JUS

El derecho a la ciberseguridad: hacia un marco jurídico para la protección de la identidad digital en la era de la inteligencia artificial

Olga Patricia Chávez Ávila

Recibido: 9 abril 2025 / Aceptado: 10 junio 2025 / Publicado: 13 agosto 2025
Sección: Artículos

Resumen: La pretensión del presente artículo se circunscribe al análisis de la necesidad de reconocer la ciberseguridad como un derecho fundamental emergente en un contexto global marcado por el auge de la inteligencia artificial y la digitalización de la vida cotidiana. A través de un análisis jurídico, se identifican las amenazas actuales a la *identidad digital*, como el *phishing*, los *deepfakes* y el *robo de datos personales*, resaltando la vulnerabilidad de los usuarios frente a marcos normativos insuficientes o desactualizados. Se examinan los instrumentos legales internacionales y nacionales existentes, señalando sus limitaciones frente a los nuevos retos tecnológicos. Asimismo, se discute el impacto de la desaparición de organismos autónomos como el INAI en México, lo que representa un retroceso significativo en la protección de la privacidad. El texto propone la construcción de un marco normativo robusto, transversal y adaptable, orientado a garantizar la *protección de datos personales*, el fortalecimiento institucional y la educación digital. Finalmente, se concluye que el reconocimiento de la ciberseguridad como derecho humano es indispensable para el ejercicio pleno de otros derechos fundamentales en la era digital.

Palabras clave: ciberseguridad, identidad digital, protección de datos, inteligencia artificial, derechos fundamentales.

Abstract: The purpose of this article is to analyze the need to recognize cybersecurity as an emerging fundamental right within a global context marked by the rise of artificial intelligence and the digitalization of everyday life. Through a legal analysis, the article identifies current threats to *digital identity*—such as *phishing*, *deepfakes*, and the theft of personal data—highlighting

JUS DERECHO SOCIEDAD ESTADO, nueva época, núm. 21, enero-junio, 2025, es una publicación electrónica semestral editada por la Universidad Juárez del Estado de Durango (UJED) con domicilio en Constitución, núm. 404, colonia Centro, C.P. 34000, Durango, Durango, teléfono 618-827-1295, página web: http://jus.ujed.mx, editorialujed@ujed.mx. Editor responsable: Martín Gallardo García. Reserva de Derechos al Uso Exclusivo número: 04-2024-011809451300-102, ISSN: 2594-4033, otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la actualización de este número: Oficina Editorial Universitaria, Constitución, núm. 404, colonia Centro, C.P. 34000, Durango, Durango. Responsable de la última actualización: Manuel Rojas Villarreal. Fecha de última modificación, 13 de agosto de 2025.

the vulnerability of users in the face of insufficient or outdated regulatory frameworks. It examines existing international and national legal instruments, underscoring their limitations in addressing the challenges posed by rapidly evolving technologies. The article also explores the impact of the dismantling of autonomous bodies such as Mexico's INAI, which represents a significant setback in the protection of privacy. It advocates for the development of a robust, cross-cutting, and adaptable regulatory framework aimed at ensuring *personal data protection*, institutional strengthening, and digital education. The article concludes that recognizing cybersecurity as a human right is essential for the full exercise of other fundamental rights in the digital age.

Keywords: cybersecurity, digital identity, data protection, artificial intelligence, fundamental rights.

1. Introducción

¿Qué pasaría si el día de mañana alguien usara tu rostro, tu voz, tus datos biométricos y generales para cometer un delito? En una era donde la constante evolución tecnológica cada vez nos envuelve más en un mundo digital en donde nuestra identidad digital es tan real –y vulnerable– como nuestra identidad física, la ciberseguridad ya no es una cuestión técnica: es una necesidad urgente de protección jurídica. En el año 2024 se han producido miles de millones de filtraciones de datos en ataques a empresas de todo el mundo, comprometiendo así a más de 500 millones de identidades digitales en ataques cibernéticos, evidenciando una creciente vulnerabilidad en la protección de los datos personales en la era de la inteligencia artificial. Con la creciente popularidad del uso indebido de herramientas como los *deepfakes*, "*phishing*" y la manipulación de información, la pregunta ya no es si la ciberseguridad es importante, sino si debería considerarse un derecho fundamental emergente y cómo los ordenamientos jurídicos deberían de evolucionar para garantizar la protección de la identidad digital frente a estos riesgos.

