

Registro obligatorio de celulares en México y la regulación biométrica en la Unión Europea: límites, garantías y lecciones comparadas

Mandatory Cell Phone Registration in Mexico and Biometric Regulation in the European Union: Limits, Guarantees, and Comparative Lessons

Por: Alma de los Ángeles Ríos Ruíz

Resumen:

En el presente trabajo se compara el registro obligatorio de líneas móviles en México con la regulación en materia de biometría que existe en la Unión Europea, con el propósito de identificar sus límites, garantías y, sobre todo, las buenas prácticas y lecciones que podrían ser aplicables en México. A partir de un marco conceptual, se revisa la evolución normativa y jurisprudencial en ambos contextos, así como los riesgos técnicos y jurídicos relacionados con estas medidas. También se sintetiza la evidencia empírica sobre eficacia, los incidentes operativos y los costos administrativos, con el fin de proponer recomendaciones prácticas que permitan mostrar que la seguridad y la protección de derechos pueden ser compatibles cuando las políticas se diseñan bajo los principios de proporcionalidad, transparencia y supervisión efectiva.

Palabras clave: Registro de líneas móviles; biometría; protección de datos; proporcionalidad; inclusión digital; seguridad de la información.

Abstract: This paper compares the mandatory registration of mobile phone lines in Mexico with the European Union's regulatory framework on biometrics, with the aim of identifying their limitations, safeguards, and, above all, good practices and lessons that could be applicable in Mexico. Based on a conceptual framework, the study reviews the regulatory and jurisprudential developments in both contexts, as well as the technical and legal risks associated with these measures. It also synthesizes empirical evidence on effectiveness, operational incidents, and administrative costs, with the purpose of proposing practical recommendations that demonstrate how security and the protection of rights can be compatible when policies are designed according to the principles of proportionality, transparency, and effective oversight.

Keywords: Mobile line registration; biometrics; data protection; proportionality; digital inclusion and information security.



Esta obra está bajo licencia Creative Commons
Attribution-NonCommercial-ShareAlike 4.0
International (CC-BY-NC-SA 4.0)

Recepción: 11 de marzo de 2026

Aceptación: 26 de mayo de 2026

Publicación: 9 de septiembre de 2026



En los últimos años, han tenido lugar dos procesos regulatorios distintos pero convergentes, por un lado, la implementación en México de un registro obligatorio de líneas móviles orientado a vincular cada número con la identidad de su titular, y por otro, la consolidación en la Unión Europea de un marco jurídico robusto en materia de tratamiento de datos biométricos, sistemas de inteligencia artificial para la identificación y biométrica remota, así como el establecimiento de obligaciones de transparencia y evaluación de riesgos. Se trata de dos fenómenos que han puesto sobre la mesa importantes cuestiones sobre proporcionalidad, seguridad pública, protección de datos e incluso garantías procesales.

En el caso de México, la medida vigente que se publicó en el año 2025 y puesta en operación en enero de 2026, exige que las líneas móviles que se encuentren activas sean vinculadas a un identificador oficial que puede ser la Clave Única de Registro de Población (CURP), la credencial emitida por el Instituto Nacional Electoral (INE) o el pasaporte, según el caso, la medida otorga a los operadores la responsabilidad de validar y custodiar la información, además de establecer plazos y sanciones operativas, como la suspensión del servicio de telefonía cuando no se cumpla con el registro dentro del plazo establecido.

Dicha medida constituye una respuesta administrativa ante la utilización de números

anónimos que pueden estar relacionados con delitos de extorsión telefónica, principalmente. Sin embargo, es necesario analizar su verdadero alcance y, sobre todo la eficacia de esta medida para la prevención del delito, considerando también los riesgos para la seguridad de la información y para la inclusión digital y que podría traer aparejados.

Para entender este tema con mayor claridad, resulta imprescindible distinguir este esquema actual del Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT) que fue un proyecto anterior en el que se planteó la recolección de datos biométricos masivos, como huellas, iris y reconocimiento facial, el PANAUT fue declarado inconstitucional por la Suprema Corte de Justicia de la Nación en 2022, al considerar que se vulneraba el derecho a la privacidad y que la medida no era proporcional frente a los fines perseguidos (Redacción, 2026).

