

► Legal challenges on the digital era:
development of AI and data protection

DESAFÍOS NORMATIVOS EN LA ERA DIGITAL: DESARROLLO DE IA Y PROTECCIÓN DE DATOS

Por:  Juan Manuel Rivera Vélez

Rivera Vélez, J. M. (2025). Desafíos normativos en la era digital: desarrollo de IA y protección de datos. *Entorno UDLAP*, 24
↩ **Recibido:** 10 de septiembre de 2024 ✓ **Aceptado:** 18 de julio de 2025

◆ RESUMEN

Este estudio se centra en la relación entre la protección de datos personales y el desarrollo de la inteligencia artificial (IA), dentro del marco jurídico mexicano e internacional. Se analiza cómo las regulaciones actuales pueden ser aplicadas a la IA para priorizar la protección de los derechos individuales, sin obstaculizar el avance tecnológico y social que la IA representa. El análisis proporciona una evaluación de la aplicación actual de las normativas en el campo de la IA y emite recomendaciones para futuras leyes especializadas.

Este equilibrio es crucial para garantizar que la tecnología avance de manera ética y responsable, respetando al mismo tiempo los derechos fundamentales de las personas. Las conclusiones obtenidas mediante este análisis son de gran importancia: no solo proporcionan una evaluación de la aplicación actual de las normativas, sino que ofrecen una visión prospectiva. De esta manera, se espera que este estudio sirva como un recurso para los legisladores, los desarrolladores de IA y todas las

partes interesadas en este campo en constante evolución.

◆ PALABRAS CLAVE

Privacidad · Regulación · Seguridad · Ética · Desarrollo tecnológico · Inteligencia artificial · Derechos humanos · GDPR · Datos personales

◆ ABSTRACT

This study focuses on the relationship between personal data protection and the development of artificial intelligence (AI), within the framework of both Mexican and international law. It analyzes how current regulations can be applied to AI in order to prioritize the protection of individual rights without hindering the technological and social progress that AI represents. The analysis provides an assessment of the current implementation of legal frameworks in the AI field and offers recommendations for future specific legislation.

Striking this balance is crucial to ensure that technological advancement proceeds in





an ethical and responsible manner while upholding the fundamental rights of individuals. The findings from this analysis are highly significant: they not only provide an evaluation of the current application of regulations, but also offer a forward-looking perspective. In this way, the study aims to serve as a resource for lawmakers, AI developers, and all stakeholders involved in this ever-evolving field.

◆ KEYWORDS

**Privacy • Regulation • Security • Ethics
• Technological development • Artificial
intelligence • Human rights • GDPR
• Personal data**

◆ INTRODUCCIÓN

Durante la última década, la inteligencia artificial ha irrumpido en el escenario mundial, y ha transformado radicalmente nuestra percepción sobre lo que somos capaces de crear como humanidad. El hito de haber innovado mediante una tecnología capaz de replicar la creación más impresionante de la naturaleza (el cerebro humano) es prueba irrefutable de la evolución tecnológica del ser humano. Hace poco menos de un siglo esta tecnología parecía inalcanzable; propia de cuentos y pesadillas reflejadas en diversas expresiones literarias, plásticas y multimedia. Hoy, es una realidad palpable en nuestra sociedad. Debido a este avance tecnológico que parece desafiar leyes preexistentes como la Ley de Moore, es inevitable cuestionarse si aún existe la posibilidad de construir un marco jurídico eficiente para regular la IA en el corto plazo, o si este desafío resulta demasiado complejo para abordarlo en tan poco tiempo. Por lo tanto, tras la publicación de una ley especializada en materia de IA realizada por la Unión Europea (UE) y los esfuerzos recientes planteados por el Poder Legislativo mexicano, este análisis tendrá como objetivo estudiar el marco jurídico existente y su desempeño en la protección de derechos ante la revolución tecnológica actual. Asimismo, concluir sobre qué deben contener las próximas actualizaciones del marco jurídico, de manera que estén completamente preparadas para afrontar estos desafíos.

Dado que el concepto de marco jurídico se refiere a todo el conjunto de leyes que rigen la

sociedad y engloba prácticamente todos los aspectos de esta, resulta complicado enfocar este trabajo en el desafío de adaptar todo el marco jurídico al avance de la IA. Lo que sí resulta viable como parte del objetivo de este trabajo es realizar un análisis centrado en un aspecto del marco jurídico: el derecho a la autodeterminación informativa de la persona en el contexto de su utilización por la IA. El propósito es establecer soluciones y recomendaciones tangibles que garanticen el cumplimiento de estos derechos por parte de los desarrolladores, sin perder de vista la importancia del desarrollo y la competitividad a través del análisis de la regulación existente. El primer paso en este proceso debe ser la definición del sujeto principal del estudio.