A medida que las sociedades evolucionan, y se digitalizan, la identidad digital se convierte en un activo presencial para la participación en la economía, la política y la vida cotidiana. Sin embargo, la constante evolución de la inteligencia artificial ha traído consigo nuevos retos, y también, nuevas amenazas, tales como el robo de identidad mediante algoritmos avanzados, la creación de falsificaciones digitales (*deepfakes*) y la manipulación masiva de datos personales.

Estas problemáticas plantean desafíos a los cuales se les debe de buscar una solución de manera urgente en materia de ciberseguridad, los cuales requieren una respuesta jurídica adecuada.

Este artículo tiene como objetivo analizar la viabilidad de considerar la ciberseguridad como un derecho fundamental emergente, y explorar los desafíos regulatorios para la protección de la identidad digital en la era de la inteligencia artificial. Para ello se examinarán las normativas actuales, las amenazas emergentes y las posibles estrategias jurídicas para la creación de un marco normativo integral.

El presente se desarrolla en cinco secciones. En la primera sección, definiremos el concepto de identidad digital y su relación con la ciberseguridad. En la segunda, analizaremos las normativas existentes de distintas jurisdicciones y sus limitaciones; posteriormente se presentarán las amenazas emergentes derivadas del uso de inteligencia artificial en ataques cibernéticos. Luego, exploraremos la posibilidad de considerar a la ciberseguridad como un derecho fundamental, comparándola con otros derechos digitales reconocidos. Finalmente, propondremos estrategias jurídicas para la implementación de un marco jurídico robusto y armonizado a nivel nacional.

Este trabajo emplea una metodología jurídico-analítica, basada en el análisis doctrinal, normativo y jurisprudencial, así como en la comparación de marcos legales nacionales e internacionales, para evaluar los desafíos actuales de la ciberseguridad en relación con los derechos fundamentales.

2. Definición de identidad digital y su relevancia en la sociedad digital

La identidad digital es toda aquella información que representa a una persona dentro de un entorno "*online*" o, mejor conocido como entorno digital. Ésta se ha convertido en algo esencial para nosotros debido a la creciente digitalización de nuestras vidas. No estamos hablando meramente de un nombre y una contraseña, cuando hablamos de la identidad digital debemos entender el significado que engloba esta palabra, ya que representa una gran importancia para los usuarios, puesto que nos estamos refiriendo a la amalgama digital de todas las formas de presencia en línea de todos los usuarios a través del mundo; esta identidad comprende una gran cantidad de información personal que define al usuario en las plataformas digitales y que puede tener consecuencias fuera del mundo digital.

2.1 Panorama de las amenazas en ciberseguridad impulsadas por la IA

El panorama de amenazas en ciberseguridad impulsadas por la inteligencia artificial es uno de los más complejos de la historia, no sólo por ser relativamente nuevo, sino porque la velocidad, la escala y la sofisticación de los "*hackers*" es alarmante. "En solo un año, el número de actores de amenazas rastreados por Microsoft saltó de 300 a más de 1500. El aumento de los ataques patrocinados por el Estado y la proliferación del *ransomware* son las principales preocupaciones de las empresas de todos los tamaños. Además, el número de ciberataques se ha disparado de 579 ataques por segundo en 2021 a la asombrosa cifra de 7000 ataques de contraseñas por segundo en 2024".[1] Los atacantes han encontrado una nueva manera de vulnerar la seguridad digital, aprovechando la inteligencia artificial, la automatización y las estrategias de ataque multifacéticas para eludir las defensas tradicionales.

Este aumento de ciberataques denota la urgente necesidad de buscar soluciones innovadoras para combatir la creciente e inevitable complejidad de las amenazas cibernéticas, así como para generar la integración de regulaciones legales destinadas al monstruo cibernético que es la inteligencia artificial.

3. Marco jurídico actual: protección de la identidad digital

En un mundo donde la tecnología avanza más rápido que la ley, la regulación de la inteligencia artificial y del mundo virtual se está quedando peligrosamente atrás.

