siempre que cada plataforma no haya creado ni modificado dicho contenido. Como antes hemos indicado, este esquema coloca a las empresas tecnológicas en una posición de inmunidad genérica y las exime de responsabilizarse por su intervención en la distribución, amplificación y posible censura o invisibilización de contenidos, así como por los efectos que genera la falta de salvaguardas para los derechos humanos en el diseño y comercialización de las tecnologías que se ofrecen a las y los usuarios.

Propuesta: Solicitamos que, si bien se reconozca el papel y las prerrogativas de los servicios informáticos en la economía digital, así como la libertad de expresión,

se equilibren los intereses corporativos con la protección efectiva de los derechos humanos. Buscamos que las plataformas pasen de un modelo de inmunidad genérica a un modelo de inmunidad condicionada, con obligaciones y responsabilidades vinculantes, en línea con los desarrollos jurídicos más recientes.

Las tres propuestas de modificación a los artículos antes señaladas han sido evaluadas con base en cinco criterios de análisis:

- ***Jurídico-constitucional:*** Verifica si la propuesta incorpora salvaguardas convencionales para que México pueda cumplir sus obligaciones constitucionales y responda a las convenciones e instrumentos internacionales de derechos humanos.
- ***Técnico-computacional:*** Evidencia la viabilidad tecnológica para implementar los cambios propuestos.
- ***Académico:*** Permite sostener la modificación de los artículos propuestos con respaldo en la literatura académica desarrollada a lo largo de años de investigación.
- ***Político:*** Revisa si la propuesta se enmarca en debates políticos vigentes, no sólo en México, sino en el mundo entero, en torno al respeto y salvaguarda de los derechos digitales.

  Económico: Criterio que busca derribar el mito de que la implementación de las propuestas tendrían costos excesivos para las plataformas.

La revisión del T-MEC en 2026 es el momento político, jurídico y técnico para corregir una arquitectura que subordina derechos fundamentales a intereses corporativos. México llega a esta negociación con instrumentos normativos progresivos (Ley Olimpia, Ley General de Protección de Datos, jurisprudencia constitucional), con el respaldo de la sociedad civil, y con el contexto regulatorio internacional más favorable desde la firma del Tratado. Así, las modificaciones que aquí proponemos no buscan obstaculizar el comercio digital, sino garantizar que sus reglas sean compatibles con el Estado de derecho, con el derecho internacional en materia de derechos fundamentales, y con el interés de las personas que utilizan los entornos digitales de Norteamérica.

Introducción

El presente documento tiene como propósito analizar el Capítulo 19, Comercio Digital, del Tratado entre México, Estados Unidos y Canadá (T-MEC) para proponer, de cara a la Revisión Conjunta del propio T-MEC, prevista para 2026, una serie de modificaciones específicas a los artículos: a) 19.12, sobre la libre circulación de información en Norteamérica; b) 19.16, sobre el acceso al código fuente de los algoritmos de tecnologías digitales; y c) 19.17, sobre la responsabilidad de las plataformas corporativas de Internet, con la finalidad de establecer un marco integral de protección de los derechos de las personas en redes sociodigitales. Los artículos antes mencionados construyen una arquitectura jurídica que protege los intereses de las grandes plataformas y empresas tecnológicas por encima de la seguridad y bienestar de la ciudadanía, lo cual hoy somete a México a adoptar esquemas regionales que le impiden aplicar con plena eficacia instrumentos de su propia legislación como la Ley Olimpia, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y determinados criterios de la Suprema Corte de Justicia de la Nación en materia de derechos digitales que se han limitado a casos concretos y no han logrado extenderse a la sociedad en general.

El problema central es que el T-MEC subordina el ejercicio de derechos fundamentales —como el derecho a una vida libre de violencia digital, el derecho a la privacidad y a la protección de datos personales, el derecho a la no discriminación algorítmica y el derecho de acceso a la justicia— a la libre circulación transfronteriza de contenidos y datos y a la inmunidad de las plataformas. No se establecen principios y criterios de ponderación para resolver la colisión entre esos derechos y tampoco reglas claras sobre los casos de excepción en los que las autoridades judiciales deben tener acceso a información privada por razones de orden público. Frente a ello, este documento propone tres modificaciones sustantivas al Capítulo 19. La primera, implica que el T-MEC establezca normas claras y operativas de protección de derechos humanos que no puedan ser desplazadas por obligaciones comerciales. La segunda, que las autoridades nacionales tengan facultades reales de auditoría algorítmica sobre los sistemas que realizan análisis automatizados de datos y toman decisiones que afectan los derechos humanos de las personas. Y la tercera, que las plataformas digitales asuman responsabilidades jurídicamente vinculantes cuando incumplan la ley, tal como ya lo establecen en la Unión Europea, el Reglamento Europeo de Servicios Digitales, la Ley de Inteligencia Artificial, la *Online Safety Act* del Reino Unido, y el Reglamento General de Protección de Datos (RGPD).

Por lo anterior, se presentan, a continuación, las propuestas de modificación antes descritas, a través de cinco apartados. El primero sitúa la revisión del T-MEC en su contexto político y jurídico. El segundo, expone el marco analítico desde el que se evalúa el Capítulo 19. Y los tres siguientes analizan, uno a uno, los artículos cuya modificación se propone (19.12, 19.16 y 19.17), explicando sus consecuencias actuales y concretas sobre los derechos digitales, y exponiendo las propuestas de reforma. Finalmente, el documento cierra con una visión integradora sobre las modificaciones y un conjunto de conclusiones.

I. Contexto: la revisión del T-MEC 2026 y los derechos digitales

1.1. La cláusula de revisión y la ventana de oportunidad

El artículo 34.7 del T-MEC establece que el Tratado tendrá una vigencia inicial de dieciséis años a partir del 1 de julio de 2020. Para renovarlo, la Comisión de Libre Comercio[1] debe reunirse el 1 de julio de 2026 y confirmar por consenso la voluntad de las tres partes de extenderlo. Si ese consenso no se alcanza, el T-MEC entrará en un ciclo de revisiones anuales durante los diez años siguientes, con posibilidad de renegociación continua hasta 2036. Para México, julio de 2026 es la primera y más importante oportunidad para proponer modificaciones al texto vigente. La Secretaría de Economía abrió en septiembre de 2025 una consulta pública nacional para recoger posiciones de sectores empresariales, academia y sociedad civil, con el propósito de integrar la postura mexicana ante la Comisión. La Oficina del Representante Comercial de Estados Unidos (USTR) inició su propio proceso de consulta el 16 de septiembre de 2025.

Este proceso es un momento de definición, lo que se negocie en 2026 determinará si la defensa de los derechos digitales seguirá supeditada a los intereses empresariales y comerciales en América del Norte, o si, por el contrario, se avanzará por un camino donde se anteponga la protección de la ciudadanía por encima de las tecnologías corporativas tal y como lo ha dictado la Suprema Corte de Justicia de la Nación en diversas sentencias y como lo establecen los Principios Rectores sobre las Empresas y los Derechos Humanos de la ONU.[2] Además, esta etapa de revisión significa para las redes feministas, los colectivos

1 Comisión compuesta por representantes del gobierno de cada Parte a nivel de ministros, o por las personas a quienes estos designen. https://www.gob.mx/t-mec/acciones-y-programas/comision-de-libre-comercio-247174?state=published

2 https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

de activismo digital y las y los investigadores académicos, una ocasión que no se puede desaprovechar para incidir en la arquitectura jurídica que determinará, en última instancia, qué pueden y no pueden hacer los Estados para proteger a sus ciudadanas y ciudadanos en el entorno digital.

1.2. Por qué el Capítulo 19 es el núcleo del problema

Cuando el T-MEC fue firmado, el 30 de noviembre de 2018, su Capítulo 19 era uno de los códigos legales sobre comercio electrónico con medidas más radicales, jamás incluido en un acuerdo comercial suscrito por Estados Unidos, con un entorno digital muy diferente. Sus dieciocho artículos y un anexo codificaron un modelo construido sobre 4 prohibiciones fundamentales: ninguna restricción a la transferencia transfronteriza de datos (artículo 19.11); ningún requisito de que los servidores con los datos de cierta población estén en su territorio nacional (artículo 19.12); ningún acceso obligatorio al código fuente de los algoritmos salvo casos de excepción (artículo 19.16); y ninguna posibilidad de responsabilizar a las plataformas por el contenido publicado por sus usuarios (artículo 19.17).

Estas cuatro prohibiciones, tomadas en conjunto, están basadas en un instrumento internacional vinculante (es decir, que crea obligaciones jurídicas conjuntas entre países): el modelo regulatorio del derecho digital estadounidense —específicamente, el de la Sección 230 de la *Communications Decency Act* de 1996[3]—, que ahora también se ha impuesto como piso obligatorio para México y Canadá. La consecuencia directa de este diseño es que cualquier reforma legislativa nacional que contradiga ese modelo puede ser impugnada como violatoria del Tratado y activar mecanismos de controversia entre Estados.

Para los derechos de la ciudadanía, esta arquitectura produce tres consecuencias que es necesario nombrar. El Capítulo 19 reduce drásticamente el margen del Estado mexicano para legislar en materia de derechos fundamentales, privacidad, protección de datos, gobernanza algorítmica y responsabilidad de plataformas. Limita la capacidad de México para cumplir sus obligaciones nacionales de derechos humanos, particularmente con los artículos 1, 4°, 6°, 16 y 17 de su Constitución Política[4], así como obligaciones internacionales

3 La Sección 230 de la *Communications Decency Act* (CDA) establece que las plataformas no deben ser tratadas como editoras o autoras legales del contenido publicado por sus usuarios. Su esencia es otorgar inmunidad civil a los intermediarios digitales por contenidos de terceros, permitiéndoles además moderar de buena fe sin asumir responsabilidad editorial plena.

4 El artículo 1° de la Constitución Mexicana garantiza los derechos fundamentales de toda y todo ciudadano; el 4° señala la igualdad jurídica entre varones y mujeres; el 6° faculta a las y los mexicanos con libertad de expresión, derecho de réplica y derecho a la información pública; el 16 prohíbe que toda persona sea molestada injustificadamente en su persona, familia, domicilio, propiedades o papeles; y el 17 indica que la o el mexicano puede tiene el derecho de acceder a la justicia de manera pronta, completa e imparcial, impartida por tribunales.

que lo conducen a responder de forma efectiva frente a la violencia contra las mujeres y niñas en línea, derivada de la adopción de los acuerdos de la Convención de Belém do Pará[5] y de la jurisprudencia de la Corte Interamericana de Derechos Humanos (CIDH). Esto no solo deja a los ciudadanos mexicanos en estado de indefensión respecto a sus derechos humanos, sino que coloca a México en una situación de desventaja estructural frente a los modelos regulatorios más avanzados del mundo —especialmente el europeo[6]—, que en los últimos cinco años han apostado precisamente por una lógica basada en esquemas legales de rendición de cuentas y responsabilidad para las plataformas en casos de orden público, transparencia algorítmica y regulación activa del entorno digital.

Más que ser un obstáculo técnico, el T-MEC es el marco que determina lo que México puede hacer para proteger a sus ciudadanos en el entorno digital. Modificar el Capítulo 19 es una condición necesaria para la salvaguarda de los derechos digitales en México, a través de un marco legal que no esté atado de manos a un pacto comercial.

II. Marco analítico: criterios para evaluar el Capítulo 19

Este documento adopta un marco analítico común, aplicable a tres artículos que, según se mencionó antes, concentran prohibiciones estructurales que van en demérito de los derechos digitales: el 19.12, 19.16 y 19.17. Cada disposición se evalúa a partir de cinco criterios:

- **Criterio jurídico-constitucional:** compatibilidad con la Constitución Política de los Estados Unidos Mexicanos (artículos 1°, 4°, 6°, 16 y 17), con el bloque de constitucionalidad en materia de derechos humanos (artículo 1° constitucional y tratados internacionales), con la legislación secundaria vigente, particularmente la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como con fallos y sentencias de la Suprema Corte de Justicia de la Nación (SCJN) en materia de salvaguarda de los derechos humanos. También se abordan jurisprudencias y marcos regulatorios internacionales.

5 La Convención de Belém do Pará, adoptada en 1994 en Brasil, es el primer tratado internacional vinculante del sistema interamericano para prevenir, sancionar y erradicar la violencia contra la mujer.

6 El marco europeo comprende, entre otros instrumentos, el Reglamento Europeo de Servicios Digitales, la Ley de Inteligencia Artificial de la Unión Europea, la Online Safety Act del Reino Unido y el Reglamento General de Protección de Datos (RGPD).

- **Criterio técnico-computacional:** consistencia entre el texto del T-MEC y el funcionamiento real de las arquitecturas computacionales contemporáneas (computación distribuida, sistemas de aprendizaje automático, procesamientos de lenguaje natural, plataformas multilaterales)[7].

- **Criterio académico:** coherencia con la literatura científica revisada por pares en materia de gobernanza algorítmica, responsabilidad de intermediarios y soberanía de datos, así como con los marcos regulatorios comparados más recientes (Unión Europea, Reino Unido, Brasil y Australia).

- **Criterio político:** viabilidad de la propuesta dentro de las posiciones declaradas de los tres gobiernos y de los actores con poder de veto (Congreso de Estados Unidos, Congreso de la Unión en México, y Parlamento canadiense).

- **Criterio económico:** impacto sobre la innovación, la inversión, la competencia y los costos de cumplimiento, evaluado con evidencia disponible.

III. Artículo 19.12 — Libre flujo de datos y ubicación de instalaciones informáticas

3.1 Texto vigente y alcance

El artículo 19.11 del T-MEC establece que ninguna Parte prohibirá o restringirá la transferencia transfronteriza de información. Sin embargo, el artículo 19.12 dispone que ninguna Parte exigirá a las compañías tecnológicas el uso o la ubicación de instalaciones informáticas en su territorio como condición para realizar negocios en él. La disposición, a diferencia de otras prohibiciones del Capítulo, sólo contempla excepciones generales como las del artículo 19.16 (2), el artículo 32.1 y las aplicables a servicios financieros bajo el Anexo 17-D del Capítulo 17[8].

7 La computación distribuida es la reunión de miles de computadoras, redes y servidores, ubicados en diferentes localizaciones, que se sincronizan para el intercambio, resguardo y análisis de información. Los sistemas de aprendizaje automático y procesamientos de lenguajes (escritos y numéricos) son procesos de machine learning fundamentales para la inteligencia artificial, y las plataformas multilaterales son entornos digitales que permiten el encuentro entre usuarios, anunciantes de publicidad, prestadores de servicios y administradores de cada plataforma, con el fin de que distintas partes moneticen la circulación de contenidos y datos.