Esta sentencia constituye un precedente jurídico clave, pues estableció que no podía exigirse de manera obligatoria la entrega de datos biométricos al Estado mexicano como condición para acceder al servicio de telefonía móvil. Sin embargo, es importante aclarar que esta decisión no impide al Estado regular la identificación administrativa de las líneas mediante documentos oficiales.

Por su parte, en el plano europeo, el Reglamento General de Protección de Datos (GDPR), junto con las directrices del Comité Europeo de Protección de Datos (EDPB, por

sus siglas en inglés) han ido definiendo paulatinamente el tratamiento de los datos biométricos como una categoría especialmente sensible.

Esto implica que su uso requiere bases jurídicas sólidas, medidas de minimización de datos y, en determinados casos, evaluaciones de impacto, toda vez que su procesamiento puede representar un alto riesgo para vulneración de derechos fundamentales. Además, en el año 2024 la Unión Europea aprobó el Reglamento de Inteligencia Artificial (IA Act), instrumento que introdujo un enfoque basado en niveles de riesgo y que prohíbe, salvo excepciones muy limitadas, determinados usos de la identificación biométrica remota en tiempo real en espacios públicos.

evaluación y la supervisión para los sistemas de Inteligencia Artificial. En conjunto, estas normas configuran un marco preventivo y restrictivo frente a la centralización de datos biométricos y la vigilancia masiva.

Como se observa, la regulación de la telefonía móvil involucra aspectos que van más allá de la seguridad pública o la operatividad de investigaciones penales, también plantea cuestiones sensibles relacionadas con la recolección, el uso y la custodia de datos personales. De hecho, la biometría está ligada a temas de privacidad, autonomía informativa e inclusión digital, especialmente cuando se trata de poblaciones vulnerables, como las personas migrantes o aquellas que no cuentan con su documentación actualizada, así como las personas usuarias de servicios

de telefonía móvil bajo un esquema de prepago.

En este sentido, para México, la experiencia europea sobre los límites de la identificación biométrica puede servir como referente para analizar salvaguardas tanto técnicas como procesales. Ante esto surge la necesidad de un enfoque integral que combine análisis jurídico, técnico y también socioeconómico,

toda vez que las decisiones sobre registros y biometría no son únicamente administrativas, sino que también determinan la forma en que



Imagen generada con Chat GPT (2026)

Asimismo, establece obligaciones relacionadas con la transparencia, la

se gestionan y protegen los datos personales, con posibles efectos sobre distintos grupos de la población y sobre sus derechos fundamentales.

Por ello, este análisis tiene como objetivo ofrecer recomendaciones normativas y de diseño institucional que prioricen la minimización de datos, la transparencia y la evaluación de impacto, para ello, se toman como referencia las salvaguardas desarrolladas por el EDPB y las lecciones derivadas de la experiencia mexicana reciente.

I. PANORAMA NORMATIVO Y JURISPRUDENCIAL COMPARADO

En México, en el marco administrativo más reciente sobre identificación de líneas móviles, se publicaron los Lineamientos para la Identificación de Líneas Telefónicas Móviles, aprobados por la Comisión Reguladora de Telecomunicaciones (Diario Oficial de la Federación, 2025). Estos lineamientos establecen una serie de obligaciones tanto para concesionarios como comercializadoras respecto a la vinculación de las líneas telefónicas con identificadores oficiales, los plazos de validación y las sanciones operativas.

Dicho esquema, resulta muy similar al PANAUT de 2022, que también proponía la recolección masiva de datos biométricos. Como ya se señaló, este proyecto fue declarado inconstitucional por la Suprema Corte de Justicia de la Nación, al considerar que vulneraba derechos de privacidad, y que

la medida no era proporcional a los fines perseguidos. Este precedente es muy importante, ya que, si bien no prohibió la identificación administrativa de líneas mediante documentos oficiales, sí estableció límites constitucionales frente a la exigencia obligatoria de datos biométricos por parte del Estado como condición para acceder a servicios de telecomunicaciones.