Actualmente, la regulación de la ciberseguridad se encuentra fragmentada y desactualizada frente a los constantes avances tecnológicos que nos obligan a permanecer en constante alerta, debido a que nos encontramos frente a una bomba de tiempo de dimensiones catastróficas; instrumentos como el Reglamento General de Protección de datos (RGPD) en la Unión Europea, o la ley de privacidad del consumidor en California (CCPA) han intentado establecer protecciones para regular a la inteligencia artificial y la ciberseguridad, pero persisten lagunas jurídicas que dejan a millones de personas vulnerables a ataques digitales.

Ante este panorama es que surge la necesidad de analizar si es necesario que la ciberseguridad sea reconocida como un derecho fundamental y

1 Microsoft, *Informe anual de defensa digital 2024*. https://www.microsoft.com/es-es/security/business/digital-defense-report (fecha de consulta: 6 de abril de 2025).

cómo los ordenamientos jurídicos deben evolucionar para proteger la identidad digital.

México cuenta con un marco normativo para la protección de la identidad digital bastante limitado, ya que este se encuentra sustentado principalmente en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), vigente desde 2010. Esta legislación establece principios y derechos, conocidos como derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), que permiten a los individuos controlar el uso de su información personal.

Sin embargo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) tiene más de una década y no aborda de manera específica los desafíos actuales relacionados con la ciberseguridad e identidad digital, tales como el uso de inteligencia artificial, la proliferación de plataformas en línea y las amenazas cibernéticas emergentes. A diferencia del Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la California Consumer Privacy Act (CCPA) en Estados Unidos, que han incorporado disposiciones más actualizadas para enfrentar estos retos, es evidente que la legislación mexicana requiere una modernización urgente para estar a la par de estas normativas internacionales y así poder regular de manera más efectiva el mundo digital.

En América Latina, países como Argentina y Chile han reconocido la necesidad de actualizar sus leyes de protección de datos para adaptarse a los avances tecnológicos y a las nuevas formas de tratamiento de información personal. México también enfrenta nuevos desafíos, como la propuesta de implementar una CURP con fotografía y huellas dactilares (datos biométricos) para facilitar la búsqueda de personas desaparecidas, propuesta que a primera instancia podría sonar bastante interesante, sin embargo, no se plantean los riesgos ni las amenazas que implica el tener fácil acceso a dichos datos biométricos, lo que plantea preocupaciones sobre la privacidad y el manejo correcto de datos biométricos.

Otro aspecto relevante es la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el cual fue oficialmente disuelto en diciembre del 2024. Y si bien sus funciones fueron transferidas a la Secretaría de Anticorrupción y Buen Gobierno (específicamente a un nuevo órgano desconcentrado llamado "Transparencia para el Pueblo") la desaparición del INAI podría generar una debilitación en la supervisión y garantía de los derechos relacionados con la

protección de datos en el país esto debido a que Transparencia para el Pueblo es un nuevo órgano desconcentrado de la Secretaría de Anticorrupción y Buen Gobierno, lo que significa que sus funciones se rigen bajo el control directo del Ejecutivo, y esto genera preocupaciones relacionadas con la independencia de la garantía del derecho de acceso a la información pública y la protección de datos personales, ya que representa un retroceso enorme en la cultura de la privacidad, puesto que el INAI cumplía un papel no solo pedagógico, sino también un papel protector, ayudando a los ciudadanos a identificar sus derechos, cómo ejercerlos y a quién acudir en caso de la violación de los mismos. Así mismo, se obstaculiza el avance hacia una cultura digital responsable ya que la desaparición de este órgano especializado en la privacidad limita la capacidad del país para adaptarse a estos nuevos e importantes desafíos.

Es evidente que, pese a que México cuenta con una base legal para la protección de la identidad digital, la falta de actualización de la misma favorece a la incapacidad de abordar eficazmente los desafíos contemporáneos a los que se enfrenta.

4. Evaluación de lagunas jurídicas en la protección de la identidad digital

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) establece que los *datos biométricos* deben ser considerados como datos personales sensibles, lo que implica un nivel reforzado de protección legal. No obstante, el marco normativo mexicano carece de disposiciones específicas que regulen de manera detallada su recolección, almacenamiento, uso y transferencia, a pesar del creciente empleo de estas tecnologías en sectores como la seguridad pública, la salud, la banca y los servicios digitales.