8 El Capítulo 32 del T-MEC señala las Excepciones y Disposiciones Generales del Tratado. En el artículo 32.1 se establecen los procedimientos para presentar y solucionar controversias. Asimismo, el Anexo 17-D (Ubicación de las Instalaciones Informáticas) establece que "no se obliga a una Parte a divulgar información relativa a los anuncios financieros o cuentas de clientes individuales de servicios financieros o proveedores transfronterizos de servicios financieros" (en correspondencia con el artículo 17.8), y que esto "no aplica a medidas existentes de Canadá por un año después de la entrada en vigor del Tratado".

En términos directos, esto significa que el T-MEC le prohíbe a México exigir que los datos personales de sus ciudadanos, incluidos aquellos sensibles, biométricos, financieros, de salud, de geolocalización y de comunicaciones, se almacenen o procesen en territorio nacional. Las grandes plataformas digitales operan con centros de datos ubicados predominantemente en Estados Unidos, Irlanda, Singapur y Australia. Según el Capítulo 19 del T-MEC, al tratarse de instalaciones privadas, México enfrenta dificultades para obligar a las compañías a compartir datos contenidos en estos territorios y debe contar con jurisdicción efectiva sobre los datos de sus ciudadanos cuando se produzcan violaciones a derechos fundamentales, de modo que las autoridades competentes puedan obtener evidencia digital en tiempo oportuno, sin depender exclusivamente de mecanismos de cooperación internacional cuya lentitud resulta incompatible con la urgencia de esas violaciones.

3.2 Problemática

3.2.1 Dimensión jurídico-constitucional

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la protección de datos personales como un derecho fundamental autónomo. Así lo establecen, la tesis P. II/2014 (10a.) del Pleno (registro 2005522)[9], el Amparo en Revisión 168/2011[10], y el Amparo Directo en Revisión 1621/2010[11]. Adicionalmente, el Amparo Directo en Revisión 2880/2020[12], resuelto por la Primera Sala el 29 de noviembre de 2023, extendió esa protección a los metadatos asociados a comunicaciones privadas.
Uno de los precedentes más relevantes es la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021, resueltas por el Pleno de la SCJN el 26 de abril de 2022. En estas sentencias se declaró inconstitucional el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT), por considerar que la recolección masiva de datos personales, telefónicos y

9 Esta tesis señala que las y los mexicanos tienen "derecho a la protección de sus datos personales, consistente en el control de cada individuo sobre el acceso y uso de su información personal en aras de preservar la vida privada". https://sjf2.scjn.gob.mx/detalle/tesis/2005522

10 El Amparo en Revisión 168/2011 (Primera Sala, 2011) establece que el derecho a la protección de datos personales es un derecho fundamental autónomo derivado del artículo 16 constitucional, e incluye la facultad de las personas de conocer qué información existe sobre ellas, acceder a ella, rectificarla y cancelarla (derechos ARCO, que es el acrónimo de Acceso, Rectificación, Cancelación y Oposición).
https://odim.juridicas.unam.mx/sites/default/files/Amparo%20en%20revisi%C3%B3n%202011_168%20%28Acceso%20a%20la%20carpeta%20de%20Rosendo%20Radilla.pdf

11 El Amparo Directo en Revisión 1621/2010 (Primera Sala, 2010) consolida la doctrina de que el derecho a la protección de datos personales forma parte del bloque de constitucionalidad mexicano y fue uno de los precedentes clave que permitió a la SCJN desarrollar los estándares de tutela reforzada sobre datos sensibles, biométricos y metadatos de comunicaciones privadas.

12 El Amparo Directo en Revisión 2880/2020 (Primera Sala, 29 de noviembre de 2023, Ministro ponente: A. Gutiérrez Ortiz Mena) extiende la protección constitucional del artículo 16 a los metadatos asociados a comunicaciones privadas, estableciendo que la Corte reconoce como derecho fundamental autónomo no solo los contenidos de las comunicaciones, sino también los datos sobre cuándo, dónde, con quién y desde dónde se realizaron.
https://www.oas.org/ext/Portals/33/Files/TreatiesB/Mex_tratbil_eua_esp_3.pdf

biométricos no era razonable ni necesaria en una sociedad democrática[13]. La Suprema Corte impone ese estándar de protección reforzada del derecho humano a la privacidad y protección de datos personales frente al propio Estado mexicano, el T-MEC no debería impedir que ese mismo Estado adopte medidas proporcionales frente al tratamiento transnacional de datos sensibles por actores privados, particularmente cuando se trata de datos sensibles de mujeres y niñas o cuando esos datos son necesarios para investigar y sancionar la violencia digital de género. Debe mencionarse aquí, también, el Amparo en Revisión 74/2024, resuelto por la Segunda Sala, el 29 de enero de 2025, que validó la geolocalización masiva de usuarios de banca en línea, y que contribuyó a dejar que las empresas extrajeran y utilizaran cierta información personal de sus clientes14. Ese fallo reforzó la vigilancia tecnológica y corporativa, precisamente porque el orden interno mexicano presenta zonas grises que han permitido validar prácticas invasivas por parte de actores privados. Es así que resulta indispensable que el T-MEC contenga salvaguardas convencionales explícitas que protejan los datos de los ciudadanos de los tres países que lo suscriben.

La tensión se profundiza cuando se consideran las obligaciones del Estado mexicano derivadas de la Convención de Belém do Pará. Asimismo, la sentencia de la Corte Interamericana en el caso *Bedoya Lima vs. Colombia*[15] establece estándares de actuación reforzada que, aplicadas al ámbito digital, exigen capacidades institucionales reales para documentar y responder a violencias contemporáneas. La ausencia de jurisdicción efectiva de México sobre los datos de sus ciudadanos tratados en instalaciones ubicadas en el extranjero reduce drásticamente la capacidad de las autoridades mexicanas de obtener evidencia digital en investigaciones por violencia digital, trata de personas y explotación sexual infantil. Las víctimas mexicanas dependen hoy de los Tratados de Asistencia Legal Mutua (MLAT)[16], cuya duración promedio supera con frecuencia los doce meses, mientras que la viralización de contenido sexual íntimo no consentido puede ocurrir en horas, causando un daño irreparable. Esta asimetría procesal es insostenible a la luz de los

13 La denuncia de que el PANAUT era "una violación del derecho de intimidad de las y los ciudadanos", porque permitía acceder a información sensible, incluyendo "características de origen racial y étnico", fue expuesta por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que, entonces, se encontraba en funciones (2002-2025). Sin embargo, esta declaratoria de inconstitucionalidad entró en tensión con la sanción de la Ley General del Sistema Nacional de Seguridad Pública (2025) y la Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (2025).
https://www2.scjn.gob.mx/juridica/engroses/cerrados/Publico/Proyecto/AI82_2021y86_2021acumuladaPL.pdf

14 https://www.scjn.gob.mx/sites/default/files/listas/documento_dos/2025-01/AR%2074.pdf

15 El caso se refiere al reconocimiento de "una serie de alegadas violaciones de derechos humanos" a una periodista, Jineth Bedoya Lima, por parte del Estado colombiano.
https://derechoshumanos.gov.co/Areas-Trabajo/Documents/2017-171221-Sentencia-Caso-BEDOYA-LIMA.pdf

16 Los Tratados de Asistencia Legal Mutua (MLAT) son acuerdos realizados entre países, en el marco de la Organización de Estados Americanos (OEA), para facilitar la cooperación jurídica y penal entre Estados. En los que México se ve involucrado, está obligado a intercambiar pruebas, evidencias y testimonios para la prevención regional de delitos.
https://www.oas.org/ext/Portals/33/Files/TreatiesB/Mex_tratbil_eua_esp_3.pdf

estándares fijados desde el caso *González* y otras (*"Campo Algodonero"*) vs. México[17].

La verificación de esta asimetría procesal exige reconocer que el problema no se agota en la celeridad de los mecanismos de cooperación internacional, sino que se extiende a la ausencia de obligaciones convencionales que impongan a las plataformas tanto la disponibilidad de herramientas tecnológicas para el intercambio urgente de información en casos de violaciones a derechos humanos, como su sometimiento efectivo a la jurisdicción nacional cuando dichas violaciones se produzcan sobre personas que residen en territorio mexicano. El artículo 12 del Código Civil Federal establece que las leyes mexicanas rigen a todas las personas que se encuentren en la República, así como los actos y hechos ocurridos en su territorio, mientras que su artículo 15 dispone que no se aplicará el derecho extranjero cuando las disposiciones de ese ordenamiento resulten contrarias a principios o instituciones fundamentales del orden público mexicano. La protección de los derechos humanos frente a la violencia digital constituye, en el marco del artículo 1° constitucional, una norma de orden público de la más alta jerarquía, lo que convierte al andamiaje jurisdiccional del Código Civil Federal en un sustento doméstico sólido para reclamar la sujeción de las plataformas al ordenamiento nacional.

Esa pretensión encuentra un respaldo adicional en la jurisprudencia constitucional comparada de los propios Estados Unidos. En *International Shoe Co.* v. Washington (326 U.S. 310, 1945), la Suprema Corte estadounidense consagró la doctrina de los "contactos mínimos" con el foro[18] como criterio suficiente para fundar la jurisdicción personal de un Estado sobre una corporación no residente. En *World-Wide Volkswagen Corp. v. Woodson* (444 U.S. 286, 1980), ese tribunal precisó la denominada *Stream of Commerce Rule*, al sostener que un Estado puede ejercer jurisdicción sobre quien introduce deliberadamente sus productos o servicios en la cadena de distribución de ese foro, con razonable anticipación de ser demandado en él. El alcance de ese principio en el entorno digital fue explorado por el Sexto Circuito Federal en *CompuServe, Inc. v. Patterson* (89 F.3d 1257, 1996), donde se determinó que los contactos electrónicos deliberados y repetidos con un foro, incluyendo la transmisión de archivos, la celebración de contratos de distribución digital y la comercialización a través de redes con sede en ese Estado, constituyen contactos suficientemente sustanciales para fundar jurisdicción personal.

Las plataformas que operan en México obtienen ingresos publicitarios generados por

17 La Corte Interamericana de Derechos Humanos (CIDH) condenó a México en 2009 por la responsabilidad e impunidad en la desaparición y asesinato de tres mujeres jóvenes cuyos cuerpos fueron hallados en Ciudad Juárez en 2001. Este fallo estableció un precedente internacional contra la violencia de género y el feminicidio, obligando al Estado a investigar con perspectiva de género y reparar a las familias.
https://www.diputados.gob.mx/sedia/biblio/virtual/centros/CEAMEG/01_Sentencia-Completa.pdf

18 Foro se refiere al término jurídico estadounidense fórum y alude al territorio, jurisdicción o tribunal ante el cual se promueve una acción judicial.

la actividad de usuarios mexicanos, moderan contenidos con efectos jurídicos sobre personas en territorio nacional y almacenan datos de ciudadanas y ciudadanos que son explotados comercialmente, cumplen con creces ese umbral. Se trata de hacer efectiva la jurisdicción mexicana en casos en que la propia lógica del derecho privado internacional norteamericano la autorizaría. Lo que el T-MEC debe incorporar, en consecuencia, es una cláusula convencional explícita que obligue a las plataformas a someter a la jurisdicción de las autoridades competentes de cada Parte las controversias derivadas de violaciones a normas de orden público y a derechos fundamentales, y que las compela a desplegar protocolos de respuesta urgente para el intercambio de información probatoria en investigaciones por violencia digital de género, trata de personas y explotación sexual infantil.

Las cifras confirman la urgencia. De las cerca de 93 millones de personas usuarias de Internet en México, el 64% utiliza servicios privados estadounidenses con almacenamiento en la nube, y el 71% tiene cuentas activas en plataformas sociodigitales con sede en Estados Unidos (Kaspersky, 2026). Esto significa que alrededor de 100.2 millones de mexicanas y mexicanos tienen información alojada en alguno de los 4,100 centros de servidores propiedad de corporaciones estadounidenses. También, el 96% de todos los sitios web en inglés del mundo extraen datos de geolocalización, personales, financieros o de tráfico que se concentran en Estados Unidos (IEEE Spectrum, 2026). Y hay 93 empresas estadounidenses dedicadas exclusivamente a captar y almacenar información para terceros —Amazon Web Services, Data Bank, Digital Realty y Equinix, entre otras— (Mordor Intelligence, 2026). Además, los 166 centros de datos existentes en México son, en su mayoría, propiedad estadounidense (Datacenters.com, 2026). Si se suma que el Departamento de Seguridad Nacional y el Departamento de Estado de Estados Unidos tienen acceso a los centros de datos bajo su jurisdicción (Brennan Center for Justice, 2026), es fundamental que las compañías que traten con datos de mexicanos respondan a la jurisdicción nacional19 y a los criterios internacionales vinculantes en materia de derechos humanos.

El problema se vuelve todavía más urgente al considerar el alcance de la violencia digital de género. Según el Módulo de Ciberacoso (MOCIBA) del INEGI (2026), casi 19 millones de mujeres en México de entre 18 y 30 años han sido víctimas de acoso en Internet, lo que representa el 22% de las internautas mexicanas. Estas víctimas enfrentan tres obstáculos estructurales: la imposibilidad práctica de acceder a historiales y registros eliminados para sustentar denuncias; la nula transparencia sobre dónde se aloja la información sensible o

19 El Amparo en Revisión 767/2023 constituye un precedente relevante en el que la SCJN sostuvo que, para efectos de la competencia territorial del INAI en materia de protección de datos personales, el servicio de un motor de búsqueda prestado por una empresa extranjera puede considerarse materializado en México cuando la información es susceptible de ser consultada desde territorio nacional. La ubicación extranjera de la sede corporativa o de los servidores no excluye, por sí misma, la aplicación de la legislación mexicana.

probatoria; y el hecho de que la violencia contra las mujeres en Internet alimenta industrias que acumulan datos, métricas y transferencias monetarias (Gaceta UNAM, 2025). A esto se añade que el 25% de las personas de entre 12 y 17 años en México —alrededor de 3 millones— ha tenido alguna experiencia de acoso en línea (UNICEF, 2025), y que, a nivel global, las amenazas oscilan entre el 48% y el 60% dependiendo del país, aunque España y Estados Unidos encabezan los índices de ataques a las infancias (Deutsche Welle, 2025). Sin acceso a los datos alojados en servidores extranjeros, la investigación y sanción de estas violencias es, en términos prácticos, imposible.