Por ello, resulta necesario reflexionar sobre aspectos clave como la proporcionalidad, razonabilidad y protección de datos personales cuando se implementan medidas de identificación masiva.

Tal es el caso del GDPR de la Unión (European Union, 2016), donde se consagra, en términos generales, el tratamiento de datos biométricos como una categoría especialmente protegida, a través de una serie de obligaciones que, en conjunto constituyen un estándar jurídico de referencia para cualquier tipo de regulación que implique identificación biométrica. De manera más específica, el EDPB (European Data Protection Board, 2023) ha desarrollado directrices sobre biometría y reconocimiento facial, incluso cuando se utilizan en el ámbito policial o de justicia.

En ellas se ha hecho hincapié en la incorporación de medidas para la mitigar los riesgos, garantizar la transparencia y fortalecer la supervisión coordinada entre las diversas autoridades en materia de protección de datos. Estas directrices sirven como guía para la interpretación técnica y aplicación

práctica del GDPR en materia biométrica, por lo que complementan sus disposiciones.

marco preventivo y restrictivo sobre biometría que combina el GDPR, la interpretación técnica del EDPB y el AI Act para priorizar la minimización de datos, la evaluación de impacto y la supervisión independiente. Se trata, por tanto, de dos enfoques normativos que permiten analizar, desde una perspectiva comparada, la compatibilidad entre la seguridad pública y la protección de los derechos como objetivos que pueden existir.

Imagen generada con Chat GPT (2026)



Otro instrumento más que contribuye a este propósito es el AI Act de 2024 (EU Artificial Intelligence Act, 2025), que introdujo un enfoque basado en niveles de riesgo para sistemas de inteligencia artificial. En este instrumento se establecen tanto prohibiciones como restricciones y, lo más importante, obligaciones de evaluación, transparencia y supervisión para aquellos sistemas que se consideran de alto riesgo.

Lo anterior nos sitúa ante un doble panorama: por un lado, el caso mexicano, donde se ha optado por un mecanismo administrativo de identificación de líneas telefónicas que delega funciones operativas a los operadores, con un antecedente claro de inconstitucionalidad en el que se establecieron límites a la exigencia de biometría obligatoria. La Unión Europea, en cambio, paulatinamente ha consolidado un

II. RIESGOS, LÍMITES, GARANTÍAS JURÍDICAS Y TÉCNICAS

La exigencia por parte de cualquier Estado o gobierno de vincular líneas móviles a identificadores oficiales puede generar riesgos para la privacidad individual, sobre todo si los fines, plazos o fundamentos jurídicos no están claramente delimitados. En el caso mexicano, como ya se ha señalado, existe un criterio del máximo tribunal que establece que recolección masiva de datos, entre ellos los biométricos, puede representar una injerencia desproporcionada en la esfera privada de los ciudadanos. A partir de este criterio, queda clara la necesidad de respetar los principios de necesidad y proporcionalidad.

Ahora bien, desde una perspectiva técnica, la centralización de identificadores o la

acumulación de datos personales sensibles incrementa la superficie de ataque, lo que aumenta la probabilidad de brechas de seguridad, reidentificación de las personas, así como de usos secundarios no previstos. Por ello, las medidas de protección, como mínimo, deben incluir cifrado de los datos tanto en tránsito como en reposo, segregación de funciones, generación de registros de acceso y políticas restrictivas de retención de datos que reduzcan la posibilidad de una exposición masiva de esta información. Estas medidas son congruentes con los principios de protección de datos establecidos en el GDPR (European Union, 2016), en particular, con los principios de confidencialidad del tratamiento e integridad.

Lo anterior se justifica porque el tratamiento de datos biométricos entraña un límite jurídico adicional, de ahí que el GDPR los clasifique como una categoría especial de datos personales y exija una base jurídica sólida, así como garantías reforzadas de minimización de datos y limitación de la finalidad.