Es imposible comprender el concepto del derecho a la autodeterminación informativa de la persona —estrechamente vinculado con el régimen de la protección de datos personales— sin haber definido previamente el derecho a la privacidad. Este derecho se encuentra reconocido en múltiples tratados internacionales vinculantes para la legislación mexicana y debe comprenderse como el derecho personal para controlar todo lo relacionado con la propia información personal (Estrada, s. f.), lo cual incluye toda la información vinculada con una persona física, así como la capacidad de decidir quiénes pueden acceder a dicho conocimiento, incluidos el Gobierno y las empresas. Esta información corresponde a los datos personales, términos que, en esencia, son intercambiables. El concepto de datos personales se divide en dos categorías: datos personales sensibles y no sensibles. La diferencia radica en que el primer tipo corresponde a toda la información personal cuyo uso indebido pueda ocasionar cualquier tipo de discriminación o daño directo hacia el titular, mientras que el segundo tipo corresponde a toda la información de una persona que no puede ser calificada como sensible y pueda ser utilizada para su distinción (Sollange, 2018).

Este derecho se encuentra regulado y protegido dentro del marco jurídico mexicano interno, mediante la constitución en su artículo 16°, párrafo segundo, el cual contiene los famosos



derechos de acceso, rectificación, cancelación y oposición (ARCO), sus leyes reglamentarias correspondientes, la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados (LGPDPPDSO) y la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP). La importancia de la protección a este derecho radica en evitar que esta información sea tratada tanto por sujetos obligados como por los particulares sin autorización y de manera arbitraria, sin dejar de lado la importancia de transmitirla para el provecho de los particulares, tomando en cuenta el beneficio económico y el progreso tecnológico que los datos personales representan en la sociedad de *big data* (Solange, 2018). Las ventajas que la información personal otorga en el ámbito económico y tecnológico se pueden observar de manera directa con el desarrollo y aplicación de la IA. La inteligencia artificial, como todo sistema dinámico, se basa en gran medida en el acceso a grandes cantidades de datos personales para entrenar algoritmos y mejorar su capacidad de análisis y predicción (Visual Storytelling Team y Murgia, 2023), lo que produce de manera directa un beneficio económico y, al mismo tiempo, contribuye al desarrollo tecnológico, aspecto que se analizará posteriormente.

Regresando a la importancia de permitir el tratamiento de los datos personales en el marco de estas arquitecturas, es imperativo mencionar que debe realizarse siempre de manera leal por parte de los responsables y encargados, en beneficio de los distintos particulares. Además, debe hacerse con fines legales y de manera clara; es decir, la información no debe ser utilizada con propósitos distintos a aquellos para los que la persona otorgó su consentimiento inicialmente. Una vez realizado el tratamiento, los responsables y encargados —e incluso algunos terceros en contextos donde hay servicios de nube, por ejemplo—, ahora quedan obligados a proteger los datos mediante medidas de seguridad razonables y adecuadas, a fin de evitar cualquier acceso no autorizado por parte del titular.

En la teoría y en la práctica, es común encontrar abusos de lenguaje asociados con el uso excesivo y, en muchas ocasiones, inapropiado de términos como «uso», «empleo»,

«transmisiones», entre otros, con los cuales se busca crear o eximir el cumplimiento de ciertas obligaciones, principalmente en contextos de tratamientos automatizados que involucran diversas tecnologías, entre las que se encuentra la IA. Por definición legal, el tratamiento de datos se debe entender como cualquier tipo de operación realizada por los particulares en su posesión que genere su uso práctico, aprovechamiento, almacenamiento, transferencia o divulgación (Domínguez, 2004). En palabras más sencillas, el tratamiento de datos implica cualquier actividad que se realice con la información, desde su recopilación inicial hasta su eventual utilización o transmisión para diferentes fines, ya sean comerciales, administrativos o de otra índole.

El último paso antes de avanzar hacia la exposición del marco teórico es definir adecuadamente el concepto de la IA. Esta tecnología puede entenderse de diferentes formas debido a que se manifiesta en múltiples presentaciones y cumple con distintos propósitos: desde la capacidad de entender y ser capaces de generar textos complejos, hasta la creación de obras de arte en constante transformación, cuyo cambio ocurre cada segundo durante un periodo indefinido. En esencia, la IA tiene aplicaciones infinitas (McCarthy, 2007).

Primordialmente, la IA busca emular el pensamiento humano y la capacidad de aprendizaje para automatizar procesos y mejorar la eficiencia en diversas áreas e industrias. Los sistemas de IA pueden aprender, reconocer patrones, tomar decisiones, resolver problemas y adaptarse a nuevas situaciones, todo ello con poca o nula intervención humana directa. El desarrollo de la IA es un proceso iterativo y multifacético que comienza con la recopilación de datos relevantes. Estos registros son la base fundamental para el entrenamiento de los algoritmos de IA. Posteriormente, se selecciona y entrena el modelo de IA más adecuado para la tarea específica que se desea realizar, ajustando sus parámetros y optimizando su rendimiento mediante el uso de los datos recopilados (Boucher, 2020).