3.2.2. Dimensión técnico-computacional

El artículo 19.12 opera sobre una representación obsoleta de la computación distribuida: la idea de que los datos residen en un único lugar geográfico, estable y jurídicamente identificable. La realidad actual es distinta. Los sistemas modernos funcionan mediante replicación geográfica de bases de datos, fragmentación (*sharding*), redes de distribución de contenido (CDN) y arquitecturas accesibles "en la nube". La replicación geográfica supone que una misma base de datos, o partes de ella, puede copiarse y sincronizarse en servidores ubicados en distintas regiones o jurisdicciones, con fines de disponibilidad, resiliencia, reducción de latencia o continuidad operativa. Esta práctica vuelve insuficiente una concepción puramente territorial del dato, pero al mismo tiempo demuestra que la localización regulatoria no tiene por qué entenderse como una exigencia rígida de almacenamiento único dentro de un país. Por el contrario, admite gradaciones técnicas perfectamente viables como la localización del dato primario, espejo local con replicación, residencia obligatoria solo para categorías sensibles, segmentación de datos según riesgo, o exigencia de copias accesibles a la autoridad nacional bajo condiciones estrictas de legalidad y control.

Al no considerar estos aspectos vinculados a la compartición de datos, el artículo 19.12 cierra de antemano el espacio para soluciones técnicas que la doctrina especializada y los reguladores europeos han desarrollado durante años. La disposición técnica toma partido por una arquitectura específica —el modelo *cloud* estadounidense, que concentra datos en pocas infraestructuras físicas y distribuye su tratamiento mediante redes globales de proveedores dominantes (Sunyaev, 2024)— y la convierte en un piso obligatorio para México y Canadá. El problema es también regulatorio y constitucional ya que, al impedir que los Estados exijan formas proporcionadas de residencia, copia local o accesibilidad soberana de los datos, el artículo reduce la capacidad pública de diseñar políticas diferenciadas según la sensibilidad de la información, el sector involucrado y los riesgos asociados a su

tratamiento transfronterizo.

3.2.3. Dimensión académica

La literatura académica ha documentado con creciente precisión la brecha entre los marcos normativos del comercio digital y las capacidades reales de los Estados para responder a vulneraciones de derechos en entornos transfronterizos. Esa brecha es el resultado de una arquitectura regulatoria que privilegia la circulación irrestricta de datos por encima de los mecanismos de acceso que los Estados requieren para investigar y sancionar violencias. Chander y Lê (2015) y Gao (2021) han caracterizado este diseño como una opción que antepone la soberanía de la firma corporativa a la soberanía del Estado y a los derechos del individuo, no solo porque impide la localización de datos, sino porque vacía de contenido operativo la capacidad estatal de obtener evidencia digital en tiempo útil. Incluso los estudios de la Information Technology and Innovation Foundation favorables al libre flujo de datos (Cory y Dascoli, 2021) reconocen que las cláusulas absolutas de no localización han generado tensiones constitucionales en India, Indonesia y Brasil, precisamente porque cierran el espacio para diseñar mecanismos proporcionales de acceso estatal a la información.

El debate académico más relevante para este argumento no es, entonces, el de la soberanía sobre la ubicación física de los servidores, sino el de la accesibilidad jurídicamente garantizada a los datos cuando están en juego derechos fundamentales. Kuner (2013) y De Hert y Papakonstantinou (2016) han demostrado que los regímenes de protección de datos más robustos no exigen necesariamente la residencia de los datos en el territorio nacional, sino la existencia de obligaciones de cooperación rápida y mecanismos de acceso condicionado que preserven la capacidad del Estado de actuar ante emergencias de derechos. Este modelo, que la doctrina denomina de adecuación condicional, es precisamente el que el RGPD europeo consagra ya que no impone la localización absoluta, sino estándares de equivalencia y protocolos de acceso que permiten a las autoridades competentes obtener información sin depender de canales de cooperación cuya lentitud es, en sí misma, una forma de denegación de justicia.

Esa asimetría temporal es el núcleo del problema académicamente documentado. Kuner (2013), Greenleaf (2014) y Aaronson y Leblond (2018) coinciden en que los marcos de libre flujo sin condicionalidades no solo desplazan geográficamente los datos, sino que desplazan con ellos la capacidad de los Estados para actuar sobre los efectos que esos datos producen en sus propias ciudadanas y ciudadanos. En el contexto específico de la violencia

digital de género, los trabajos de Gurumurthy y Chami (2022) han mostrado que esa asimetría opera de forma particularmente aguda sobre mujeres y niñas en jurisdicciones del Sur Global porque la viralización de contenido íntimo no consentido, el acoso sistemático y la explotación sexual en línea generan daños en tiempo real, mientras que los mecanismos de cooperación disponibles operan en tiempos institucionales incompatibles con la urgencia de esas violencias. Lo que Mejias y Couldry (2024) denominan colonialismo de datos adquiere así una dimensión adicional que no solo es extractiva en términos económicos, sino también estructuralmente protectora de la impunidad, en la medida en que la arquitectura del libre flujo irrestricto funciona como un escudo procesal para quienes cometen violaciones de derechos a través de plataformas radicadas en otras jurisdicciones.

Un estudio del Tlatelolco Lab del PUEDJS-UNAM (Caloca y Ramírez, 2023) refuerza este diagnóstico al documentar que el extractivismo informático que caracteriza el modelo de las grandes plataformas no es una práctica opaca y vertical, sino una cadena de actores empresas de contenido, vendedores de publicidad y agentes de monetización de tendencias que operan de forma distribuida y coordinada. Esa distribución del procesamiento de datos no elimina la responsabilidad jurídica de las plataformas sobre los efectos que producen en las personas usuarias, la refuerza, en la medida en que el beneficio económico de esa cadena se acumula sobre la base de datos generados en México por personas mexicanas. La literatura revisada converge en que el acceso estatal oportuno a esos datos, cuando están en juego derechos humanos, no es una restricción al comercio digital, sino una condición de legitimidad del sistema regulatorio que lo sustenta.

3.2.4. Dimensión política

Cuando los datos personales y los metadatos de comunicaciones de personas en territorio mexicano son tratados, almacenados y procesados en jurisdicciones extranjeras, cuya legislación faculta a autoridades de seguridad nacional a acceder a ellos sin orden judicial mexicana, como ocurre bajo la *Cloud Act* estadounidense o la *Foreign Intelligence Surveillance Act*[20], el control efectivo del titular y la garantía de autorización judicial federal que exige la Suprema Corte quedan operativamente vaciados y hacen nugatorio el derecho a la vida privada y a la autodeterminación informativa previstos en los tratados internacionales de derechos humanos. El problema radica en la ausencia de mecanismos convencionales que

20 La *Cloud Act* es la Ley de Aclaración del Uso Legal de Datos en el Extranjero, aprobada por Estados Unidos en 2018. Obliga a los proveedores de servicios informáticos a entregar a las autoridades de ese país, los datos almacenados dentro y fuera de la Unión Americana. https://www.justice.gov/criminal/cloud-act-resources
Por otro lado, la *Foreign Intelligence Surveillance Act* faculta al gobierno estadounidense para vigilar la información de sus telecomunicaciones, con el fin de guardar fuentes para fines de Inteligencia.
https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286

obliguen a las plataformas a responder de forma inmediata y verificable ante las autoridades mexicanas competentes cuando se producen vulneraciones a derechos fundamentales. Se trata de garantizar que las plataformas que manejen datos de personas mexicanas cuenten con capacidad institucional real y localizada para atender solicitudes de información urgentes. Esa capacidad puede instrumentarse, de forma proporcional y compatible con los marcos vigentes, mediante la obligación de mantener una representación local con facultades efectivas de respuesta, lo que es consistente con el Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo de Modernización, instrumentos que establecen la obligación de designar representantes en el territorio de las partes cuando se tratan datos de sus ciudadanos y que son vinculantes para México en virtud de su adhesión.

Ese modelo no es ajeno a los marcos normativos de los propios socios del T-MEC. El *Data Privacy Framework* entre Estados Unidos y la Unión Europea, conocido como P*rivacy Shield 2.0*, establece protocolos de transferencia legal de datos que admiten el acceso a información ante peticiones de tribunales u organismos de seguridad, lo que demuestra que la apertura de canales de acceso estatal a datos en poder de corporaciones privadas es compatible con el ordenamiento estadounidense cuando existe un marco normativo que lo exige. En el caso canadiense, la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA) regula las condiciones bajo las cuales las empresas recopilan, usan y divulgan datos personales, y contempla supuestos de divulgación ante autoridades públicas en casos de interés público. Ambos marcos demuestran que la exigencia de acceso estatal oportuno a datos en manos de actores privados no constituye una restricción al comercio digital, sino una condición operativa reconocida por los propios ordenamientos de las Partes del Tratado. Lo que el T-MEC debe incorporar es la obligación de que esa capacidad de respuesta exista, sea verificable y opere en tiempos compatibles con la urgencia que caracteriza a las vulneraciones de derechos en entornos digitales.

3.2.5. Dimensión económica

La experiencia europea ofrece la evidencia empírica más sólida para evaluar los efectos de los regímenes de condicionalidad sobre transferencias internacionales de datos. El Reglamento General de Protección de Datos de la Unión Europea no impone localización absoluta de datos ni exige que las corporaciones extranjeras trasladen su infraestructura al territorio de los Estados miembros. Lo que establece son condiciones de equivalencia para la transferencia internacional y obligaciones de acceso verificable por parte de las autoridades competentes cuando están en juego los derechos de las personas titulares. Esa

distinción es fundamental porque el modelo europeo demuestra que es posible garantizar el acceso estatal oportuno a datos sin imponer la residencia física de los servidores, lo que convierte al RGPD en el referente más directo para el tipo de reforma que este documento propone al artículo 19.12 del T-MEC. Significativamente, ese estándar no es exclusivo del ordenamiento europeo. California, Colorado, Virginia y Connecticut, entre otros estados de la Unión Americana, han adoptado leyes de protección de datos personales que replican los criterios sustantivos del RGPD, incluyendo obligaciones de respuesta ante solicitudes de acceso, rectificación y supresión, así como deberes de transparencia sobre el tratamiento de datos sensibles. La convergencia regulatoria entre la Unión Europea y segmentos significativos del propio ordenamiento estadounidense evidencia que los estándares de condicionalidad que México requiere no son ajenos a sus socios del T-MEC, sino expresión de una tendencia normativa en curso dentro de sus propias jurisdicciones.

Este diseño no ha impedido el crecimiento de la economía digital en Europa ni ha desincentivado la inversión extranjera en infraestructura regional. Microsoft, Amazon Web Services y Google han construido regiones *cloud* específicas para la Unión Europea en respuesta directa a ese marco regulatorio, lo que demuestra que las obligaciones de condicionalidad y acceso pueden funcionar como incentivo para el desarrollo de capacidades locales de respuesta institucional, sin que ello implique una carga desproporcionada sobre las corporaciones. Esa arquitectura fue validada por el Tribunal de Justicia de la Unión Europea en el caso *Schrems II* (C-311/18, 16 de julio de 2020), que confirmó la facultad de los Estados para condicionar las transferencias internacionales de datos a estándares de protección equivalente y que estableció, además, que la mera transferencia de datos personales a una jurisdicción cuya legislación no garantiza una protección equivalente constituye en sí misma una vulneración de los derechos del titular[21].

Los estudios del European Centre for International Political Economy y del ITIF (Bauer et al., 2014; Cory, 2017), frecuentemente citados por la industria tecnológica, estiman pérdidas en los PIB europeos asociadas a requisitos de localización forzosa. Sin embargo, esos estudios modelan un escenario de localización absoluta que no corresponde ni al modelo europeo ni a la propuesta aquí desarrollada, lo que limita sustancialmente su pertinencia como contraargumento. Aaronson y Leblond (2018) y Mishra (2019) han cuestionado esa metodología y demuestran que los costos disminuyen de forma significativa cuando la obligación se circunscribe a categorías específicas de datos sensibles y se acompaña de

21 Según este caso, un particular (Maximilian Schrems) acudió al Data Protection Commissioner de Irlanda para reclamar la transferencia de sus datos personales, por parte de Facebook Ireland a las sedes de la corporación Meta en Estados Unidos.
https://www.icab.es/es/actualidad/noticias/noticia/SENTENCIA-DEL-TRIBUNAL-DE-JUSTICIA-Gran-Sala-de-16-de-julio-de-2020-dictada-en-el-asunto-C-311-18-que-tiene-por-objeto-una-peticion-de-decision-prejudicial-planteada-con-arreglo-al-articulo-267-TFUE-por-la-High-Court-Tribunal-Superior-Irlanda-../

regímenes de transferencia con salvaguardas equivalentes. Ese es exactamente el modelo que la experiencia europea ha demostrado viable, y es el modelo que la propuesta de modificación al artículo 19.12 recoge.

3.3. Propuesta de modificación al artículo 19.12 del T-MEC

El artículo 19.11 no requiere modificación en su principio general de libre flujo de datos. Sin embargo, este queda inoperante sin una modificación urgente del artículo 19.12 para que ese flujo no ocurra a costa de los derechos de las personas y la capacidad de los Estados de investigar y sancionar violencias. Se propone, entonces, la siguiente reformulación:

Texto vigente (esencia)

Ninguna Parte exigirá a una persona cubierta el uso o la ubicación de instalaciones informáticas en territorio de esa Parte como condición para realizar negocios en ese territorio.

Texto propuesto (esencia)

1. Las Partes reconocen el valor del libre flujo transfronterizo de datos para el desarrollo del comercio digital.
2. No obstante lo dispuesto en el párrafo 1, cada Parte podrá adoptar o mantener medidas que establezcan que las personas cubiertas de otra Parte que realicen actividades cuyos efectos se produzcan en su territorio, estarán sujetas a la legislación y jurisdicción de dicha Parte respecto de controversias derivadas de violaciones a normas de orden público o de protección de derechos fundamentales. Las Partes podrán adoptar o mantener requisitos de solicitud de información y atención a los ciudadanos en su territorio cuando sean necesarios para: a) proteger datos personales sensibles conforme a la legislación nacional; b) garantizar el acceso oportuno y efectivo de las autoridades nacionales competentes a evidencia digital en investigaciones penales, particularmente en casos de violencia contra las mujeres y niñas, explotación sexual y trata de personas; (c) proteger datos relativos a la seguridad nacional o a infraestructuras críticas; o d) proteger derechos humanos y cumplir obligaciones internacionales en esa materia.