La ausencia de criterios técnicos y jurídicos claros –como el consentimiento expreso, la limitación de finalidad, la minimización de datos y la protección mediante cifrado– expone a los titulares a un riesgo elevado de usos indebidos, discriminación, suplantación de identidad y vigilancia masiva. En contraste, legislaciones como el Reglamento General de Protección de Datos de la Unión Europea (RGPD) han establecido salvaguardas explícitas, como auditorías, análisis de impacto y restricciones severas al tratamiento automatizado de estos datos. La falta de armonización con es-

tándares internacionales posiciona a México en una situación de desventaja jurídica en materia de *biometría y privacidad*.

4.1 El derecho al olvido: una garantía pendiente en el orden jurídico mexicano

El derecho al olvido –entendido como la facultad de un individuo para solicitar la supresión de información personal irrelevante, inexacta o desactualizada de los motores de búsqueda– representa una figura jurídica en expansión dentro del derecho a la privacidad en el entorno digital. En la Unión Europea, su desarrollo ha sido ampliamente respaldado por el Tribunal de Justicia de la UE (caso *Google Spain v. AEPD*, C-131/12), lo que ha permitido construir una doctrina sólida que equilibra la protección de datos personales con la libertad de expresión y el derecho a la información.

En México, sin embargo, el reconocimiento y la aplicación del derecho al olvido son aún limitados. Si bien la Suprema Corte de Justicia de la Nación ha abordado casos relacionados con la supresión de datos, no existe una regulación expresa ni procedimientos administrativos eficaces para su ejercicio frente a empresas tecnológicas. Esta omisión normativa limita el control de los individuos sobre su información digital y vulnera principios como la autodeterminación informativa, el libre desarrollo de la personalidad y la reputación en línea.

La falta de un mecanismo formal para ejercer este derecho obstaculiza el acceso efectivo a la *rectificación digital* y genera una asimetría de poder entre los titulares de los datos y las corporaciones tecnológicas. Para avanzar en este terreno, México requiere una reforma legislativa que reconozca el derecho al olvido como una dimensión del derecho a la protección de datos personales, con procedimientos accesibles, recursos efectivos y estándares proporcionales que garanticen un equilibrio con el interés público.

5. Amenazas emergentes en ciberseguridad

En el año 2025, el panorama de la ciberseguridad enfrenta desafíos cada día más complejos y sofisticados. La rápida evolución tecnológica ha dado lugar a amenazas emergentes que requieren y obligan a los profesionales a brindarle una atención y preparación constantes para poder combatir las nuevas amenazas digitales. A continuación se detallan algunas de las principales amenazas actuales en el ámbito de la ciberseguridad y cómo estas afectan la identidad física y digital del usuario.

5.1 Uso de la inteligencia artificial en la suplantación de identidad

Los *deepfakes* son imágenes, videos y audios manipulados mediante inteligencia artificial para que parezcan reales, estos tienen una precisión verdaderamente alarmante que facilita la suplantación de identidad. Por ejemplo, en 2020 se reportó un caso donde un video manipulado fue utilizado para hacerse pasar por el CEO de una empresa europea, ordenando una transferencia de fondos significativa a cuentas controladas por delincuentes.[2] Además, la inteligencia artificial ha sido empleada para clonar voces, permitiendo a los estafadores realizar llamadas telefónicas e incluso ya están comenzando a incorporar las videollamadas o videos enviados por whatsapp en los que se hacen pasar por familiares o amigos en problemas, solicitando dinero urgente. Un ejemplo de ello es la estafa del "familiar en problemas", donde los delincuentes utilizan información personal y tecnología avanzada para recrear la voz de la persona que supuestamente se encuentra en problemas o ha sido secuestrada para hacer la estafa más creíble.