Una vez entrenado el modelo, se evalúa y valida su rendimiento, recurriendo a grupos de datos de prueba separados que pueden incluir



PRIMORDIALMENTE, LA IA BUSCA EMULAR EL PENSAMIENTO HUMANO Y LA CAPACIDAD DE APRENDIZAJE PARA AUTOMATIZAR PROCESOS Y MEJORAR LA EFICIENCIA EN DIVERSAS ÁREAS E INDUSTRIAS. LOS SISTEMAS DE IA PUEDEN APRENDER, RECONOCER PATRONES, TOMAR DECISIONES, RESOLVER PROBLEMAS Y ADAPTARSE A NUEVAS SITUACIONES, TODO ELLO CON POCA O NULA INTERVENCIÓN HUMANA DIRECTA.

registros sintéticos. Esto asegura que el modelo pueda generalizar bien los datos nuevos y no vistos. Finalmente, una vez validado, el modelo se despliega en un entorno de producción donde puede realizar la tarea necesaria en tiempo real. Un monitoreo continuo garantiza la eficacia del modelo y permite realizar ajustes y actualizaciones según sea necesario. Este proceso riguroso es fundamental para el desarrollo exitoso de la IA y su implementación en diversos campos y aplicaciones.

En las siguientes secciones, se expondrá el marco teórico relevante para abordar el desarrollo de la inteligencia artificial en concordancia con el marco jurídico establecido. Este enfoque teórico servirá como base de la discusión para saber cómo diseñar y aplicar sistemas de IA de manera ética y legalmente conforme.

◆ METODOLOGÍA

Principios legales relacionados con la protección de datos personales

Para que el tratamiento de datos personales sea legítimo en cualquier operación, es necesario atender los principios que rigen su recolección y uso. Estos principios están establecidos en las regulaciones correspondientes, particularmente en el artículo 5 de nuestra LFPDPPP, el cual establece lo siguiente: «el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales». Estos principios, que pueden representar obstáculos para el desarrollo de la inteligencia artificial, constituyen al mismo tiempo garantías del derecho a la autodeterminación informativa de las personas. Se conforman de la manera que a continuación se describe.

Inicialmente, es fundamental considerar el consentimiento, ya que representa uno de los aspectos más importantes cuando una institución o persona desea recolectar datos personales. En la doctrina jurídica, el consentimiento es definido como el acuerdo de voluntades respecto un objeto en común (Martínez, 1991); en este caso, una persona física acuerda con otra —ya sea física o moral— el traspaso de su información personal para un uso específico.

Existen diversas formas de entender el consentimiento; sin embargo, en materia de protección de datos personales, estas transmisiones siempre deben realizarse mediante un consentimiento expreso. Es decir, debe ser otorgado de manera clara y explícita, sin ambigüedades ni coerción por parte del responsable del trata-

miento de los datos. Este principio se conecta directamente con otro: la licitud. Esta exige que el objeto de la transacción —es decir, el propósito para el cual se realizará el tratamiento de la información— sea conforme a la ley y no vulnere ninguna regulación en cualquier materia. Siguiendo con la lista, el principio de finalidad establece que deben estar explícitamente estipulados todos los posibles usos que se le dará a la información personal. Con lo anterior referido, es acertado decir que todos los usos que estén fuera del acuerdo serán completamente inválidos, debido a que la persona que accedió solo brindó su consentimiento a los fines estipulados en la transferencia, generalmente en presencia de un aviso de privacidad.

Sobre el punto antes referido, el principio de información se sitúa entre los otros dos previamente señalados, ya que implica que, en el proceso de la transferencia de datos, la persona que los proporciona debe ser informada de manera completa por la otra parte sobre qué datos serán utilizados, incluyendo los datos de contacto del responsable. Por su parte, el principio de lealtad se vincula con el de información en tanto que toda comunicación del responsable hacia el titular de los datos, en relación con la transferencia, debe realizarse de manera honesta y transparente.

Por otro lado, el principio de proporcionalidad establece que el responsable únicamente debe utilizar la información estrictamente necesaria para cumplir con el propósito de la transferencia. En resumen, este principio protege toda aquella información personal que no esté directamente relacionada con la finalidad aceptada por el titular. Asimismo, este principio establece las obligaciones del responsable respecto al tratamiento de los datos, entre los que destacan: implementar medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados; garantizar su precisión y actualización, y respetar los derechos de los titulares. Cabe mencionar que, una vez concluido el uso práctico de los datos personales, tratándose de su almacenamiento, estos deben ser eliminados. Es decir, el procesamiento de este tipo de información no puede mantenerse de forma indefinida. En su defecto, se deberán aplicar técnicas de anonimización (Marques y Bernardino, 2020), como los mecanismos de privacidad diferencial propuestos por instituciones como el National Institute of Standards and Technology (NIST)¹.