3. Las medidas adoptadas conforme al párrafo 2 deberán ser proporcionales al objetivo perseguido y no constituirán una restricción encubierta al comercio.

3.4 Sustento integrado de la propuesta

El siguiente cuadro sistematiza los fundamentos de la propuesta de modificación al artículo 19.12 desde sus múltiples dimensiones. Su finalidad es mostrar la convergencia entre los distintos planos de análisis desarrollados en los apartados precedentes:

Criterio	Sustento
Jurídico	Incorpora salvaguardas convencionales para que México pueda cumplir sus obligaciones constitucionales derivadas del artículo 16 y sus obligaciones internacionales de derechos humanos (Convención de Belém do Pará, jurisprudencias Bedoya Lima y Campo Algodonero). El AR 74/2024 evidencia la insuficiencia del marco interno y refuerza la necesidad de un piso convencional.
Técnico	La propuesta permite gradaciones técnicas (residencia parcial, espejo local, replicación). Es compatible con arquitecturas cloud distribuidas y con la práctica de hyperscalers en Europa; es decir, grandes proveedores de servicios en la nube que ofrecen infraestructura para almacenamiento, analítica y transferencia a escala masiva.
Académico	Adopta el modelo de adecuación condicional consagrado en el RGPD, ampliamente respaldado en la literatura revisada por pares (Aaronson & Leblond, 2018; De Hert & Papakonstantinou, 2016; Greenleaf, 2014; Kuner, 2013) como punto de equilibrio razonable entre flujo de datos y protección de derechos.
Político	Es compatible con las posiciones recientes del Departamento de Comercio de Estados Unidos sobre Privacy Shield 2.0 y con la política canadiense en materia de PIPEDA. No exige a Estados Unidos modificar su derecho interno; amplía el espacio de excepción para los tres países.
Económico	La evidencia europea demuestra que un régimen de adecuación condicional no impide el crecimiento del comercio digital ni desincentiva la inversión cloud. Por el contrario, ha generado inversión directa en regiones cloud nacionales con efecto positivo sobre el empleo calificado.

IV. Artículo 19.16 — Código Fuente y Auditoría Algorítmica

4.1. Texto vigente y alcance

El artículo 19.16 del T-MEC establece, en su párrafo 1, que ninguna Parte requerirá la transferencia o el acceso al código fuente de un programa informático propiedad de una persona de otra Parte, ni al algoritmo expresado en ese código fuente, como condición para la importación, distribución, venta o uso de ese programa. El párrafo 2 incluye una excepción: los organismos reguladores y las autoridades judiciales pueden exigir la preservación y puesta a disposición del código fuente en investigaciones, inspecciones y procedimientos judiciales específicos, sujeto a salvaguardas contra la divulgación no autorizada. Esta excepción existe, pero no funciona. Presenta limitaciones estructurales que la vacían de contenido regulatorio real y que este apartado desarrolla en detalle.

4.2. Problemática

4.2.1. Las limitaciones estructurales de la excepción reguladora

La primera limitación es de alcance. Se puede interpretar que la excepción opera únicamente en casos específicos (investigación, inspección, examen, acción de cumplimiento o procedimiento judicial individualizados) lo que impide la creación de regímenes de auditoría algorítmica sistemática o preventiva y la posibilidad establecer obligaciones de transparencia. La disposición admite el examen del código fuente cuando ya existe un procedimiento en curso, pero bloquea la posibilidad de que un Estado establezca un sistema general de revisión y auditoría obligatoria sobre algoritmos de alto riesgo, como el que consagra la Ley de Inteligencia Artificial de la Unión Europea o en casos urgentes en que los daños de imposible reparación sean inminentes. Dicho de otra forma, México podría revisar el algoritmo después del daño, no antes.

La segunda limitación es procesal. La nota al pie 6 del artículo 19.16 establece que la divulgación no debe interpretarse de forma que afecte negativamente el estatus del código fuente como secreto comercial. Esta cláusula es utilizada sistemáticamente por la industria tecnológica para resistir órdenes de acceso, exigiendo medidas de protección código que en la práctica demoran el ejercicio de la facultad regulatoria hasta hacerla ineficaz.

La tercera limitación es interpretativa. El artículo cubre tanto el código fuente como el algoritmo expresado en él. Este último concepto es deliberadamente amplio y las plataformas lo han utilizado para argumentar que cualquier requisito de transparencia y auditoría sobre criterios de moderación, sistemas de recomendación o decisiones automatizadas equivale a una solicitud de acceso al algoritmo y, por tanto, está prohibido por el T-MEC. Bajo esa interpretación, la opacidad algorítmica queda blindada por un tratado comercial.

4.2.2. Implicaciones para la gobernanza algorítmica de la violencia digital

La relevancia del artículo 19.16 para los derechos digitales se manifiesta con particular intensidad en cuatro frentes que no pueden seguir ignorándose:

El primero son los sistemas de recomendación que amplifican la violencia. La evidencia acumulada en los últimos cinco años —informes de UN Women de 2025[22] y estudios de Amnistía Internacional sobre TikTok[23]— documenta que los sistemas de recomendación algorítmica privilegian sistemáticamente contenido emocionalmente intenso, lo que incluye discurso de odio misógino, contenido sexualizado y material que objetiva a mujeres y niñas. Las auditorías independientes de estos sistemas son técnicamente posibles y no requieren que el código fuente sea transferido ni divulgado a la autoridad regulatoria. Las metodologías de verificación externa —entre ellas las pruebas de caja negra, el red *teaming* y las evaluaciones diferenciales de comportamiento— permiten que un organismo competente evalúe los criterios, sesgos y efectos de un sistema algorítmico sin que la plataforma ceda la propiedad intelectual de su arquitectura técnica.

El segundo frente son las aplicaciones de inteligencia artificial generativa y la violencia sexual digital. La proliferación de aplicaciones "*nudify*" —que generan imágenes íntimas no consentidas mediante modelos de inteligencia artificial— ha sido caracterizada por la literatura especializada como una industrialización a escala de la violencia digital de género (Henry et al., 2026; Umbach et al., 2026). Las víctimas mexicanas amparadas por la Ley Olimpia enfrentan agresores que utilizan estas herramientas con creciente frecuencia.

22 El Informe de UN Women 2025 establece el crecimiento de las violencias contra las mujeres y las niñas facilitadas por las tecnologías (technology-facilitated violence against women and girls) como una amenaza para las usuarias de plataformas sociodigitales.
https://www.unwomen.org/en/digital-library/publications/2025/11/brief-model-framework-for-legislation-on-technology-facilitated-violence-against-women-and-girls.
Y, por otra parte, en otra separata del documento indica que la aceleración en los modelos de inteligencia artificial está vulnerando la integridad de las mujeres, a causa de la manipulación y generación de contenido agresivo o sensible:
https://www.unwomen.org/en/digital-library/publications/2025/12/how-ai-is-exacerbating-technology-facilitated-violence-against-women-and-girls

23 De acuerdo con Amnistía Internacional, el diseño del feed de TikTok motiva autolesiones, ideas suicidas y trastornos de salud mental en adolescentes. https://www.amnesty.org/en/documents/pol40/7350/2023/en/

La tipificación penal alcanza al usuario que difunde, pero no regula efectivamente al desarrollador ni al distribuidor del *software*, cuyo escrutinio técnico está limitado por este artículo. Como señala San Martín (2023), la transparencia algorítmica no solo permitiría acciones punitivas en casos de violencia sexual digital, sino también medidas preventivas, al visibilizar sesgos y falencias en los códigos que alimentan esas tecnologías.

El tercer frente son las decisiones automatizadas sobre moderación de contenido. Cuando una de las plataformas decide algorítmicamente eliminar, restringir o conservar un contenido reportado como violencia digital, esa decisión opera con criterios completamente opacos. La auditoría externa de esos criterios es indispensable para verificar que las plataformas cumplan con las obligaciones que les imponga la legislación nacional y los estándares de derechos humanos de nuestro país. En su redacción vigente, el artículo 19.16 dificulta esa auditoría y somete la moderación de contenidos a los Términos y Condiciones que las propias plataformas se auto-imponen, sin ningún escrutinio externo.

El cuarto frente es el sesgo algorítmico y la discriminación interseccional. La literatura ha documentado de manera robusta que los sistemas algorítmicos predictivos reproducen y amplifican sesgos de género, raza y clase (Köchling & Wehner, 2020; Wang et al., 2024), al segmentar públicos por geolocalización, ingresos, consumos y escolaridad, y recomendar comportamientos a partir de métricas de probabilidad —lo que se denomina *perfilamiento* o *profiling* (Hubbard, 2017). La capacidad del Estado para auditar estos sistemas y verificar el cumplimiento de la prohibición constitucional de discriminación (artículo 1° constitucional) queda severamente restringida cuando el acceso al algoritmo se condiciona a procedimientos individuales y reactivos.

4.2.3. Sustento jurídico-constitucional

La facultad del Estado mexicano para auditar sistemas algorítmicos es una obligación derivada del bloque de constitucionalidad. El artículo 1° constitucional impone al Estado el deber de promover, respetar, proteger y garantizar los derechos humanos, lo que en el contexto digital se traduce en la obligación de auditar los sistemas algorítmicos para que no reproduzcan patrones discriminatorios, amplifiquen violencia ni vulneren la integridad personal o la dignidad.

El artículo 4° constitucional refuerza esta obligación desde dos dimensiones. Primero, consagra el interés superior de la niñez, lo que en el entorno digital contemporáneo impone al Estado garantizar que los sistemas algorítmicos no constituyan factores de daño para

las infancias, ya sea mediante la amplificación de contenidos nocivos, la explotación de vulnerabilidades psicológicas o la exposición sistemática a violencia simbólica. Segundo, reconoce el derecho de toda persona a una vida libre de violencia, mandato que adquiere plena relevancia frente a la evidencia sobre cómo los sistemas de recomendación pueden funcionar como infraestructuras de viralización de contenidos sexistas, agresivos, discriminatorios y misóginos. Leídas en conjunto con el artículo 1° constitucional, ambas disposiciones consolidan la base normativa que obliga al Estado mexicano a ejercer potestades de auditoría y supervisión sobre los sistemas algorítmicos que operan en su jurisdicción. La omisión de esa supervisión constituye una violación por acción insuficiente de los deberes de protección y garantía constitucionalmente establecidos.

La aplicación del test de proporcionalidad reiterado por la SCJN en la jurisprudencia P./J. 130/200724 a la valoración del artículo 19.16 produce como resultado que la excepción reguladora del párrafo 2, al exigir procedimientos específicos individualizados, no resulta idónea para alcanzar el fin constitucionalmente legítimo de prevenir la discriminación algorítmica y la violencia digital sistémica. Una herramienta que solo actúa caso por caso no puede prevenir daños estructurales.

Los criterios interamericanos apuntan en la misma dirección. El caso *Bedoya Lima vs. Colombia* (2021), el caso *González* y otras ("*Campo Algodonero*") vs. México (CIDH, Serie C No. 205, 2009), y la Opinión Consultiva OC-23/17[25] sobre obligaciones estatales en materia de derechos humanos, imponen al Estado el deber de adoptar medidas positivas de prevención frente a riesgos sistémicos. La auditoría algorítmica obligatoria sobre sistemas de alto riesgo es la traducción técnica contemporánea de ese deber.

4.2.4. Sustento académico

La crítica académica más sistemática al artículo 19.16 proviene del trabajo de Irion (2022), que demuestra que las cláusulas de protección del código fuente en acuerdos comerciales son un instrumento de doble filo que entra en tensión directa con la rendición de cuentas algorítmica, y que las excepciones como las del T-MEC son insuficientes para sustentar regímenes regulatorios sistemáticos. Los trabajos de Kaminski (2019) sobre transparencia

24 El test de proporcionalidad señalado en la jurisprudencia antes mencionada es una herramienta metodológica para verificar si la restricción de un derecho fundamental, por parte de un legislador, está justificada. En el caso del artículo 19.16 del T-MEC es claro que no hay justificación para que los sistemas algorítmicos de alto riesgo queden exentos de auditoría regulatoria con salvaguardas de confidencialidad, en aras de prevenir y combatir las violencias.
https://sjf2.scjn.gob.mx/detalle/tesis/170740

25 Esta opinión consultiva de la Comisión Interamericana de Derechos Humanos (CIDH) obliga a los Estados a proteger el medio ambiente y los entornos de desarrollo de las personas, a favor de los derechos humanos.
https://elaw.org/es/resource/iachr_co2317

algorítmica y de Pasquale (2015) sobre la opacidad de la "caja negra" (*black-boxing*), junto con la literatura sobre auditorías algorítmicas obligatorias (Mitchell et al., 2019; Mökander & Floridi, 2021; Raji et al., 2020), apuntan a que la efectividad regulatoria depende de un acceso total que los acuerdos comerciales actuales no garantizan.

Este diagnóstico se refuerza con evidencia mexicana. El estudio de Tlatelolco Lab del PUEDJS-UNAM *Campañas negras y elecciones: el mercado de la desinformación en Facebook* (Atilano, Zumaya, Caloca et al., 2024) documentó que los contenidos de ataque o manipulación, cuando reciben financiamientos cuantiosos, son propagados masivamente por los algoritmos, con independencia de si infringen los Términos y Condiciones de las propias plataformas o los marcos legales que garantizan una vida libre de violencia. Las pautas publicitarias aceleran la difusión de contenido dañino, y eso ocurre precisamente porque los algoritmos que lo permiten no están sujetos a fiscalización externa. El *Decálogo de Derechos Digitales en Redes Sociales* (Tlatelolco Lab, 2023) va en la misma dirección. En su Punto 7, sobre Segmentación y disposición de contenidos, exige que las plataformas informen de manera transparente y precisa a los usuarios cuando su información ha sido usada para mecanismos publicitarios o técnicas automáticas de priorización de contenidos (p. 32), que desarrollen indicadores para identificar mecanismos de manipulación de tráfico (p. 33), y que publiquen informes con sus metodologías y criterios de toma de decisiones, incluyendo los algoritmos de recomendación y los riesgos de sus posibles sesgos (p. 33).