5.2 Ataques de manipulación de datos en infraestructuras críticas

La IA también ha sido utilizada para desarrollar *malware* sofisticado capaz de infiltrarse en infraestructuras críticas. Un ejemplo es VenomRAT, un software malicioso que permite el acceso remoto a sistemas infectados, facilitando el robo de credenciales y otros datos sensibles. Este tipo de *malware* se propaga principalmente a través de anuncios no deseados y sitios web comprometidos, representando una amenaza significativa para la seguridad de infraestructuras esenciales.[3]

5.3 Casos recientes de robo de identidad digital y sus implicaciones legales

En 2023 se registraron 26 175 casos de robo de identidad en el sistema bancario mexicano, con pérdidas económicas que ascendieron a 6 169 millones de pesos. Este incremento se atribuye, en parte, al uso de *deepfakes* y técnicas avanzadas de *phishing* que dificultan la detección de fraudes.[4] Además, en España, se reportó el robo de datos personales de aproximadamente 130 000

2 Mejía, Laura, "El fin del INAI y sus repercusiones en el derecho a la información", *Revista Digital de Derecho Público*, 2025. https://revistaderechopublico.org (fecha de consulta: 4 de abril de 2025).

3 Meristation, "Hackers explotan inteligencia artificial para vulnerar redes de empresas", 2025. https://as.com/meristation (fecha de consulta: 6 de abril de 2025).

4 Stark, Michael, "Artificial intelligence and cybersecurity threats", *Cyberlaw Review*, vol. 34, núm. 2, 2024, pp. 77–89.

agentes de la Policía Nacional, comprometiendo su seguridad y resaltando la necesidad de fortalecer las medidas de protección de datos.

5.4 Implicaciones legales en el mundo no digital

Las consecuencias legales de la suplantación de identidad mediante IA van más allá del ámbito digital. Las víctimas pueden enfrentar pérdidas financieras significativas, daños a su reputación y complicaciones legales derivadas de acciones fraudulentas realizadas en su nombre. Por ejemplo, la creación y difusión de contenido manipulado sin consentimiento puede constituir delitos de difamación o violaciones a la privacidad, sujetos a sanciones legales según la jurisdicción correspondiente.

5.5 Violencia digital y uso indebido de inteligencia artificial

El avance acelerado de la inteligencia artificial ha traído consigo no solo beneficios tecnológicos, sino también riesgos que afectan de manera desproporcionada a ciertos grupos sociales. Uno de los fenómenos más alarmantes es el uso de estas herramientas para generar y difundir contenido falso con fines de violencia digital, particularmente contra mujeres y personas con identidades de género diversas.

Deepfakes pornográficos, suplantación de identidad, manipulación de imágenes íntimas sin consentimiento, acoso automatizado y campañas de desprestigio digital, son solo algunas formas en las que la violencia de género ha migrado al entorno digital, adoptando nuevas expresiones gracias al uso malicioso de tecnologías emergentes. Estos actos no solo vulneran la intimidad y dignidad de las víctimas, sino que generan daños emocionales profundos, afectan su libertad de expresión, participación pública y hasta sus oportunidades laborales.

Los marcos normativos actuales en México y en muchos otros países no han evolucionado al ritmo de estas agresiones. Si bien existen leyes que abordan la violencia digital, como la Ley Olimpia, estas resultan insuficientes frente a la complejidad de los ataques potenciados por la inteligencia artificial. Urge una reforma legal que no solo sancione estas conductas, sino que también contemple mecanismos de prevención, reparación del daño, educación digital con perspectiva de género, y garantías reales de acceso a la justicia para las víctimas.

Reconocer la violencia digital como una extensión de la violencia estructural contra las mujeres y actualizar el derecho para protegerlas eficaz-

mente en estos nuevos escenarios, ya no es una opción: es una obligación ineludible del Estado.

6. ¿Es la ciberseguridad un nuevo derecho fundamental?

La ciberseguridad se ha convertido en una parte esencial de la vida moderna, nos encontramos en un panorama interconectado, por lo que la información digital se ha vuelto un recurso sumamente valioso tanto para las empresas, las cuales buscan capitalizar dicho recurso, como para los *hackers*, que buscan aprovechar sus habilidades y las debilidades del mundo digital (y de la ingeniería social, la cual es una técnica de manipulación psicológica utilizada para engañar a las personas y así poder obtener información confidencial de manera digital) para hacer mal uso de la información digital de los usuarios.

Es bien sabido que hay un largo camino por recorrer, y un arduo trabajo legislativo por hacer en materia de ciberseguridad para garantizar la seguridad de los usuarios alrededor del mundo, por lo que analizaremos a varios expertos y organizaciones que han abogado por reconocer a la ciberseguridad como un derecho fundamental.