1 Para conocer más sobre esta técnica, véase:

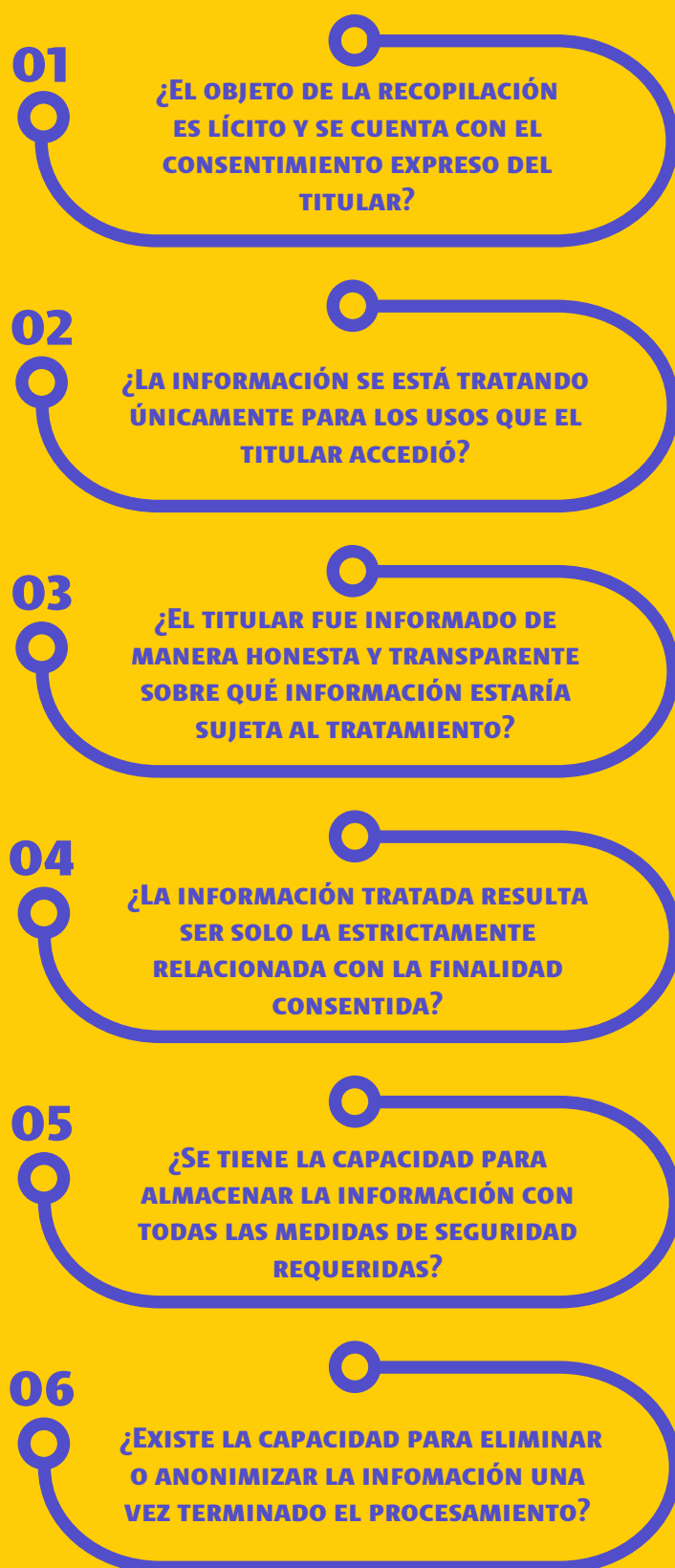


Figura 1. Pasos para implementar información que contenga datos personales.
Fuente: elaboración propia.

Con el objetivo de ilustrar la aplicación práctica de estos principios en el tratamiento de datos personales, se presenta la figura 1, la cual muestra un sistema de seis pasos a considerar para la implementación de información que incluya datos personales.

En el primer paso se encuentran los principios de legalidad y consentimiento. Antes de que cualquier persona interesada pueda establecer un objetivo para el tratamiento de datos personales, debe asegurarse de que dicho propósito sea lícito y cumpla con todas las disposiciones legales pertinentes. Una vez confirmada la licitud del objetivo, se procederá al tratamiento de la información, siempre y cuando exista un consentimiento expreso por parte del titular de los datos.