4.2.5. Sustento político

Entre 2018, año de la firma del T-MEC, y 2026, el consenso regulatorio internacional sobre rendición de cuentas algorítmica ha cambiado radicalmente. La Unión Europea adoptó el Reglamento de Servicios Digitales (2022) y el Reglamento de Inteligencia Artificial (2024), que consagran la auditoría algorítmica obligatoria sobre sistemas de alto riesgo. El Reino Unido aprobó la *Online Safety Act* (2023). En los propios Estados Unidos, estados como Colorado, California y Nueva York han adoptado normas que imponen obligaciones de transparencia y auditoría sobre sistemas algorítmicos en empleo, vivienda y servicios financieros (Colorado AI Act de 2024; NYC Local Law 144). El modelo de no acceso al código fuente ya no es un estándar global, es una excepción regulatoria del derecho federal estadounidense de 1996 que el T-MEC trasladó al espacio norteamericano y que hoy contradice la práctica de la propia Unión Americana a nivel estatal. A la par de esto, "mientras la *Federal Trade Commission*, el *Department of Justice* y diversas agencias federales de Estados Unidos han iniciado investigaciones por sesgos algorítmicos discriminatorios, sometiendo a las compañías a procesos de auditoría sobre sus sistemas algorítmicos y sus

datos de entrenamiento como parte de esos procedimientos, el T-MEC limita la capacidad de México para ejercer facultades regulatorias análogas frente a las mismas plataformas. Esto es insostenible y debe corregirse.

El frente político mexicano acompaña esta demanda. La agenda impulsada por el movimiento Ley Olimpia LATAM, así como las iniciativas recientes de la Presidencia de la República y la Secretaría de las Mujeres,26 han posicionado el tema en la agenda pública. Sin embargo, la vía de los acuerdos voluntarios con las plataformas, que ha sido objeto de crítica fundada desde la academia y los centros universitarios, no puede sustituir la reforma estructural que este artículo requiere. Los acuerdos voluntarios dependen de la buena voluntad de quienes tienen interés en la opacidad; la reforma al T-MEC crea obligaciones exigibles.

4.2.6. Sustento económico

El argumento tradicional de la industria es que el código fuente constituye el activo intangible central de la economía digital y que su protección frente a transferencias forzosas es indispensable para sostener la inversión en investigación y desarrollo. La evidencia europea refuta esta tesis. La Unión Europea estableció obligaciones de auditoría sobre sistemas de alto riesgo mediante el AI Act y la Ley de Servicios Digitales sin que eso provoque desinversión en el sector. Las grandes empresas tecnológicas estadounidenses operan en Europa cumpliendo con esas obligaciones. El costo regulatorio existe, pero es acotado y no ha impactado negativamente al mercado, sino que ha sido una medida positiva. Lo que sí ha generado es una supeditación del factor económico a la garantía de derechos en el entorno digital.

La distinción que este debate exige es también lo que omite el artículo 19.16: la diferencia entre *transferencia* del código fuente, que implica ceder la propiedad intelectual, y *auditoría* por parte de una autoridad regulatoria independiente, sujeta a estrictos deberes de confidencialidad. Una auditoría no transfiere el código, sino que lo supervisa. Confundir ambas figuras, o permitir que se confundan, es una opción política en favor de la opacidad corporativa.

---

26 En las últimas semanas, la Presidencia de la República del Gobierno de México, a través de la Secretaría de las Mujeres, ha implementado una serie de acuerdos voluntarios con las plataformas digitales con la finalidad de erradicar la violencia en las redes sociales hacia las mujeres.
https://www.gob.mx/presidencia/prensa/gobierno-de-mexico-firma-primer-acuerdo-de-colaboracion-voluntaria-con-google-meta-y-tiktok-para-combatir-violencia-digital-contra-mujeres?idiom=fr.
Sin embargo, el carácter de colaboración voluntaria ha sido criticado fuertemente por espacios académicos y universitarios.
https://puedjs.unam.mx/pronunciamiento-dirigido-a-la-atdt-del-gobierno-de-mexico/

4.3 Propuesta de modificación al artículo 19.16

Se propone reformular el párrafo 2 del artículo 19.16 y añadir un nuevo párrafo 3:

Texto vigente (párrafos 1 y 2)

1. Ninguna Parte requerirá la transferencia de, o el acceso a, un código fuente del programa informático propiedad de una persona de otra Parte, o el algoritmo expresado en ese código fuente, como condición para la importación, distribución, venta o uso de tal programa informático, o de productos que contengan tal programa informático, en su territorio.

2. Este Artículo no impide que un organismo regulador o autoridad judicial de una Parte exija a una persona de otra Parte que preserve y ponga a disposición el código fuente del programa informático, o el algoritmo expresado en ese código fuente, al organismo regulador para una investigación, inspección, examen, acción de cumplimiento o procedimiento judicial específicos, sujeto a salvaguardias contra la divulgación no autorizada.

Texto propuesto (esencia)

2. Este Artículo no impide que un organismo regulador, autoridad judicial o autoridad nacional competente designada por una Parte exija a una persona de otra Parte que preserve, ponga a disposición o someta a auditoría el código fuente del programa informático o el algoritmo expresado en ese código fuente, en los siguientes supuestos: (a) investigaciones, inspecciones, exámenes, acciones de cumplimiento o procedimientos judiciales específicos; (b) verificaciones al cumplimiento de normas aplicables en el estado Parte para la protección de derechos fundamentales o normas de orden público (c) para la prevención y protección de derechos humanos,; (c) rendiciones de cuentas vinculantes y sistémicas sobre las afectaciones a derechos provocadas por sistemas algorítmicos clasificados como de alto riesgo por la legislación nacional, particularmente aquellos que intervengan en la moderación de contenidos, la generación de contenido sintético, la toma de decisiones que afecten derechos fundamentales o la prevención de la violencia digital de género; y (d) verificaciones de cumplimiento de obligaciones de transparencia algorítmica, evaluaciones de impacto sobre derechos humanos y mitigación de sesgos discriminatorios.

3. Las medidas adoptadas conforme al párrafo 2 estarán sujetas a salvaguardas contra la divulgación no autorizada y respetarán el carácter de secreto comercial del código fuente, sin que ello pueda interpretarse en el sentido de impedir el ejercicio efectivo de la facultad regulatoria.

4.4 Sustento integrado de la propuesta

El siguiente cuadro sistematiza los fundamentos de la propuesta de modificación al artículo 19.12 desde sus múltiples dimensiones:

Criterio	Sustento
Jurídico	Habilita el ejercicio efectivo de las facultades regulatorias derivadas del artículo 1° constitucional (no discriminación) y del bloque interamericano (Bedoya Lima vs. Colombia, OC-23/17). Aplica el test de proporcionalidad de la SCJN (P./J. 130/2007). Habilita la auditoría regulatoria con salvaguardas de confidencialidad sobre sistemas algorítmicos de alto riesgo, incluyendo aquellos utilizados para la generación de contenido sintético como los deepfakes que objetivan y cosifican a las personas.
Técnico	La distinción entre transferencia (que quedaría prohibida) y auditoría con salvaguardas (que sería permitida) es técnicamente operativa, porque existen metodologías como pruebas de caja negra, auditorías de "equipo rojo" (red teaming), que simulan ataques informáticos para reforzar defensas, y evaluaciones diferenciales que permiten supervisar sistemas sin transferir el código.
Académico	Adopta el marco de algorithmic accountability desarrollado por la academia (Irion, 2022; Pasquale, 2015; Kaminski, 2019; Raji et al., 2020; Mitchell et al., 2019) y converge con el modelo de marcos regulatorios como la AI Act y la Ley de Servicios Digitales (DSA) de la Unión Europea, que ponen normas a los usos cotidianos de tecnologías como las inteligencias artificiales para garantizar la seguridad de las y los propios usuarios.
Político	La Federal Trade Commission, el Department of Justice y diversos estados de Estados Unidos han iniciado procesos similares (Colorado AI Act, NYC Local Law 144). La propuesta reconoce el espacio soberano y regulatorio que México y Canadá necesitan y que el propio derecho estadounidense, a nivel estatal, ya está construyendo.
Económico	La evidencia europea (DSA, AI Act) demuestra que los regímenes de auditoría no desincentivan la inversión ni impactan negativamente al mercado; sino que es una medida positiva. Los costos de cumplimiento son significativamente menores que los costos sociales de la violencia digital.

V. Artículo 19.17 — Servicios Informáticos Interactivos y Responsabilidad de Plataformas

5.1 Texto vigente y alcance

El artículo 19.17 traslada al T-MEC el régimen de inmunidad de los intermediarios digitales consagrado en la Sección 230 de la *Communications Decency Act* estadounidense de 1996. En esencia, dispone que ninguna Parte adoptará o mantendrá medidas que traten a un proveedor o usuario de un servicio informático interactivo como proveedor del contenido para determinar su responsabilidad por daños relacionados con la información almacenada, procesada, transmitida o distribuida por el servicio. Añade la denominada "cláusula del buen samaritano" que señala que ningún proveedor puede ser responsabilizado por las acciones que adopte voluntariamente y de buena fe para restringir el acceso a material que considere dañino.

El Anexo 19-A pospuso la aplicación del artículo en México hasta el 1 de julio de 2023 y precisó tres acotaciones: los artículos 145 y 146 de la hoy derogada Ley Federal de Telecomunicaciones y Radiodifusión no son incompatibles con este artículo; está sujeto a las excepciones generales del artículo 32.1; y la inmunidad no cubre la responsabilidad bajo el régimen de derechos de autor, que se rige por el Capítulo 20. Lo que el T-MEC hizo, en síntesis, fue tomar un modelo regulatorio diseñado en 1996 para proteger a pequeños tableros de avisos electrónicos y convertirlo en obligación jurídica vinculante para México y Canadá en 2018. Eso es justo lo que hay que corregir, por las razones que se exponen a continuación.

5.2 Problemática

5.2.1 Dimensión jurídica

El artículo 19.17 entra en tensión con un cuerpo normativo y jurisprudencial creciente que choca de frente con ese modelo de inmunidad. La tensión se manifiesta en cuatro frentes: El primero es el legislativo nacional. La Ley Olimpia —reformas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal, 2021— tipifica la violación a la intimidad sexual y obliga a las plataformas digitales a retirar contenido ilícito cuando este se denuncia. La efectividad de esa obligación depende de mecanismos de coordinación con las plataformas, plazos de respuesta y, ante el incumplimiento, instrumentos de exigibilidad. La inmunidad genérica del artículo 19.17 debilita la posición

jurídica de la víctima y dificulta la articulación de un régimen sancionatorio efectivo. La estructura del Tratado opera como un tope regulatorio que acota el alcance protector de la legislación interna mexicana.

El segundo frente es el jurisprudencial mexicano. La doctrina de la SCJN sobre moderación de contenido, desarrollada en el Amparo en Revisión 16/2023[27] (Primera Sala, 28 de mayo de 2025) y en el Amparo en Revisión 673/2024[28] (Primera Sala, 9 de julio de 2025), confirma que el orden constitucional mexicano admite la imposición de obligaciones procedimentales sobre las decisiones de moderación, siempre que se respete el test de proporcionalidad. La inmunidad genérica del artículo 19.17 va más allá de lo que la propia jurisprudencia mexicana exige y, en esa medida, constituye una concesión innecesaria al modelo regulatorio estadounidense. El Amparo en Revisión 587/2017 (caso Ulrich Richter Morales contra Google Inc.)[29] y el AR 556/2022[30] promovido por la organización ARTICLE 19 refuerzan la idea de que cualquier modelo de notificación, retiro o responsabilidad debe construirse con garantías de debido proceso, transparencia y revisión judicial, para evitar la deriva hacia censura privada o automatizada.

Un mecanismo concreto ilustra tanto la necesidad de regular la moderación de contenido como los riesgos de hacerlo sin marco adecuado. La Jurisprudencia 21/2018 del TEPJF[31] avaló el uso de medidas cautelares en casos de Violencia Política por Razones de Género, incluyendo expresiones en Internet. A partir de ella, el Instituto Nacional Electoral (INE) consolidó un sistema mediante el cual ordena a plataformas como Facebook, Instagram, YouTube y X (antes Twitter) la remoción de contenidos en plazos no mayores a seis horas, sin que medie una decisión judicial previa que determine si el contenido es efectivamente ilícito. Entre 2016 y 2023, el INE emitió 959 medidas cautelares de este tipo, con tendencia creciente desde 2018. Las plataformas acatan esas órdenes, lo que demuestra que la

27 El Amparo en Revisión 16/2023 de la Primera Sala de la SCJN analiza si el bloqueo de comentarios en YouTube por el INE constituye censura previa, afectando la libertad de expresión y acceso a la información.
https://www.scjn.gob.mx/sites/default/files/listas/documento_dos/2025-05/250522-AR-16-2023.pdf

28 El Amparo en Revisión 673/2024, resuelto por la Primera Sala de la SCJN en julio 2025, determinó que una Gobernadora (Campeche) vulneró los derechos al honor y presunción de inocencia de un senador al calificarlo en su programa de redes sociales como "traficante de influencias".
https://www.scjn.gob.mx/sites/default/files/listas/documento_dos/2025-07/250702-AR-673-2024.pdf

29 El Amparo en Revisión 587/2017, resuelto por la Suprema Corte de Justicia de la Nación (SCJN) en 2017, trató sobre la competencia de los jueces mexicanos para juzgar a empresas extranjeras como Google por daño moral. El caso derivó de una demanda por contenido difamatorio en un blog, marcando un precedente sobre la responsabilidad de plataformas digitales.
https://www2.scjn.gob.mx/juridica/engroses/1/2017/2/2_218201_3735_firmado.pdf

30 El Amparo en Revisión 556/2022 (A.R. 556/2022), resuelto por la Primera Sala de la Suprema Corte de Justicia de la Nación (SCJN) de México, analiza la constitucionalidad de los artículos 114 Quinquies, 114 Octies, 232 Ter y 232 Quinquies de la Ley Federal del Derecho de Autor (LFDA), reformados en 2020 relacionados con el mecanismo de "notificación y retirada".
https://www.scjn.gob.mx/sites/default/files/listas/documento_dos/2024-01/240110-AR-556-2022.pdf

31 https://elecciones2021.te.gob.mx/IUSTEMP/Jurisprudencia%2021-2018.pdf

inmunidad genérica del artículo 19.17 no ha impedido en la práctica que actúen como moderadoras por encargo del Estado. Pero lo hacen de manera opaca, sin criterios públicos anclados en estándares de derechos humanos y sin mecanismos de revisión accesibles ni rendición de cuentas, lo que ha generado remociones que alcanzan contenidos de crítica política legítima. La conclusión evidencia que la inmunidad del artículo 19.17 no suprime la moderación de contenido; suprime el marco que haría que esa moderación fuera legítima, transparente y verificable.