El abogado especialista en protección de datos, Reusser, enfatiza que "la ciberseguridad debería ser considerada un derecho fundamental de las personas y no solo una herramienta para defender al Estado". Esta perspectiva subraya la necesidad de que los individuos tengan el derecho a proteger su información personal y a estar libres de amenazas cibernéticas.

Además, la organización Red en Defensa de los Derechos Digitales (R3D) sostiene que "las políticas de ciberseguridad deben tener como objetivo principal el proteger y garantizar el ejercicio de derechos humanos". Esta afirmación resalta la interdependencia entre la seguridad digital y la protección de los derechos humanos en el entorno virtual.

Considerando la creciente dependencia de las tecnologías digitales y los riesgos asociados, es entendible abogar por la ciberseguridad como un derecho fundamental. Proteger la información personal y garantizar un entorno digital seguro son cosas esenciales para el ejercicio pleno de otros derechos humanos, como la libertad de expresión y el derecho a la privacidad. No obstante, este reconocimiento debe ir acompañado de un marco legal que equilibre de manera adecuada la seguridad y las libertades individuales, asegurando que las medidas de protección no infrinjan derechos fundamentales.

Desde una perspectiva legal, la ciberseguridad se ha integrado en diversas legislaciones como un medio para proteger derechos fundamentales. Por ejemplo, la Ley Marco de Ciberseguridad y Protección de Infraestructuras Críticas de Chile establece a la Agencia Nacional de Ciberseguridad (ANCI) como la autoridad encargada de regular y proteger los servicios esenciales frente a ciberataques. Sin embargo, es crucial que tales leyes equilibren la seguridad con la protección de libertades individuales, evitando posibles abusos.

7. Análisis doctrinal sobre la posible configuración de la ciberseguridad como un derecho fundamental

La ciberseguridad en México se ha convertido en un tema cada vez más relevante, especialmente considerando los avances tecnológicos y los riesgos que estos conllevan en términos de protección de datos y privacidad. En este contexto, la posibilidad de configurar la ciberseguridad como un derecho fundamental en el marco jurídico mexicano plantea una serie de interrogantes sobre su viabilidad, alcance y las implicaciones para los derechos humanos.

Desde una perspectiva doctrinal, uno de los primeros aspectos a considerar es la evolución de los derechos fundamentales en el mundo digital. Los derechos humanos, tal y como los conocemos, han tenido que adaptarse a los nuevos contextos derivados de la tecnología. El derecho a la privacidad, por ejemplo, ya se ha visto expandido a la protección de datos personales en línea. Sin embargo, este enfoque sigue siendo insuficiente para enfrentar las amenazas cibernéticas que, en muchos casos, no solo afectan a individuos, sino a organizaciones, gobiernos y, en última instancia, a la seguridad nacional.

La inclusión de la ciberseguridad como derecho fundamental en México podría tener un impacto significativo, no solo porque refuerza la protección contra ciberataques, sino también porque garantizaría un espacio digital seguro para el ejercicio de otros derechos fundamentales. Por ejemplo, el derecho a la libre expresión o a la participación política digital estaría directamente relacionado con la seguridad en línea. Si no se garantiza un entorno seguro, las personas podrían verse desincentivadas a participar en actividades en línea por temor a ser víctimas de cibercrimen.

No obstante, configurar la ciberseguridad como un derecho fundamental implicaría un desafío para el sistema legal mexicano, que aún no

tiene una legislación plenamente adaptada a las nuevas amenazas digitales. Aunque existen marcos normativos como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley de Protección de Infraestructura Crítica, estos no abordan específicamente la ciberseguridad en términos de un derecho fundamental. La actualización de la legislación para incluir este derecho sería un paso necesario, pero podría resultar complicado dado que, por un lado, se tendrían que equilibrar las medidas de protección con el respeto a la privacidad y otros derechos fundamentales, y, por otro lado, se tendría que crear una infraestructura estatal capaz de hacer cumplir dicho derecho.

Muchos expertos en Derecho señalan que incluir la ciberseguridad como un derecho fundamental no solo es una cuestión de normativa, sino también de cultura jurídica. Es necesario que exista un cambio de mentalidad en la sociedad y en las instituciones gubernamentales. De nada sirve declarar la ciberseguridad como un derecho fundamental si no se cuentan con los mecanismos adecuados para protegerlo. Esto implica educación en ciberseguridad, una mayor cooperación internacional y un compromiso real por parte de las autoridades en la implementación de medidas efectivas de protección.