Si el primer paso ha sido respondido afirmativamente, es posible continuar con la prueba. En el segundo paso, se observa el principio de finalidad, el cual exige que el interesado revise con precisión los fines para los cuales el titular ha dado su consentimiento para el tratamiento de su información. En esta etapa, el interesado debe confirmar que el titular ha aceptado expresamente el tipo de tratamiento que se pretende realizar.

En caso de que el paso anterior se haya completado satisfactoriamente, el tercer paso incorpora los principios de información y lealtad. En esta fase el interesado debe entregar información clara y completa sobre el uso de sus datos: cuáles estarán sujetos a la transferencia y cómo se utilizarán, y proporcionar los datos de contacto del interesado en caso de que el titular requiera comunicarse. Toda esta información debe ser otorgada con total transparencia y honestidad.

Una vez que se hayan cumplido las disposiciones de este paso, la siguiente etapa implica la limitación de uso de la información recopilada. Esta fase se basa en el principio de proporcionalidad, el cual garantiza la protección de toda aquella información que no sea relevante para el propósito del tratamiento. Durante este punto, el interesado debe asegurarse de que la información recopilada se utilice únicamente para los fines correspondientes, mediante el consentimiento del titular.

Por último, el quinto y sexto paso contienen el principio de responsabilidad. El primero de los dos implica que el interesado debe contar con los medios necesarios para proteger de ma-

nera adecuada la información durante el transcurso de su tratamiento. El siguiente cubre la obligación de desechar adecuadamente los datos personales, que el interesado está sujeto a realizar una vez que termine con su objetivo.

De acuerdo con esta prueba, cualquier interesado puede garantizar el cumplimiento de los principios básicos en materia de protección de datos personales, que a la par permite una gestión más responsable y ética de la información privada. Este proceso no solo fortalece la confianza entre los individuos y las entidades que administran sus datos, sino que también contribuye al respeto de los derechos fundamentales de privacidad y seguridad de la información. En última instancia, esta iniciativa promueve un entorno digital más seguro y transparente para todos los involucrados.

◆ RESULTADOS Y DISCUSIÓN

Protección de datos personales en el contexto de la IA

Una vez discutidos los principios que rigen el tratamiento de datos personales, es menester explicar la existencia de un marco teórico aplicado a su desarrollo que respeta estos preceptos. Es fundamental entender que la IA necesita acceder a cantidades masivas de información para especializarse en un área específica. Este acceso inicial para la fase de entrenamiento

se puede presentar de múltiples formas, dependiendo del objetivo de los desarrolladores (Mendoza, 2021). Durante este proceso, la protección a los datos personales tiene un primer contacto con la IA, ya que la cantidad masiva de información puede contener datos personales o inclusive el entrenamiento del modelo puede llegar a estar basado completamente en información de carácter personal.

Durante la adquisición inicial de datos personales, la problemática de legitimar su adquisición puede reducirse, en apariencia, a una transferencia de datos ordinaria sin hacer distinción alguna respecto a la naturaleza de la tecnología involucrada. Esta perspectiva se basa en el hecho de que, en el momento de recopilar los datos para el entrenamiento, aún no existe una inteligencia artificial implicada como tal. Por lo tanto, no habría una variable adicional que considerar en la correcta aplicación de las regulaciones existentes (Castellanos, 2020).

El mayor reto para los desarrolladores —quienes, en esta etapa, resultan responsables del tratamiento de la información personal—, reside en el cumplimiento del principio de finalidad. En caso de que los datos hayan sido obtenidos sin que el titular otorgara un consentimiento explícito para su uso en el desarrollo de una IA, dichos datos no deberían ser tratados, ya que ello implicaría una violación a dicho principio (Sistema Na-

Tabla 1. Principios legales relacionados con la protección de datos personales.

Principio	Descripción
1. Consentimiento	Definido como el acuerdo de voluntades respecto a un objeto en común; en este caso, una persona física acuerda con otra —ya sea física o moral— el traspaso de su información personal para un uso específico.
2. Licitud	Este principio exige que el objeto de la transacción —es decir, el propósito para el cual se realizará el tratamiento de la información— sea conforme a la ley y no vulnere ninguna regulación en cualquier materia.
3. Finalidad	Establece que deben estar explícitamente estipulados todos los posibles usos que se le dará a la información personal.
4. Información	Implica que, en el proceso de la transferencia de datos, la persona que los proporciona debe ser informada de manera completa por la otra parte sobre qué datos serán utilizados, incluyendo los datos de contacto del responsable.
5. Lealtad	Se vincula con el de información, en tanto que toda comunicación del responsable hacia el titular de los datos, en relación con la transferencia, debe realizarse de manera honesta y transparente.
6. Proporcionalidad	Establece que el responsable únicamente debe utilizar la información estrictamente necesaria para cumplir con el propósito de la transferencia.