El tercer frente es el interamericano. La Corte Interamericana ha avalado la aplicación *ex post* y de manera proporcional de los límites necesarios a la libertad de información y expresión para asegurar la no afectación de otros derechos[32], y ha extendido al ámbito digital el estándar de responsabilidad reforzada frente a la violencia contra las mujeres. La sentencia del 26 de agosto de 2021 en el caso *Bedoya Lima y otra vs. Colombia* (Serie C No. 431) establece que el Estado debe adoptar medidas eficaces para prevenir, investigar y sancionar la violencia digital de género, incluyendo la facilitada por plataformas. Este estándar, leído junto con la sentencia *Campo Algodonero* (Serie C No. 205, 2009), es incompatible con la limitación que el artículo 19.17 introduce. La Relatoría Especial para la Libertad de Expresión, en su informe de 2024 sobre Inclusión Digital y Gobernanza de Contenidos en Internet, recomienda expresamente que los Estados adopten las disposiciones necesarias para que las plataformas apliquen el test tripartito, garanticen garantías procesales en sus prácticas de moderación, e instituyan mecanismos de evaluación de riesgo y la correspondiente responsabilidad[33].

El cuarto frente es el comparado. El Tribunal Europeo de Derechos Humanos ha consolidado un cuerpo jurisprudencial que respalda la viabilidad del modelo de responsabilidad. La sentencia de la Gran Sala en *Delfi AS vs. Estonia* (demanda 64569/09, 16 de junio de 2015) confirmó que la condena civil a un portal de noticias por comentarios anónimos extremos no viola la libertad de expresión34. Así también, la sentencia en *MTE e Index.hu vs. Hungría* (demanda 22947/13, 2 de febrero de 2016)[35] precisó ese precedente. El caso *K.U. vs. Finlandia* (demanda 2872/02, 2 de diciembre de 2008)[36] declaró la responsabilidad del Estado por no contar con un marco normativo que permitiera identificar al autor de un anuncio sexual falso publicado contra un menor en una plataforma: un precedente directamente aplicable al supuesto de la Ley Olimpia. Incluso la Suprema Corte de Estados

32 Caso Herrera Ulloa vs. Costa Rica, sentencia de la Corte Interamericana de Derechos Humanos de 22 de julio de 2004, https://www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf
33 https://www.oas.org/es/cidh/expresion/informes/Inclusion_digital_esp.pdf
34 https://hudoc.echr.coe.int/fre?i=001-155105
35 https://hudoc.echr.coe.int/eng?i=002-10868
36 https://hudoc.echr.coe.int/eng?i=001-139376

Unidos ha empezado a cuestionar el modelo Sección 230 en los casos *González v. Google LLC* (598 U.S. 617, 18 de mayo de 2023)[37] y *Twitter, Inc. vs. Taamneh* (598 U.S. 471, 18 de mayo de 2023)[38], donde se responsabilizaba a las empresas gestoras de las plataformas por su distribución de contenido. En *Moody vs. NetChoice* (1 de julio de 2024)[39], por su parte, la Corte de los Estados Unidos reconoció que la moderación de contenido constituye un acto editorial protegido, pero dejó expresamente abierta la puerta a regulaciones procedimentales que no interfieran con el contenido expresivo. La distinción entre regulación de contenido y regulación procedimental, fijada por el tribunal que más ha defendido el modelo de la Sección 230, es precisamente la base que sustenta la viabilidad constitucional de las obligaciones y responsabilidades aquí propuestas.

5.2.2 Dimensión técnico-computacional

La Sección 230 de la *Communications Decency Act* fue concebida en 1996 para un ecosistema digital radicalmente distinto del actual. Las plataformas de aquella época eran tableros de avisos electrónicos sin sistemas de recomendación algorítmica, sin monetización por publicidad personalizada y sin moderación automatizada a escala masiva. La arquitectura técnica contemporánea ha transformado la naturaleza del servicio al precisar que las plataformas operan hoy con sistemas de recomendación que curan y jerarquizan contenido en tiempo real, modelos de aprendizaje automático que optimizan el *engagement* del usuario y procesos de moderación que combinan revisión humana con clasificadores automatizados a escala global. Además de que dicha arquitectura técnica tiene un efecto multiplicador de la información que puede generar daños irreparables y que exige un deber de diligencia mayor para los creadores y operadores de dicha tecnología. Las plataformas dejaron de ser tecnologías neutrales hace tiempo. Se convirtieron en editores algorítmicos.

La amplificación viral de contenido violento, incluyendo discurso de odio misógino y materiales que constituyen violencia digital de género, es una consecuencia directa del diseño técnico de los sistemas de recomendación, calibrados para maximizar el tiempo de uso y, con ello, la exposición publicitaria (Klonick, 2018). La distancia técnica entre el servicio que la Sección 230 protegía en 1996 y el servicio que las plataformas prestan en 2026 hace que cualquier régimen de inmunidad heredado sea, en términos técnicos, un anacronismo.

37 https://supreme.justia.com/cases/federal/us/598/21-1333/
38 https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf
39 https://www.supremecourt.gov/opinions/23pdf/22-277_d18f.pdf

La realidad técnica también permite distinguir con precisión entre obligaciones viables y obligaciones desproporcionadas. Las plataformas ya operan sistemas de detección automatizada de contenido, mecanismos de notificación masiva y procesos de revisión escalonada. La obligación de operar mecanismos eficaces de notificación y retiro para casos de violencia digital de género es, técnicamente, una extensión menor de capacidades que ya están desplegadas. El argumento de inviabilidad técnica no se sostiene. El *Decálogo de Derechos Digitales en Redes Sociales* (Tlatelolco Lab, PUEDJS-UNAM, 2024) lo confirma en su Punto 8, sobre el derecho a la no discriminación y a la vida libre de violencia en plataformas ya que exige que las plataformas brinden a las usuarias mujeres mecanismos de reportes y notificación específicos para casos constitutivos de violencia de género (p. 52) y que los usuarios de pueblos indígenas cuenten con protocolos en su lengua para denunciar discriminación.

5.2.3 Dimensión académica

La doctrina especializada en responsabilidad de intermediarios ha construido, en la última década, un consenso crítico sobre la insostenibilidad del modelo de inmunidad genérica. Los trabajos de Citron y Wittes (2017) sostienen que la Sección 230, en su lectura jurisprudencial expansiva, ha generado externalidades negativas significativas, particularmente en la protección de víctimas de violencia digital de género. La denominación de *bad samaritans* para las plataformas que invocan la inmunidad sin cumplir obligaciones mínimas captura con precisión la asimetría que el artículo 19.17 traslada al ámbito trinacional.

Klonick (2018) ha caracterizado a las plataformas digitales como new governors del discurso público en línea, derivado del poder editorial que ejercen mediante sus sistemas de moderación y recomendación. Si las plataformas ejercen funciones cuasi-públicas, no pueden simultáneamente reclamar la inmunidad de los actores privados pasivos. Tal como señalan Silva García y Gómez Sámano “En el mundo globalizado y digital, las relaciones asimétricas de potestad-sujeción se dan también entre particulares. Los poderes fácticos del mercado que no están regulados son fuentes de desigualdades y de no libertad que, a falta de límites legales, tienden a acumularse de formas absolutas” (2019 p.36).

Balkin (2018) profundiza esta línea con su modelo del triángulo de la libertad de expresión: la regulación de plataformas debe equilibrar tres vértices —Estado, plataforma y usuario— en lugar de privilegiar exclusivamente la inmunidad del intermediario. La literatura sobre alternativas regulatorias (Goldman, 2020; Keller, 2019) ha identificado el modelo de inmunidad condicionada como el horizonte regulatorio del siglo XXI en materia de

responsabilidad de intermediarios. Bajo ese modelo, la inmunidad por contenido que la plataforma no tiene conocimiento efectivo se preserva, pero se condiciona al cumplimiento de obligaciones en torno a la auditoría algorítmica.

La literatura crítica feminista, a través de los trabajos de Citron sobre *cyber harassment*, los de Suzor (2019) sobre gobernanza digital, y los de Gurumurthy y Chami (2022), ha demostrado que la inmunidad genérica reproduce y amplifica asimetrías de género en el espacio digital. Las víctimas de violencia digital, mayoritariamente mujeres y niñas, asumen el costo de la moderación que la plataforma elude bajo el manto de la inmunidad. Ese desplazamiento del costo regulatorio hacia la víctima es el reverso operativo del artículo 19.17. Al respecto, Tlatelolco Lab del PUEDJS-UNAM, a través de su artículo *Moderación de contenidos, desinformación y discursos de odio. El nuevo modelo autorregulatorio de Meta* (Neubauer, 2025), ha señalado la urgencia de innovar marcos adecuados que detecten discursos degradantes, discriminatorios, excluyentes o abiertamente violentos, sin incurrir en censura ni menoscabar la libertad de expresión, pero fomentando una cultura de la no violencia.

5.2.4 Dimensión política

La regulación internacional de plataformas atraviesa, en la antesala de la revisión 2026 del T-MEC, un punto de inflexión que no puede ignorarse. La Unión Europea adoptó en 2022 el Reglamento de Servicios Digitales (DSA), que introduce un modelo radicalmente distinto al de la Sección 230. El Reino Unido aprobó en 2023 la *Online Safety Act*[40]. Brasil reformó su Marco Civil de Internet para incorporar obligaciones y responsabilidades[41]. Australia, India, Japón y Corea del Sur han adoptado regímenes de responsabilidad graduada. El modelo Sección 230, lejos de ser un estándar global, se ha convertido en una excepción regulatoria del derecho federal estadounidense que el T-MEC trasladó al espacio norteamericano en 2018 y que hoy el mundo entero está abandonando.

La asimetría política del artículo 19.17 evidencia que México y Canadá se sumaron en 2018 a un modelo diseñado para los intereses de las corporaciones digitales estadounidenses, en un momento en que la propia legislación interna mexicana apuntaba en dirección contraria.

40 Se trata de una ley histórica al considerar el comportamiento de motores de búsqueda, curación de contenidos en plataformas y tipos de publicaciones distribuidas, con el fin de proteger a las infancias y usuarios en general de contenido ilegal y perjudicial.
https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

41 En su ley 12965 Brasil hace valer la neutralidad de la Red, seguridad de las y los usuarios, protección de la privacidad y protección de datos personales.
https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

La revisión 2026 es el momento para corregir esa asimetría. Canadá, mediante el proyecto de *Online Harms Act* y sus desarrollos posteriores, ha construido una posición regulatoria convergente con el modelo europeo. Existe, por tanto, una mayoría política trinacional —México y Canadá— para impulsar una reformulación del artículo 19.17 compatible con los desarrollos regulatorios internacionales. En el propio Congreso estadounidense se han presentado al menos catorce proyectos de reforma a la Sección 230 desde 2020, entre ellos el SAFE TECH Act y el EARN IT Act, lo que evidencia consenso bipartidista sobre la necesidad de reforma, aun sin resolución legislativa interna.

El frente doméstico mexicano es igualmente favorable. El movimiento Ley Olimpia LATAM ha posicionado la violencia digital de género en la agenda pública con una capacidad de movilización que no puede subestimarse. La trayectoria de Olimpia Coral Melo en torno a la lucha por la justicia frente a la violencia digital encuentra un techo en el carácter transnacional de las plataformas y en la asimetría de poder con las corporaciones digitales. Ese techo está fijado, en parte, por el artículo 19.17.

La articulación con organizaciones canadienses (Internet Society of Canada, Canadian Internet Policy and Public Interest Clinic) y estadounidenses (Electronic Frontier Foundation, Center for Democracy & Technology) amplía el frente político y permite construir un consenso que trasciende una agenda unilateral mexicana. ONU Mujeres publicó en 2025 un Modelo de Marco Legislativo sobre violencia digital facilitada por la tecnología que recomienda expresamente incorporar obligaciones y responsabilidades a las plataformas. La convergencia entre la agenda de género, la agenda regulatoria europea y la agenda comercial trinacional configura el momento político más propicio en años para modificar este artículo.

5.2.5 Dimensión económica y comercial

El argumento económico contra la modificación del artículo 19.17 sostiene que las obligaciones y responsabilidades hacia las plataformas elevarán costos, desincentivan la inversión y producen un efecto disuasivo sobre la innovación. La evidencia empírica reciente refuta cada uno de esos argumentos.

Los costos de cumplimiento son asumibles. La Unión Europea adoptó el DSA en 2022 y las grandes plataformas (Meta, Alphabet, Amazon, X, TikTok) han desplegado sin mayor fricción los sistemas de cumplimiento exigidos: equipos de moderación, mecanismos de notificación accesibles, transparencia algorítmica documentada y auditorías externas

obligatorias. Los reportes financieros de estas corporaciones no muestran impactos materiales adversos atribuibles al DSA. La capacidad técnica y económica para cumplir obligaciones ya existe y ya está operando.

Las plataformas no se retiran de mercados regulados que garantizan el respeto a los derechos fundamentales. La amenaza de retirada, frecuentemente esgrimida contra la regulación, no se ha materializado en ninguna jurisdicción que adoptó regímenes de responsabilidad. El mercado mexicano, con más de 100 millones de usuarios de Internet y una penetración de *smartphones* superior al 80%, es estructuralmente atractivo para las plataformas globales. La probabilidad de retirada en respuesta a obligaciones razonables es prácticamente nula. El modelo de inmunidad condicionada penaliza a las plataformas que omiten cumplir obligaciones procesales. Una regulación que recompensa la responsabilidad y sanciona la omisión no impone cargas uniformes a toda la industria. Las plataformas que ya cumplen estándares europeos no enfrentarán costos incrementales significativos por extender ese cumplimiento al mercado mexicano; de hecho, están obligadas a cumplir con dichos estándares en México al procesar datos de origen europeo.

La regulación puede, además, constituir una ventaja competitiva. Un marco regulatorio claro, predecible y compatible con el europeo facilita la operación transfronteriza de plataformas que no son las grandes incumbentes estadounidenses: empresas mexicanas, canadienses, latinoamericanas y europeas que buscan competir en el espacio digital se benefician de reglas comunes. La inmunidad genérica del artículo 19.17 blinda a los actores dominantes. La modificación propuesta abre espacio competitivo para nuevos entrantes y garantiza el cumplimiento de legislación internacional y tratados aplicables en México por el origen de datos y nacionalidad de las empresas.