También contempla la realización de evaluaciones de impacto cuando se identifique que el tratamiento implica o puede implicar un alto riesgo para los derechos, deberes y libertades fundamentales de las personas. Esto permite destacar un aspecto fundamental: cualquier política que pretenda incorporar biometría o ampliar la identificación automatizada deberá someterse previamente a una evaluación de impacto, que permita verificar la existencia de controles y garantías jurídicas adecuadas.

De igual forma, resultan determinantes las garantías tanto procesales como de supervisión, por lo que es imprescindible contar con un órgano administrativo independiente con facultades de supervisión, investigación y, sobre todo, sanción, que permita prevenir abusos y, en caso de que se presenten, corregir oportunamente los posibles errores o incumplimientos.

Por ello, puede identificarse un punto de coincidencia entre la decisión de la SCJN respecto del PANAUT y el marco europeo del GDPR: para ambos, tanto la supervisión efectiva como la posibilidad de contar con recursos judiciales o administrativos son condiciones indispensables para evitar que las medidas de identificación se conviertan en mecanismos de vigilancia masiva sin controles ni contrapesos.

Otro tema de gran relevancia tiene que ver con aspectos sensibles de exclusión y acceso, toda vez que la obligación de vincular líneas con identificadores oficiales puede generar efectos negativos sobre grupos en situación de vulnerabilidad, como las personas migrantes, quienes no cuentan con documentación actualizada e incluso personas usuarias del esquema prepago. Esto evidencia la necesidad de diseñar mecanismos alternativos, así como excepciones razonadas.

Desde una perspectiva de proporcionalidad jurídica, las políticas deben contemplar salvaguardas que eviten la desconexión digital o estigmatización y, en caso de presentar

algún problema, establecer procedimientos de subsanación accesibles para quienes enfrenten errores de verificación (Suprema Corte de Justicia de la Nación, 2022). Estos posibles efectos sobre distintos grupos de la población deben ponderarse frente a los fines de seguridad pública que se persiguen.

Es así que, ante la presencia de sesgos técnicos y jurídicos, resulta imprescindible incorporar desde el diseño medidas tendentes a mitigar estos riesgos, como son la minimización de datos, la pseudonimización, la limitación temporal de la conservación, las auditorías independientes e incluso establecer la obligación de realizar y publicar evaluaciones de impacto en materia de protección de datos. Estas medidas deben considerarse requisitos mínimos para garantizar que el tratamiento de datos sensibles se realice sin controles previos y de una manera transparente.

Si se combinan límites jurídicos claros sobre las prohibiciones o restricciones aplicables a la biometría obligatoria, la exigencia de proporcionalidad y bases jurídicas claras, junto con garantías técnicas de cifrado, segregación, auditoría y mecanismos de supervisión independiente, se puede avanzar hacia un modelo que permita compatibilizar los objetivos legítimos de seguridad pública con la protección de los derechos fundamentales, sin tener que renunciar a controles democráticos.

III. EVIDENCIA EMPÍRICA Y EFECTOS OBSERVADOS

En términos generales, la evidencia sobre la eficacia de los registros obligatorios de tarjetas SIM para reducir delitos como la extorsión telefónica es limitada y heterogénea, particularmente porque la identificación de usuarios puede facilitar investigaciones específicas. Sin embargo, se reconoce que la reducción sostenida de un delito depende de factores institucionales, por lo que no existe un consenso empírico que atribuya de forma directa y exclusiva la disminución delictiva a la mera existencia de un padrón.

De hecho, lo que sí se ha observado como un común denominador es la documentación de efectos adversos por parte de organizaciones de derechos digitales y diversos análisis académicos sobre los temas ya señalados: exclusión de poblaciones vulnerables, cargas administrativas tanto para usuarios como para operadores y riesgos de usos secundarios de los datos que van más allá de su finalidad original. Estos riesgos son particularmente relevantes en contextos con alta informalidad documental. La obligatoriedad, cuando no está acompañada de mecanismos alternativos, puede traducirse en desconexión digital, lo que genera costos sociales que deben ponderarse frente a los beneficios en materia de seguridad.