Fuente: elaboración propia.



CUALQUIER INTERESADO PUEDE GARANTIZAR EL CUMPLIMIENTO DE LOS PRINCIPIOS BÁSICOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES, QUE A LA PAR PERMITE UNA GESTIÓN MÁS RESPONSABLE Y ÉTICA DE LA INFORMACIÓN PRIVADA. ESTE PROCESO NO SOLO FORTALECE LA CONFIANZA ENTRE LOS INDIVIDUOS Y LAS ENTIDADES QUE ADMINISTRAN SUS DATOS, SINO QUE TAMBIÉN CONTRIBUYE AL RESPETO DE LOS DERECHOS FUNDAMENTALES DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

cional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, s. f.).

Ante esta situación, los desarrolladores han acudido a figuras jurídicas contempladas en la legislación europea que permiten el tratamiento de datos personales sin que dicho uso respete directamente el principio de finalidad. Dado que, al momento de preparar esta contribución, la legislación mexicana aplicable no ofrece una definición igualmente clara y completa, para este análisis se utilizará como referencia el Reglamento General de Protección de Datos (o GDPR, por sus siglas en inglés) correspondiente al marco legal de la Unión Europea (General Data Protection Regulation, 2024).

Retomando los argumentos que podrían ser utilizados en favor de los desarrolladores en este uso «injusto», la legislación europea contiene la posibilidad de justificarlo en el contenido de sus artículos 6° y 89°. La fracción 6.4 establece la figura de reutilización de datos, la cual se permite siempre y cuando el nuevo tratamiento esté alineado con el consentimiento inicial del titular. Para ello, deben considerarse factores como la relación entre el responsable y el titular, así como la sensibilidad de la información. Esta condicionalidad puede observarse claramente en el siguiente ejemplo práctico: en el supuesto de que se desarrolle una IA similar al modelo de ChatGPT, con información personal proveniente de múltiples fuentes, justificar dicho tratamiento bajo la figura de reutilización se vuelve extremadamente complejo e incluso inviable, debido a la diversidad de fuentes y a la inexistente relación con los titulares de la información. En cambio, si una institución privada desarrolla un modelo basado en IA para agilizar sus operaciones a partir de datos personales de sus propios trabajadores, la posibilidad de

invocar esta figura es mucho más viable. Esto se debe, entre otros factores, a las excepciones previstas en el artículo 9, fracción IV, de nuestra LFPDPPP, a la relación directa entre los trabajadores y el desarrollador, y a que el nuevo propósito —el desarrollo de una IA— puede alinearse más fácilmente con el tratamiento inicial, bajo la justificación de un beneficio laboral.

Las disposiciones contenidas en el artículo 89° también contemplan la posibilidad de aplicar la figura de reutilización; sin embargo, en este caso la legislación se enfoca en el interés público, un aspecto llamativo para el desarrollo de IA. Esta sección permite justificar el tratamiento de datos personales considerado «injusto» cuando existe un interés público, ya sea por motivos de investigación científica o por fines relacionados con archivos históricos.

No obstante, la aplicación de esta disposición en el desarrollo de IA resulta limitada, ya que el artículo solo contempla esos dos supuestos. Además, la definición que se ofrece para considerar una actividad como investigación científica no se ajusta del todo al desarrollo de IA. En el recital 159° de la misma legislación, se restringe el concepto de investigación científica en el ámbito tecnológico únicamente a aquellas investigaciones que representen un avance tecnológico fundamental. Esta característica resulta difícil de argumentar en el caso del tratamiento de datos personales para el desarrollo de IA, ya que la utilización ilegítima de dichos datos no califica como investigación en sentido estricto. Incluso si lo hiciera, su implementación no contribuiría directamente al avance tecnológico, dado que entrenar una IA mediante métodos ordinarios y preestablecidos no implica innovación. Este criterio resulta especialmente interesante si se contrasta con el marco legal de

Estados Unidos, donde se emplea para justificar la figura del «uso transformativo», desarrollada a partir del caso *Campbell vs. Acuff-Rose Music*. Actualmente, este concepto se utiliza para defender el uso «libre» de contenidos, incluidos los datos personales verificables, en el contexto de los derechos conexos ejercibles por intérpretes y ejecutantes.

Dado que las dos posibles alternativas contenidas en el GDPR para justificar el tratamiento de datos personales con fines no consentidos por el titular no terminan de adecuarse del todo al contexto del desarrollo de IA, la mejor opción para legitimar el uso de dicha información sigue siendo el consentimiento expreso del titular.