Finalmente, los costos económicos de la inacción son sistemáticamente omitidos en los cálculos convencionales. La violencia digital de género produce costos directos (ausentismo laboral, gastos médicos y psicológicos, abandono de empleos por mujeres víctimas, pérdida de capital humano) que la OIT y ONU Mujeres han cuantificado en pérdidas de productividad superiores al 1% del PIB en países afectados. Una contabilidad económica integral, que incorpore tanto costos de cumplimiento como costos de inacción, favorece sustancialmente al régimen de inmunidad condicionada.

5.2.6 Síntesis: la asimetría entre la víctima y la plataforma

La estructura de inmunidad del artículo 19.17 traslada el costo de la moderación a la víctima como externalidad negativa. Cuando un contenido sexual íntimo no consentido se difunde por una plataforma, la víctima debe identificar la publicación, reportarla, esperar a que la plataforma actúe y, si esta no lo hace, iniciar un litigio cuya viabilidad jurídica está disminuida por la inmunidad que el Tratado consagra. En el ecosistema de Internet la carga más alta de protección recae en el agente más débil que es el usuario y la carga menos fuerte en las plataformas que no enfrentan ninguna obligación correlativa de responsabilidad. La inmunidad opera antes del daño y la cláusula del buen samaritano protege incluso la decisión de no actuar, con la sola invocación de la buena fe.

La asimetría se torna estructural porque las víctimas son individuos, mayoritariamente mujeres y niñas; las plataformas son corporaciones globales con capacidades técnicas y jurídicas incomparablemente superiores. La inmunidad genérica profundiza esa asimetría. La propuesta que se desarrolla a continuación busca redistribuir el costo de la moderación conforme a la capacidad de cada actor, preservando la inmunidad por contenido del que la plataforma no tiene conocimiento efectivo y condicionándola al cumplimiento de obligaciones y responsabilidades (Citron & Wittes, 2017; Goldman, 2020; Keller, 2019) para contribuir a un Internet más seguro para todas y todos. El modelo de referencia es el DSA europeo que podemos considerar para diseñar un modelo seguro que se ajuste a la realidad de nuestro país. Su viabilidad queda en evidencia ya que las plataformas estadounidenses no se han retirado del mercado europeo y cumplen sus obligaciones. La revisión 2026 del T-MEC es la ventana institucional para que México y Canadá converjan hacia ese horizonte regulatorio.

5.3 Propuesta de modificación al artículo 19.17

Se propone reformular el artículo 19.17 para sustituir el modelo de inmunidad genérica por un modelo de inmunidad condicionada al cumplimiento de obligaciones y responsabilidades, en línea con los desarrollos comparados más recientes.

Texto propuesto (esencia)

1. Las Partes reconocen el papel de los servicios informáticos interactivos en la economía digital y la libertad de expresión, así como la necesidad de equilibrar dichos intereses con la protección efectiva de los derechos de las personas, en particular de las mujeres, niñas, niños y adolescentes frente a la violencia digital.

2. Sujeto a lo dispuesto en los párrafos siguientes, ninguna Parte tratará a un proveedor o usuario de un servicio informático interactivo como proveedor del contenido publicado por terceros para efectos de responsabilidad civil.
3. La protección establecida en el párrafo 2 estará condicionada al cumplimiento, por parte del proveedor, de las siguientes obligaciones, conforme a la legislación de cada Parte: (a) establecimiento de mecanismos eficaces y accesibles para la notificación y retiro de contenidos ilícitos; (b) plazos razonables de respuesta a notificaciones, particularmente en casos de violencia digital de género, contenidos íntimos no consentidos y material relativo a niñas, niños y adolescentes; (c) transparencia respecto de las políticas y prácticas de moderación; (d) cooperación oportuna con las autoridades nacionales competentes en investigaciones criminales y (e) sujeción a la legislación y jurisdicción nacionales en casos de controversias derivadas de violaciones a disposiciones de orden público o protección de derechos fundamentales de los ciudadanos de cada Parte. 4. Las Partes podrán imponer obligaciones reforzadas de evaluación de riesgos y auditoría a las plataformas que, por su tamaño o función sistémica, presenten mayores riesgos para los derechos de las personas.

5. Las Partes cooperarán en el intercambio de buenas prácticas regulatorias y en el desarrollo de marcos compatibles para la atención de la violencia digital de género.

5.4 Sustento integrado de la propuesta

El siguiente cuadro sistematiza los fundamentos de la propuesta de modificación al artículo 19.12 desde sus múltiples dimensiones:

Criterio	Sustento
Jurídico	Restituye el equilibrio entre libertad de expresión y derechos de las víctimas, conforme al test de proporcionalidad de la SCJN y a la sentencia Bedoya Lima vs. Colombia (Corte IDH, 2021). El precedente K.U. vs. Finlandia (TEDH, 2008) sustenta que la inmunidad no puede impedir las obligaciones positivas del Estado frente a la violencia digital.
Técnico	Las obligaciones propuestas (notificación-retiro, plazos, transparencia, cooperación) están técnicamente normalizadas en estándares ISO/IEC, directrices de la OCDE y en los propios compromisos de autorregulación de las plataformas. Su implementación es factible y está parcialmente desplegada.
Académico	Adopta el modelo de inmunidad condicionada, dominante en la literatura especializada (Citron & Wittes, 2017; Goldman, 2020; Keller, 2019; Klonick, 2018) y operativo en el DSA europeo, la Online Safety Act británica (2023) y el Marco Civil de Internet brasileño en su reforma reciente.
Político	El Congreso de Estados Unidos ha presentado al menos catorce proyectos de reforma a la Sección 230 desde 2020 (SAFE TECH Act, EARN IT Act, PACT Act). Existe consenso bipartidista sobre la necesidad de reforma. Moody v. NetChoice (2024) deja expresamente abierto el espacio para la regulación procedimental.
Económico	El DSA europeo no ha generado salida de las plataformas estadounidenses del mercado. Los costos de cumplimiento (como externalidades positivas) son menores que los costos sociales documentados de la violencia digital, estimados por la OIT y ONU Mujeres en pérdidas de productividad superiores al 1% del PIB en países afectados (como externalidades negativas).

VI. Visión integradora: tres eslabones de una misma cadena

Para que una víctima de violencia digital en México pueda obtener justicia efectiva, deben confluir tres condiciones simultáneas. Las autoridades nacionales deben tener acceso oportuno a la evidencia digital. Deben poder exigir rendición de cuentas y auditar los sistemas algorítmicos que amplifican o moderan la violencia. Y la plataforma debe estar sujeta a un régimen efectivo de obligaciones y eventual responsabilidad. Los artículos 19.12, 19.16 y 19.17 del T-MEC, en su redacción vigente, bloquean cada una de esas tres condiciones. Las modificaciones propuestas en este documento las restituyen.

El primer eslabón es la evidencia. Sin acceso efectivo y oportuno a los datos almacenados por las plataformas, la autoridad investigadora opera en un vacío probatorio que hace materialmente imposible documentar, perseguir y sancionar las violaciones de derechos que se producen en entornos digitales. Aquí cobra relevancia la jurisdicción que rige sobre los datos que las plataformas almacenan, qué procedimientos se activan ante una solicitud de información urgente y cuánto tiempo transcurre entre esa solicitud y la obtención de la evidencia. Un modelo de representación local con facultades reales de atención a solicitudes de información logra ese objetivo de forma proporcional, sin imponer cargas de infraestructura desproporcionadas y sin contradecir los marcos normativos vigentes en los propios Estados Unidos y Canadá. El artículo 19.12, en su formulación actual, no garantiza que las autoridades mexicanas puedan obtener evidencia oportunamente. Su modificación es la condición de arranque de todo el mecanismo.

El segundo eslabón es la comprensión del sistema que amplifica el daño. Las plataformas y sus algoritmos determinan qué contenido se suprime, qué se amplifica y a qué velocidad. Una víctima de acoso coordinado no solo padece los mensajes individuales, sino el diseño del sistema que los hace virales. Sin la facultad de auditar ese sistema, que es lo que restituye la modificación del artículo 19.16, la autoridad puede tener acceso a la evidencia del daño sin poder determinar si ese daño fue facilitado, acelerado o amplificado por una decisión algorítmica de la plataforma. La auditoría es el instrumento que permite distinguir entre un daño que ocurrió a pesar de los sistemas de moderación y uno que ocurrió gracias a ellos o por su propio diseño.

El tercer eslabón es la consecuencia. La evidencia y el conocimiento del funcionamiento algorítmico solo se traducen en protección efectiva si la plataforma está sujeta a un régimen

que la obligue a actuar y que la responsabilice cuando no lo hace. Eso es lo que introduce la modificación del artículo 19.17, un estándar de responsabilidad que exige mecanismos proactivos, auditables y verificables. Sin este régimen, las dos modificaciones anteriores quedan suspendidas en el aire, son facultades de investigación sin correlato sancionatorio, herramientas que documentan el daño, pero no crean incentivo alguno para prevenirlo.
Las tres modificaciones no son propuestas independientes. Forman una arquitectura en la que cada eslabón valida y sostiene a los demás. Es esa coherencia interna la que convierte esta propuesta en una reforma capaz de abordar, de manera soberana y sistémica, la violencia digital como problema estructural y no como serie de casos aislados.

VII. Conclusiones

Las tres propuestas de modificación desarrolladas en este documento son una exigencia jurídica que el Estado Mexicano está obligado a formular en el marco de la Revisión Conjunta 2026. El diseño actual de los artículos 19.12, 19.16 y 19.17 del T-MEC produce una incompatibilidad estructural con obligaciones constitucionales e interamericanas que el actual gobierno no puede seguir tolerando. La inacción en el proceso de revisión sería la ratificación tácita de un régimen normativo que activamente obstaculiza la protección de víctimas de violencia digital y que subordina el ejercicio de la soberanía regulatoria a los intereses corporativos de plataformas tecnológicas extranjeras, que están sujetas a reglas a veces más estrictas en sus países de origen.

La modificación al artículo 19.12 es la condición para que las autoridades mexicanas puedan cumplir con las obligaciones y responsabilidades reforzadas que emanan de la Convención de Belém do Pará, de la jurisprudencia de la Corte Interamericana de Derechos Humanos en materia de violencia contra las mujeres y de los artículos constitucionales y fallos judiciales desarrollados a lo largo de este documento. Cuando la ausencia de jurisdicción efectiva de México sobre los datos tratados por plataformas extranjeras hace técnica o jurídicamente inaccesible la evidencia que una víctima necesita para acceder a la justicia, el tratado comercial está operando como instrumento de denegación de justicia. El problema reside en la inexistencia de obligaciones convencionales que sometan a las plataformas a la autoridad competente mexicana cuando en su territorio se producen violaciones a derechos fundamentales.

La modificación al artículo 19.16 responde a una distorsión que el texto vigente consagra con consecuencias que trascienden el comercio digital. Al prohibir el acceso al código fuente sin

establecer una excepción operativa para la auditoría por autoridad competente, el Tratado blinda los sistemas algorítmicos de las grandes plataformas frente a cualquier escrutinio institucional. Esa opacidad es la condición que hace posibles los sistemas de moderación que discriminan, los mecanismos de amplificación que viralizan contenido sexual íntimo no consentido y las decisiones automatizadas que producen daños irreversibles sin que ninguna institución del Estado pueda verificar sus criterios. México debe exigir que la distinción entre transferencia de código fuente y auditoría regulatoria con salvaguardas de confidencialidad quede incorporada expresamente al texto del Tratado. Sin esa distinción, la supervisión algorítmica es contractualmente imposible.

La modificación al artículo 19.17 es la más urgente desde la perspectiva de los derechos de las víctimas. La inmunidad irrestricta que el texto vigente otorga a las plataformas es la materialización en un instrumento de derecho internacional de un privilegio corporativo que ningún otro agente económico o jurídico posee en el ordenamiento mexicano. Un prestador de servicios digitales que obtiene ingresos publicitarios derivados de la circulación de contenido sexual íntimo no consentido, que cuenta con capacidad técnica para implementar mecanismos de detección y retiro expedito, y que no actúa frente a la denuncia de una víctima, no puede invocar la inmunidad del Tratado para eximirse de responsabilidad sin que el Estado mexicano sea cómplice de esa evasión. La inmunidad debe quedar expresamente condicionada al cumplimiento de obligaciones y responsabilidades. La viabilidad técnica y económica de esas obligaciones ha sido demostrada a lo largo de este documento.

El sustento de las tres propuestas converge en cinco dimensiones que se refuerzan mutuamente. Jurídicamente, las modificaciones son condición necesaria para que México pueda cumplir obligaciones internacionales que ya ha asumido y que no están sujetas a renegociación comercial. En el plano técnico-computacional, la viabilidad operativa de las tres medidas ha sido demostrada: la infraestructura *cloud* distribuida admite gradaciones de residencia de datos; las auditorías algorítmicas pueden realizarse sin transferir código fuente; los mecanismos de notificación y retiro expedito ya están desplegados por las propias plataformas en el mercado europeo. Académicamente, las propuestas se inscriben en el modelo regulatorio que mayor legitimidad internacional ha acumulado: el modelo de adecuación condicional del RGPD, la rendición de cuentas algorítmica del AI Act y la inmunidad condicionada del Reglamento de Servicios Digitales. Políticamente, el alineamiento entre la agenda del movimiento Ley Olimpia en América Latina, la postura regulatoria canadiense y el debate legislativo en el Congreso estadounidense sobre la reforma a la Sección 230 configura el contexto más propicio para la reforma desde la

entrada en vigor del Tratado. Económicamente, la experiencia europea refuta de manera concluyente los argumentos de desinversión: las plataformas estadounidenses operan en Europa cumpliendo obligaciones equivalentes o más exigentes que las aquí propuestas, sin que sus reportes financieros registren impactos materiales adversos.

Este documento ha buscado hacer visible que detrás de cada disposición técnica hay una decisión distributiva sobre quién asume los costos de la inacción regulatoria. En el diseño actual del Capítulo 19, ese costo lo asumen las víctimas de violencia digital, que son mayoritariamente mujeres y niñas, que no tienen voz en los procesos de negociación comercial y que no disponen de los recursos jurídicos ni económicos para litigar contra plataformas globales. Cuando una víctima reporta un contenido sexual íntimo no consentido y la plataforma no actúa, o actúa tarde, o actúa de manera opaca sin que ninguna autoridad pueda verificar sus criterios, el daño es el resultado previsible y en gran medida evitable de un marco normativo diseñado sin considerar sus derechos. Ese marco normativo tiene nombre y número de artículo. Y puede cambiarse.