Actualmente los incidentes operativos y riesgos de seguridad informática asociados a la concentración de identificadores han sido documentados por agencias de ciberseguridad, que advierten que la exposición de datos biométricos e

identificadores únicos tiene efectos duraderos porque estos datos no son fácilmente reemplazables.

Por ejemplo, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) (ENISA, s.f.) ha enfatizado la necesidad de desarrollar controles criptográficos, segregación de funciones, auditorías y políticas de retención estrictas para mitigar estos riesgos.

En el ámbito europeo, la evidencia sobre la utilidad de las salvaguardas regulatorias muestra cómo aquellos marcos normativos que exigen evaluaciones de impacto, transparencia y supervisión independiente, pueden ayudar a identificar y mitigar riesgos antes del despliegue de sistemas biométricos. En este sentido, el texto consolidado del GDPR constituye una de las principales referencias normativas respecto de estas obligaciones.

Asimismo, tanto las directrices como los documentos técnicos del European Data Protection Board (EDPB) y la propia Comisión Europea muestran cómo la transparencia y el establecimiento de medidas de mitigación puede contribuir a detectar riesgos técnico-sociales, entre los que destacan los sesgos en algoritmos, los errores de verificación y los

impactos en grupos vulnerables, desde antes de su implementación. Como parte del seguimiento, también pueden surgir otros desafíos, relacionados con la uniformidad en la capacidad de supervisión de algunos Estados miembros.

En conjunto, estas medidas han contribuido a establecer límites y controles para el



Imagen generada con Chat GPT (2026)

reconocimiento facial u otras técnicas biométricas en contextos sensibles (European Data Protection Board, 2023).

Un aspecto que también debe considerarse son los costos administrativos y operativos, porque se trata de inversiones significativas en infraestructura de verificación, sistemas de custodia, atención a reclamaciones y campañas informativas. De ahí la importancia de contar con un esquema claro de financiamiento o compensación, evitando que la carga recaiga exclusivamente en operadores o usuarios, como ocurre con

frecuencia. De lo contrario, los costos pueden afectar la calidad de la verificación y la cobertura del servicio. Por ello, se deben evaluar antes y después de su implementación los costos frente a los beneficios en seguridad.

En general, se puede afirmar que los registros obligatorios aportan herramientas útiles para investigaciones puntuales, pero no constituyen por sí solos una solución definitiva para la prevención del delito. Sus efectos dependen del diseño institucional, de las salvaguardas técnicas y jurídicas implementadas, así como de los mecanismos de supervisión y evaluación que permitan medir sus resultados y ajustar políticas con base en evidencia verificable.

IV. LECCIONES COMPARADAS Y RECOMENDACIONES POLÍTICAS

Con todo lo analizado hasta ahora, como primera lección se puede señalar la importancia de priorizar la minimización de datos y la evaluación previa de riesgos, esto significa que, antes de imponer obligaciones de identificación masiva, deben realizarse evaluaciones de impacto en materia de protección de datos para identificar riesgos técnicos, jurídicos o sociales, y diseñar, a partir de sus resultados, medidas de mitigación proporcionales a la finalidad de seguridad pública.

El enfoque preventivo es un pilar del marco europeo que se deriva directamente de las obligaciones contenidas en el GDPR, que establece requisitos específicos para aquellos tratamientos que entrañen un alto riesgo para los derechos, y libertades de las personas (European Union, 2016).

La siguiente lección es que establecer de manera anticipada límites claros al uso de tecnologías biométricas que pueden representar un alto riesgo para los derechos fundamentales, esto representa una medida preventiva ante la posibilidad de una vigilancia masiva.

En la UE se han incorporado estas limitaciones en su marco regulatorio reciente, así como en las directrices del EDPB sobre reconocimiento facial, con el propósito de que cualquier excepción se justifique legalmente, sea proporcional y cuente con controles estrictos, esto muestra cómo un marco basado en niveles de riesgo puede permitir usos legítimos de la tecnología sin necesidad de normalizar la centralización biométrica (European Union, 2024).