Si bien obtener este consentimiento puede resultar más tedioso para los desarrolladores de esta tecnología, es la única manera de asegurarse de que el tratamiento de los datos se realiza sin violar el derecho a la privacidad de las personas. Cabe señalar que este paso adicional, aunque no favorezca directamente a los desarrolladores, representa una protección fundamental para los titulares de la información y justifica, en gran medida, cualquier posible retraso en el avance tecnológico con tal de salvaguardar las garantías individuales.

Como se determinó previamente, la IA no solo requiere de un flujo de información durante su entrenamiento, sino que, en su etapa de despliegue y operación, continúa recolectando datos mientras cumple con sus funciones. Esta información adicional es utilizada para aprender de forma autónoma. Sin embargo, al igual que los bloques de datos empleados en su entrenamiento, la información recolectada de manera «propia» también puede incluir datos personales.

Una solución aparentemente sencilla a esta problemática sería condicionar el uso de la IA a la aceptación de un acuerdo de privacidad,

como sucede en la mayoría de los casos. Este acuerdo debería ajustarse a los principios del tratamiento de datos personales y permitir, bajo ciertas condiciones, la transferencia de información con fines de mejora del modelo. No obstante, el debate se complejiza cuando se consideran modelos de IA que operan sin que medie una intención explícita de ser utilizados y que, en ese proceso, recaban datos personales. Tal es el caso de sistemas diseñados para monitorear el desempeño laboral o tecnologías de vigilancia potenciadas por IA.

Cualquier modelo que, por su diseño, impida obtener un consentimiento previo y directo para la recolección y tratamiento de datos personales representa una transgresión al marco jurídico y teórico desarrollado en este análisis. Esta situación se agrava si se toma en cuenta lo dispuesto en el artículo 22 del Reglamento General de Protección de Datos (GDPR), que establece: «todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar». Para enfrentar este desafío, se contemplan dos escenarios: uno en el que existe una relación directa y posibilidad de comunicación entre el responsable y el titular de los datos, y otro en el que dichas condiciones no se cumplen.

Comenzando con el primer supuesto, la importancia de que exista una relación y comunicación entre ambas partes radica en que el responsable tiene la posibilidad de obtener directamente el consentimiento expreso del titular. De esta manera, la transferencia de datos





resultaría legítima. Respecto a este primer supuesto, existe una forma de evadir, en cierta medida, dicho requerimiento, siempre que se trate de la recolección de información personal en un contexto de relación laboral. El artículo 6.1, inciso b del GDPR, otorga la posibilidad de realizar un tratamiento de datos, siempre y cuando estos sean necesarios para el cumplimiento de un contrato al cual el titular esté sujeto. Este supuesto se puede utilizar de manera directa en la implementación de modelos de IA para cualquier forma de optimización en un contexto laboral. Es decir, si cualquier empresa incluye una cláusula que establezca la necesidad de compartir datos personales —en tanto estén relacionados con actividades laborales de manera que se evite la violación al principio de proporcionalidad—, la implementación de cualquier modelo cuya operación constante recabe datos personales resultaría legítima. Aunado a esto, la definición brindada por el recital 155° de la misma regulación permite que los acuerdos laborales establezcan reglas específicas para el tratamiento de datos personales.

Es importante aclarar que esta posible alternativa para la recolección de datos personales por parte de una IA en un entorno laboral no exime, en ningún caso, del cumplimiento de los principios y disposiciones establecidos en la normativa vigente.

En cuanto al segundo escenario —en el que no existe relación ni forma de comunicación entre las partes—, salvo que el tratamiento se encuentre expresamente contemplado en alguna excepción legal, cualquier procesamiento de datos personales sin el consentimiento del titular constituye una violación a la legislación vigente. En los casos en los que no sea posible obtener dicho consentimiento de

manera factible y no exista un contexto de relación laboral, el tratamiento de los datos se considera ilegítimo e ilegal, sin que exista justificación válida alguna.

CONCLUSIÓN

Proteger el derecho a la autodeterminación informativa de la persona no debe considerarse como un obstáculo para el desarrollo de la IA. El debate sobre si debe prevalecer la protección y el consentimiento de los titulares respecto al tratamiento de datos personales por la IA, o si la justificación del desarrollo tecnológico y el beneficio social que proporcionan los avances de los modelos basados en esta tecnología se sobrepone a las disposiciones básicas de este derecho, resulta innecesario. Ambas posturas no son contradictorias entre sí: el derecho a la privacidad no interfiere con el desarrollo de la IA, y esta última no necesita violar las regulaciones para poder implementarse.

Este análisis siguió un enfoque basado en la aplicación de los principios que rigen la protección de datos personales y sus respectivas regulaciones en la Unión Europea y en México, con el objetivo de contextualizar los conceptos relacionados dentro del ámbito de la inteligencia artificial (IA). El resultado confirmó que el marco jurídico vigente, tanto a nivel nacional como internacional, cuenta con la capacidad de regular las interacciones básicas entre la IA y la protección de la privacidad.