México llega a la Revisión Conjunta 2026 con un cuerpo normativo interno en expansión —la Ley Olimpia, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la reforma constitucional en materia de paridad y una jurisprudencia constitucional que ha comenzado a poner atención a estas problemáticas— con el respaldo de una sociedad civil organizada y técnicamente competente, y con el contexto político-regulatorio internacional más favorable que ha existido desde la firma del Tratado. Ante esa convergencia excepcional, la pasividad negociadora sería una omisión que el Estado mexicano no puede justificar ni ante sus propias instituciones ni ante el sistema interamericano de derechos humanos.

Las modificaciones aquí propuestas son el mínimo indispensable para que el Capítulo 19 deje de operar como obstáculo al ejercicio de la soberanía regulatoria de México en materia de derechos fundamentales. Exigirlas en la Revisión 2026 es el ejercicio responsable e irreductible de la soberanía en el espacio digital, coherente con los estándares internacionales de derechos humanos a los que México se ha vinculado voluntariamente y con el interés legítimo de garantizar que sus instituciones sean capaces de proteger a las víctimas de violencia digital.

VIII. Referencias

Referencias académicas

Ackerman, J., Ardissom, R., Miranda, R. & Neubauer, D. (coords.). (2026). *La regulación de plataformas y redes: los derechos digitales a debate.* PUEDJS UNAM-Akal.

Ackerman, J. & Escamilla, A. (coords.). (2023). *La disputa por la democracia en las redes y en los medios*. PUEDJS UNAM-Akal.

Ackerman, J., Atilano, J., Aguilar, E., Miranda, R. & Pérez, P. (2023). *Decálogo de las personas usuarias de redes sociodigitales*. PUEDJS UNAM.

Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, 21(2), 245–272. https://doi.org/10.1093/jiel/jgy019

Atilano, J., Zumaya, M., Caloca, E., Espitia, D. Escobar, A. & Sánchez, M. (2024). Campañas negras y elecciones. El mercado de la desinformación en Facebook. https://x.com/PUEDJSUNAM/status/1767370065157017744

Balkin, J. M. (2018). Free speech is a triangle. *Columbia Law Review*, 118(7), 2011–2056.

Brennan Center for Justice (2025). Gobierno recopila, cada vez, más información de redes sociales. https://www.brennancenter.org/es/our-work/research-reports/gobierno-estados-unidos-recopila-mas-informacion-redes-sociales-inmigracion

Barquier, M. (2025). Australia prohíbe las redes sociales a menores: ¿solución o parche? https://dobetter.esade.edu/es/australia-prohibicion-redes-sociales-menores

Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). *The costs of data localisation: Friendly fire on economic recovery* (ECIPE Occasional Paper No. 3/2014). European Centre for International Political Economy.

Caloca, E. y Ramírez, R. (2023). Facebook: *Capitalismo socio-digital y democracias en riesgo. Lecciones para México*. PUEDJS-UNAM.

Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal,* 64(3), 677–739.

Citron, D. K., & Wittes, B. (2017). The Internet will not break: Denying bad Samaritans § 230 immunity. *Fordham Law Review*, 86(2), 401–423.

Comisión Europea (2026). Disposiciones de la Ley de Seguridad Digital. https://digital-strategy.ec.europa.eu/es/policies/digital-services-act

Cory, N. (2017). *Cross-border data flows: Where are the barriers, and what do they cost?* Information Technology and Innovation Foundation.

Cory, N., & Dascoli, L. (2021). *How barriers to cross-border data flows are spreading globally, what they cost, and how to address them*. Information Technology and Innovation

Foundation. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

Datacenters.com (2026). Mexico Data Centers Locations. https://www.datacenters.com/locations/mexico

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

Deutsche Welle (2025). La lucha contra los abusos a menores en Internet. https://www.dw.com/es/la-lucha-contra-los-abusos-a-menores-en-internet/a-71316482

Gaceta UNAM (2025). La violencia digital ha crecido exponencialmente. https://www.gaceta.unam.mx/la-violencia-digital-ha-crecido-exponencialmente/

Gao, H. (2021). *Data sovereignty and trade agreements: Three digital kingdoms*. En A. Mishra & J. Kim (Eds.), Data sovereignty: From the digital silk road to the return of the state (pp. 217–243). Oxford University Press.

Goldman, E. (2020). Why section 230 is better than the First Amendment. *Notre Dame Law Review Reflection*, 95(1), 33–46.

Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives.* Oxford University Press.

Gurumurthy, A., & Chami, N. (2022). Beyond data bodies: New directions for a feminist theory of data sovereignty. *Available at SSRN 4037321*.

Henry, N., Umbach, R., Shelby, R., Beard, G., & Given, L. M. (2026). 'It's still abuse': community attitudes and perceptions on AI-generated image-based sexual abuse. *Information, Communication & Society,* 1–21.

Hubbard, D. (2007). Everything is measurable. CIO.
https://www.cio.com/article/272044/it-organization-everything-is-measurable.html

IEEE Spectrum (2026). Data center growth. https://spectrum.ieee.org/data-center-growth

Irion, K. (2022). Algorithms off-limits? If digital trade law restricts access to source code of software then accountability will suffer. En *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22)* (pp. 1561–1570). Association for Computing Machinery. https://doi.org/10.1145/3531146.3533212

Kaminski, M. E. (2019). Binary governance: Lessons from the GDPR's approach to algorithmic accountability. *Southern California Law Review*, 92(6), 1529–1616.

Kaspersky (2026). Informe Global de Kaspersky Security Services
https://latam.kaspersky.com/enterprise-security/resources/reports/mdr-ir-analyst-reports

Keller, D. (2019). Internet platforms: Observations on speech, danger, and money. *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper, 1902.*

Klonick, K. (2018). The new governors: The people, rules, and processes governing online speech. *Harvard Law Review*, 131(6), 1598–1670.

Köchling, A., & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, 13(3), 795–848.

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

Mejias, U. A., & Couldry, N. (2024). *Data grab: The new colonialism of big tech and how to fight back*. University of Chicago Press.

Mishra, N. (2019). Building bridges: International trade law, internet governance, and the regulation of data flows. *Vanderbilt Journal of Transnational Law*, 52(2), 463–509.

Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. En *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT '19)* (pp. 220–229). Association for Computing Machinery. https://doi.org/10.1145/3287560.3287596

MOCIBA-INEGI (2026). Estadísticas a propósito del Día Internacional de la Eliminación de la Violencia contra la Mujer. https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2025/EAP_VioVSMujeres_25.pdf

Mökander, J., & Floridi, L. (2021). Ethics-based auditing to develop trustworthy AI. *Minds and Machines*, 31(2), 323–327. https://doi.org/10.1007/s11023-021-09557-8

Mordor Intelligence (2026). Mercado de centros de datos en Estados Unidos: Análisis de tamaño y participación en tendencias de crecimiento y pronósticos hasta 2029. https://www.mordorintelligence.com/es/industry-reports/united-states-data-center-market

Neubauer, D. (2025). Moderación de contenidos, desinformación y discursos de odio. El nuevo modelo autorregulatorio de Meta. *Revista Tlatelolco*. https://puedjs.unam.mx/revista_tlatelolco/moderacion-de-contenidos-desinformacion-y-discurso-de-odio-el-nuevo-modelo-autorregulatorio-de-meta/

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. En *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT '20)* (pp. 33–44). Association for Computing Machinery. https://doi.org/10.1145/3351095.3372873

Silva García, F., & GÓMEZ SÁMANO, J. (2019). El juicio de amparo frente a particulares. *Editorial Porrúa*, México, 2.

San Martín, D. (2023). Prevención algorítmica de la violencia de género: La discrecionalidad policial como decisión tecnológica. *Estudios Penales y Criminológicos*, 44, pp. 1-37.

Sunyaev, A. (2024). Cloud computing. Sunyaev, A. (2024). Internet computing. *Principles of Distributed Systems and Engineering Internet-Based Technologies*. Springer, pp. 165-209.

Suzor, N. (2019). Lawless: *The secret rules that govern our digital lives*. Cambridge University Press. (citado en §5.2.3 pero sin entrada; verificar si esta es la referencia correcta o si se trata de otro texto)

Umbach, R., Henry, N., Shelby, R., Stevens, G., & Gonzalez-Pons, K. (2026). AI-generated image-based sexual abuse: Perpetration and consumption across three regions. *Computers in Human Behavior*, 108935.

UNICEF (2025). Mantener seguros a niñas, niños y adolescentes en Internet. https://www.unicef.org/mexico/mantener-seguros-ni%C3%B1as-ni%C3%B1os-y-adolescentes-en-internet

Wang, X., Wu, Y. C., Ji, X., & Fu, H. (2024). Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. *Frontiers in Artificial Intelligence,* 7, 1320277.

Informes y documentos institucionales

ARTICLE 19 México y Centroamérica. (2020). *Posicionamientos sobre la implementación del T-MEC en materia de libertad de expresión*. https://articulo19.org/

Cámara de Diputados, Observatorio Legislativo de Asuntos Globales. (2025). *Revisión T-MEC 2026: Anatomía del proceso*. H. Cámara de Diputados.

Comisión Interamericana de Derechos Humanos. (2013). *Libertad de expresión e Internet*. Relatoría Especial para la Libertad de Expresión, Organización de los Estados Americanos.

Comisión Interamericana de Derechos Humanos. (2024). *Inclusión digital y gobernanza de contenidos en Internet*. Relatoría Especial para la Libertad de Expresión, Organización de los Estados Americanos.

Frente Nacional para la Sororidad. (2025). *Ley Olimpia LATAM: Documentos de posicionamiento sobre derechos digitales y violencia digital*. Movimiento Ley Olimpia.

ONU Mujeres. (2025a). *How AI is exacerbating technology-facilitated violence against women and girls*. United Nations Entity for Gender Equality and the Empowerment of Women.

ONU Mujeres. (2025b). *Model framework for legislation on technology-facilitated violence against women and girls*. United Nations Entity for Gender Equality and the Empowerment of Women.

Red en Defensa de los Derechos Digitales. (2022). *Análisis sobre la implementación del T-MEC en México y el caso PANAUT*. https://r3d.mx/

Red en Defensa de los Derechos Digitales. (2025, febrero 4). *Ministras Batres, Esquivel y Pérez Dayán validan la geolocalización indiscriminada de usuarias de la banca en línea.* https://r3d.mx/2025/02/04/

Jurisprudencia

SCJN – Pleno

Suprema Corte de Justicia de la Nación, Pleno. (2022, 26 de abril). *Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021 [PANAUT]* (Ministra ponente: N. L. Piña Hernández).

Tesis P. II/2014 (10a.), Pleno. (2014). Personas morales: derecho a la protección de datos equiparables a los personales [Registro digital 2005522]. *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 3, Tomo I, p. 274.

Tesis P./J. 130/2007, Pleno. (2007). Garantías individuales: razonabilidad y proporcionalidad. *Semanario Judicial de la Federación y su Gaceta*, Novena Época, Tomo XXVI, p. 8.

Tlatelolco Lab (2024). Campañas negras y elecciones: el mercado de la desinformación en Facebook. PUEDJS-UNAM. https://x.com/PUEDJSUNAM/status/1767370065157017744

Tlatelolco Lab (2024). *Decálogo de Derechos Digitales en Redes Sociales*. PUEDJS-UNAM.

SCJN – Primera Sala

Suprema Corte de Justicia de la Nación, Primera Sala. (2011, 30 de noviembre). *Amparo en Revisión 168/2011* (Ministro ponente: A. Zaldívar Lelo de Larrea).

Suprema Corte de Justicia de la Nación, Primera Sala. (2017). *Amparo en Revisión 587/2017 [Caso Ulrich Richter Morales c. Google Inc.].*

Suprema Corte de Justicia de la Nación, Primera Sala. (2023, 29 de noviembre). *Amparo Directo en Revisión 2880/2020* (Ministro ponente: A. Gutiérrez Ortiz Mena).

Suprema Corte de Justicia de la Nación, Primera Sala. (2025, 9 de julio). *Amparo en Revisión 673/2024* (Ministra ponente: A. M. Ríos Farjat).

Suprema Corte de Justicia de la Nación, Primera Sala. (2025, 13 de agosto). *Amparo en Revisión 16/2023.*

Suprema Corte de Justicia de la Nación, Primera Sala. *Amparo en Revisión 556/2022 [ARTICLE 19 c. reformas T-MEC].*

SCJN – Segunda Sala

Suprema Corte de Justicia de la Nación, Segunda Sala. (2025, 29 de enero). *Amparo en Revisión 74/2024 [R3D c. geolocalización en banca en línea].*

Corte Interamericana de Derechos Humanos

Corte Interamericana de Derechos Humanos. (2009, 16 de noviembre). *Caso González y otras ("Campo Algodonero") vs. México*. Serie C No. 205.

Corte Interamericana de Derechos Humanos. (2017, 15 de noviembre). *Medio ambiente y derechos humanos, Opinión Consultiva OC-23/17*. Serie A No. 23.

Corte Interamericana de Derechos Humanos. (2021, 26 de agosto). *Caso Bedoya Lima y otra vs. Colombia*. Serie C No. 431.

Tribunal Europeo de Derechos Humanos

Tribunal Europeo de Derechos Humanos. (2008, 2 de diciembre). K.U. c. *Finlandia,* demanda no. 2872/02.

Tribunal Europeo de Derechos Humanos, Gran Sala. (2015, 16 de junio). *Delfi AS c*. Estonia, demanda no. 64569/09.

Tribunal Europeo de Derechos Humanos. (2016, 2 de febrero). *Magyar Tartalomszolgáltatók Egyesülete (MTE) e Index.hu Zrt c. Hungría*, demanda no. 22947/13.

Tribunal de Justicia de la Unión Europea

Tribunal de Justicia de la Unión Europea, Gran Sala. (2020, 16 de julio). *Data Protection Commissioner c. Facebook Ireland Ltd y Maximillian Schrems [Schrems II]*, asunto C-311/18.

Suprema Corte de los Estados Unidos

González v. Google LLC, 598 U.S. 617 (2023).

Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

Moody v. NetChoice, LLC, 603 U.S. _____ (2024).

PUEDJS

PROGRAMA UNIVERSITARIO
DE ESTUDIOS SOBRE
DEMOCRACIA, JUSTICIA Y SOCIEDAD

475+ UNIVERSIDAD 1551 MÉXICO 2026

#LEY OLIMPIA

defensoras digitales

BMA
100 AÑOS
BARRA MEXICANA COLEGIO DE ABOGADOS