En cuanto a las posibles dificultades, la configuración de la ciberseguridad como un derecho fundamental podría verse obstaculizada por la falta de consenso sobre lo que constituye exactamente este derecho. Por ejemplo, ¿debería incluir la ciberseguridad una infraestructura pública dedicada exclusivamente a proteger a los ciudadanos, o se trataría más bien de un derecho a la protección individual de los datos? El debate es amplio y abarca muchas aristas, desde la regulación del acceso a la información hasta el manejo de incidentes cibernéticos de carácter masivo.

Finalmente, es fundamental reflexionar sobre los efectos de la ciberseguridad como derecho fundamental en la vida diaria de los mexicanos. Si bien es cierto que la tecnología ha mejorado la calidad de vida de muchas personas, también ha traído consigo un incremento en los riesgos. El cibercrimen y los ataques a sistemas de información son cada vez más frecuentes y sofisticados. Por lo tanto, garantizar la ciberseguridad podría ser considerado como una extensión del derecho a la seguridad y la protección, un derecho que, históricamente, ha sido parte del núcleo fundamental de la protección estatal.

Aunque la ciberseguridad aún no es reconocida formalmente como un derecho fundamental en México, el análisis doctrinal sugiere que su configuración podría ser un paso importante hacia la consolidación de los derechos digitales. La propuesta de hacerlo no solo sería una respuesta ante el auge de los ciberdelitos, sino también una medida para garantizar un entorno digital seguro en el que los ciudadanos puedan ejercer otros derechos fundamentales sin temor a ser vulnerados. Sin embargo, para que esta propuesta se haga realidad, será necesario un esfuerzo conjunto entre el sector público y privado, así como un compromiso serio con la formación de una cultura jurídica y social en materia de ciberseguridad.

8. Hacia un marco jurídico integral para la protección de la identidad digital

En un contexto donde los avances tecnológicos están cada vez más integrados en todos los aspectos de la vida cotidiana, las amenazas cibernéticas son cada vez más sofisticadas y devastadoras. Por ello, la inclusión de la ciberseguridad como un derecho fundamental en los marcos constitucionales y legales se está convirtiendo en una prioridad para muchos países. En particular, México enfrenta una serie de desafíos en la regulación de la ciberseguridad que requieren atención urgente, especialmente si se compara con otras jurisdicciones que ya han comenzado a desarrollar leyes y políticas más robustas en este campo.

8.1 Situación actual de la ciberseguridad en México

México ha experimentado un crecimiento exponencial en el uso de tecnologías digitales en los últimos años, lo que ha incrementado significativamente los riesgos asociados con los ciberataques. Aunque existen marcos normativos que abordan algunos aspectos de la ciberseguridad, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley de Protección de Infraestructura Crítica, el país aún no cuenta con una legislación integral que regule de manera específica la ciberseguridad de manera exhaustiva.

En 2023, el gobierno mexicano propuso la creación de la Ley Federal de Ciberseguridad, una iniciativa que busca establecer una Agencia Nacional de Ciberseguridad, regular los delitos cibernéticos, y crear políticas de protección en tecnologías de la información y comunicación (TIC). Sin embargo, esta propuesta aún se encuentra en proceso de discusión y no ha sido

aprobada, lo que deja a México vulnerable frente a las crecientes amenazas cibernéticas que afectan tanto a entidades públicas como privadas. Además, la falta de mecanismos de implementación adecuados y la falta de capacitación en ciberseguridad de los usuarios y funcionarios públicos también contribuyen a la vulnerabilidad del país.

Un ejemplo relevante de la situación de México en ciberseguridad es el fraude sufrido por una empresa en Monterrey en 2023, que resultó en una pérdida de 3.4 millones de dólares debido a un ataque cibernético que involucró transferencias fraudulentas. Este tipo de incidentes pone de manifiesto la importancia de establecer marcos legales y normativos eficaces para prevenir y mitigar los efectos de los ciberataques.