No obstante, es necesario un mayor refinamiento de las normas existentes y, en el caso mexicano, no resulta indispensable la creación de un nuevo cuerpo legislativo. Las transferencias de información personal y la recolección ilegítima de datos no deben abordarse de manera distinta por el solo hecho de involucrar tecnología novedosa. En materia de protección de datos personales, los lineamientos que regu-

lan la transferencia de información del titular hacia el responsable ya se encuentran claramente definidos.

Es importante destacar que estas medidas de protección no representan un obstáculo para el desarrollo de la inteligencia artificial; por el contrario, constituyen una garantía para el ejercicio de un derecho humano. Respetar el consentimiento del titular y cumplir con los principios establecidos al momento de tratar los datos personales en el desarrollo de un modelo de IA no impide su avance, ya que no limita la posibilidad de recolectar datos de forma legítima.

En este sentido, puede concluirse que la legislación vigente en materia de protección de datos personales es plenamente capaz de enfrentar los desafíos que plantea la era de la inteligencia artificial a nivel global. Dicho esto, la IA tiene únicamente dos caminos al manejar información personal: hacerlo de forma legítima o incurrir en un tratamiento ilegítimo, lo cual implica una violación a la ley. No existe excepción ni debe existir.

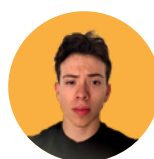
En consecuencia, es razonable afirmar que no es necesaria una legislación especializada en IA para regular la protección de datos personales, su recolección y tratamiento en el contexto de esta tecnología. No obstante, una ley específica podría aportar beneficios concretos, especialmente si incorpora regulaciones más detalladas sobre los estándares de transparencia que los modelos de IA deben cumplir.

A manera de reflexión final, el derecho a la privacidad no debe ejercerse de forma pasiva, en espera de que los particulares respeten y hagan buen uso de nuestra información solo porque existen leyes que así lo ordenan. Por el contrario, es un derecho que debe ejercerse de manera activa por parte de los titulares, otorgando un consentimiento informado y consciente para el tratamiento de sus datos personales. El primer paso para garantizar este derecho es protegerlo nosotros mismos.



REFERENCIAS

- Angulo-Molina, A., Méndez-Rojas, M. A., Palacios, T. J., Contreras, O. E., Hirata, G., Flores, J. C., Merino, S., Valenzuela, O., Hernández, J. y Reyes, J. (2014). Magnetite nanoparticles functionalized with a-tocopheryl succinate (a-TOS) promote selective cervical cancer cell death. *Journal of Nanoparticle Research*, 16(8), 2528.
- Barrio, M. (2021). Towards legal regulation of artificial intelligence. *Revista IUS*, 15(48), pp. 35-53. <https://doi.org/10.35487/rius.v15i48.2021.661>
- Boucher, P. (2020). *Artificial intelligence: How does it work, why does it matter, and what can we do about it?* European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU\(2020\)641547_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf)
- Castellanos, J. (2020). La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. *Métodos de Información*, 11(21), pp. 42-58.
- Domínguez, A. G. (2004). *Tratamiento de datos personales y derechos fundamentales*. Librería-Editorial Dykinson.
- Estrada, J. C. (s. f.). *El derecho a la intimidad y su necesaria inclusión como garantía individual*. <https://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf>
- General Data Protection Regulation. (2024, 22 de abril). *General Data Protection Regulation (GDPR)*. <https://gdpr-info.eu/>
- Marques, J. F. y Bernardino, J. (2020). Analysis of data anonymization techniques. En *KEOD*, pp. 235-241.
- Martínez, J. (1991). *Teoría de las obligaciones* (2.ª ed.). Porrúa.
- McCarthy, J. (2007). *What is artificial intelligence?* Stanford University. <https://www-formal.stanford.edu/jmc/whatisai.pdf>
- Mendoza, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48), pp. 179-207. <https://doi.org/10.35487/rius.v15i48.2021.743>
- Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (s. f.). Marco normativo. <https://proyectos.inai.org.mx/pronadatos/index.php/inicio/informacion/marconormativo>
- Solange, M. (Ed.). (2018). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, comentada*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. <https://idaip.org.mx/bibliotecadigital/product/ley-general-de-proteccion-de-datos-personales-en-posesion-de-sujetos-obligados-comentada/>
- Visual Storytelling Team y Murgia, M. (2023, 11 de septiembre). Generative AI exists because of the transformer. *Financial Times*. <https://ig.ft.com/generative-ai/>



Juan Manuel Rivera Vélez

Estudiante de la Licenciatura en Derecho en la Universidad de las Américas Puebla y miembro del Programa de Honores en dicha

institución educativa.

juan.riveravz@udlap.mx