Un elemento indispensable que se observa en la experiencia analizada es que las salvaguardas técnicas son inseparables de las garantías jurídicas, en conjunto, un cifrado adecuado en tránsito y en reposo, estrategias de pseudonimización, segregación de funciones, registros de acceso y auditorías independientes pueden contribuir a reducir el impacto y la posibilidad de brechas de

seguridad. Se trata de medidas mínimas que deberían estar presentes en cualquier base de datos que contenga identificadores sensibles. Además, estas medidas deben incorporarse desde el diseño de los sistemas y no únicamente después de que se presenten incidentes.

Como una aportación desde el contexto mexicano, otra lección es la necesidad de respetar los límites constitucionales y considerar los posibles efectos sobre distintos grupos de la población. En su momento, la SCJN estableció límites constitucionales relevantes para el diseño de medidas de identificación que pudieran afectar derechos y libertades fundamentales.

Respecto a los diseños regulatorios, también resulta necesario incorporar mecanismos efectivos de supervisión independiente y transparencia operativa. Por ello, es necesario que exista una autoridad dotada de facultades de inspección, auditoría y sanción, a la par que se publiquen métricas relacionadas con los incidentes de seguridad, el número de verificaciones, las causas de suspensión del servicio e indicadores de exclusión que permitan desarrollar una evaluación posterior de la eficacia y de los efectos colaterales de cualquier política en la materia.

De forma concreta, es necesario priorizar los siguientes aspectos: limitar los datos recabados a lo estrictamente necesario, evitando la recolección biométrica obligatoria



Imagen generada con Chat GPT (2026)

salvo que se cuente con una base legal clara y excepcional; exigir evaluaciones de impacto en materia de protección de datos como lo contempla el RGPD, que sean realizadas y, cuando corresponda publicadas con anterioridad al despliegue de cualquier iniciativa, programa o plan gubernamental; establecer tanto vías alternativas como excepciones razonadas para evitar la exclusión de personas sin la documentación requerida; crear mecanismos claros de atención y reclamación, así como autoridades de supervisión independiente que cuenten con capacidad sancionadora y mecanismos de coordinación interinstitucional entre las autoridades de telecomunicaciones, seguridad pública y protección de datos. Asimismo, deberían publicarse informes

periódicos sobre el funcionamiento y los resultados de estas medidas. Se trata de prácticas que ya se contemplan en distintos instrumentos del marco regulatorio europeo.

Una lección transversal incluso es que toda política pública debe ser evaluable y reversible, es decir, antes de institucionalizar un registro obligatorio, es fundamental contar con un plan de monitoreo independiente, con indicadores específicos sobre su impacto en la exclusión e incidentes de seguridad, que permitan modificar o, en caso necesario suspender la medida si los costos para derechos o la seguridad superan los beneficios.

No se trata solo de pensar en la reducción de ciertos fraudes, también se debe cuidar que no surjan mercados paralelos ante determinadas barreras de acceso. Por ello, se deben prever plazos razonables, puntos de atención, mecanismos de verificación comunitaria y excepciones que garanticen la continuidad del servicio mientras se regularizan determinadas situaciones particulares.

Es necesario reconocer que la confianza pública y la legitimidad de los registros están ligadas a la claridad sobre sus finalidades, plazos de retención, accesos autorizados y mecanismos de protección y reparación disponibles para las personas afectadas.

Finalmente, la experiencia de la UE muestra que su marco normativo y sus herramientas técnicas que sirven como referencia para el diseño de salvaguardas en contextos con

menor tradición de protección de datos, siempre que estas se adapten a las condiciones jurídicas, institucionales y sociales de cada país.

CONCLUSIONES

Es un hecho que la regulación de la vinculación obligatoria de líneas móviles, así como la normativa sobre biometría, plantean un dilema común de carácter estructural; conciliar objetivos legítimos de seguridad con la protección de los derechos fundamentales, de tal suerte que, si una política pretende ser eficaz, necesita priorizar la minimización de datos, demostrar su necesidad y plantear alternativas menos intrusivas antes de imponer medidas masivas.

La regulación europea en la materia da muestra que un enfoque basado en la clasificación por riesgo, prohibiciones claras y obligaciones de transparencia, cuando estos elementos actúan en conjunto, pueden reducir la probabilidad de que se lleve a cabo una vigilancia masiva y facilitar la supervisión técnica y jurídica. En el caso de México, al igual que en otras jurisdicciones, es posible adoptar y adaptar esos principios, respetando las características y necesidades de sus propios contextos institucionales.

Respecto a la seguridad de los sistemas, ésta depende tanto de buenas prácticas de ingeniería, como el cifrado, la pseudonimización o la separación de funciones, como de auditorías externas y pruebas demográficas que permitan detectar sesgos, incluidos aquellos que puedan afectar

de manera diferenciada a distintos grupos de la población. Todo ello, resulta necesario para evitar que cualquier beneficio operativo sea anulado por filtraciones de información, errores discriminatorios o pérdida de confianza pública.

Las políticas de registro deben ser diseñadas de manera evaluable y reversible, mediante los pilotos que puedan ser evaluados, indicadores de éxito, mecanismos de corrección y, sobre todo, cláusulas de reversibilidad en caso de que las afectaciones o daños superen los beneficios. En este sentido, la evaluación continua resulta imprescindible para determinar si la medida cumple con sus objetivos y si sus costos sociales y jurídicos son razonables.

Otro tema no menos importante se relaciona con la inclusión social, que debe constituir un criterio central de la regulación y no un elemento adicional. Esto implica incorporar vías alternativas de verificación, plazos razonables y atención prioritaria a los grupos vulnerables, para evitar situaciones de exclusión digital.

En suma, la lección central es que la seguridad y la protección de los derechos no son objetivos necesariamente antagónicos cuando una regulación es diseñada bajo los principios de proporcionalidad, transparencia y control independiente. Además, las decisiones gubernamentales relacionadas con registros y biometría deben apoyarse en evidencia, controles técnicos y, sobre todo, marcos institucionales capaces de detectar y

corregir riesgos, así como de proteger los derechos de la ciudadanía.

REFERENCIAS

- Diario Oficial de la Federación. (2025, 16 de julio). Acuerdo mediante el cual el Pleno de la Comisión Reguladora de Telecomunicaciones aprueba y emite los Lineamientos para la Identificación de Líneas Telefónicas Móviles. https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5775677
- ENISA. (s.f.). Publicaciones. <https://www.enisa.europa.eu/publications>
- EU Artificial Intelligence Act. (2025, 02 de febrero). Artículo 5: Prácticas de IA prohibidas. <https://artificialintelligenceact.eu/article/5/>
- European Data Protection Board. (2023, 17 de mayo). Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley. https://www.edpb.europa.eu/our-work-tools/our-documents/topic/biometrics_en
- European Union. (2016, 04 de mayo). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- European Union. (2024, 13 de junio). (Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre la inteligencia artificial y se modifican

los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Ley de Inteligencia Artificial). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Redacción. (2026, 27 de enero). Suprema Corte declara inconstitucional el registro obligatorio de líneas telefónicas. <https://atiempo.mx/sucesos/suprema-corte-declara-inconstitucional-el-registro->

<obligatorio-de-lineas-telefonicas/#:~:text=%20La%20Suprema%20Corte%20de%20Justicia%20de,privacidad%20y%20la%20protecci%C3%B3n%20de%20datos%20personales>

Suprema Corte de Justicia de la Nación. (2022, 25 de abril). Pleno de la SCJN Declara Inconstitucional el Sistema Normativo que crea el Padrón Nacional de Usuarios de Telefonía Móvil. <https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=6857>



Dra. Alma de los Ángeles Ríos Ruiz
Facultad de Derecho
Universidad Autónoma del Estado de México

 <https://ror.org/01tmp8f25>
 <https://orcid.org/0000-0003-3939-0600>
 alma_rios_r@hotmail.com