8.2 El contexto internacional de la ciberseguridad

A nivel internacional, la ciberseguridad ha sido abordada desde diferentes perspectivas en diversas jurisdicciones. En Europa, la regulación de la ciberseguridad está mucho más avanzada. La Unión Europea, por ejemplo, ha implementado varias iniciativas para fortalecer la seguridad en el ciberespacio, destacando la Estrategia Digital de la UE y el Reglamento General de Protección de Datos (RGPD), que pone énfasis en la protección de la privacidad de los datos personales de los ciudadanos. A través de la Directiva de Ciberseguridad de la UE (NIS Directive), la región ha establecido políticas que requieren que los países miembros desarrollen medidas de seguridad para proteger infraestructuras críticas y servicios esenciales contra ciberataques.

La Directiva NIS establece normas para la seguridad de las redes y sistemas de información, promoviendo la cooperación entre los estados miembros de la UE y las empresas privadas en la protección contra amenazas cibernéticas. A la par, el RGPD ha sido un punto clave para garantizar que los datos personales de los ciudadanos estén protegidos de accesos no autorizados o de usos indebidos por parte de terceros, integrando medidas de ciberseguridad dentro de la gestión de la privacidad.

En Estados Unidos, la ciberseguridad también es una prioridad, y a nivel federal, existen leyes como el Cibersecurity Act de 2015, que tiene como objetivo mejorar la cooperación entre el sector público y privado en la defensa contra ciberataques. Además, la Ley de Protección de la Privacidad de la Información de los Consumidores de California (CCPA) establece estrictos estándares sobre cómo las empresas deben manejar la información

personal de los consumidores, con un enfoque significativo en la protección digital frente a amenazas cibernéticas.

Estos esfuerzos reflejan un enfoque integral donde la ciberseguridad no solo se ve desde una perspectiva técnica, sino también como una parte esencial de la protección de los derechos fundamentales de los individuos, como la privacidad y la seguridad.

8.3 Propuestas para la inclusión de la ciberseguridad en el marco constitucional y legal de México

Una de las principales propuestas para México es la creación de una ley integral de ciberseguridad que contemple aspectos más allá de la protección de datos personales. Esta ley debe abordar los diferentes aspectos de la ciberseguridad, incluyendo la protección de infraestructuras críticas, la regulación de los delitos cibernéticos y el establecimiento de un sistema robusto para la respuesta ante incidentes cibernéticos. La legislación debe garantizar que el Estado y las entidades privadas cuenten con las herramientas necesarias para prevenir y mitigar los efectos de los ciberataques.

Además, México debería incluir en esta ley el establecimiento de una agencia nacional encargada de supervisar y coordinar las acciones en ciberseguridad. Esta agencia podría ser responsable de la formación de los recursos humanos, de la elaboración de directrices para las empresas y del establecimiento de medidas preventivas en el sector público y privado.

8.4 Creación de un sistema de respuesta rápida y cooperación internacional

Otra propuesta clave es la creación de un sistema de respuesta rápida ante ciberincidentes, que permita a las autoridades y a las empresas privadas actuar de manera inmediata ante ataques cibernéticos. Este sistema podría incluir una red de expertos en ciberseguridad que colabore con organismos internacionales para intercambiar información sobre amenazas cibernéticas y mejores prácticas de defensa.

La cooperación internacional es esencial para enfrentar los ataques cibernéticos, que a menudo cruzan fronteras. México debe alinearse con las iniciativas internacionales, como el Convenio de Budapest sobre delitos cibernéticos, que promueve la cooperación internacional para combatir los delitos en línea. Al integrarse en estos acuerdos, México fortalecería su capacidad para enfrentar amenazas globales y proteger sus activos digitales.

8.5 Incentivar la educación en ciberseguridad

México también debe considerar la implementación de programas de educación en ciberseguridad en todos los niveles educativos. Estos programas deberían estar orientados a crear conciencia sobre los riesgos cibernéticos y promover buenas prácticas digitales. En el sector público, los funcionarios deben ser capacitados de manera continua sobre cómo manejar la información sensible y cómo responder ante las ciberamenazas.

Asimismo, las empresas privadas deben ser incentivadas a invertir en la capacitación de sus empleados y a establecer políticas internas que fomenten la ciberseguridad en el lugar de trabajo. Esto contribuiría a la creación de una cultura de seguridad digital tanto a nivel personal como profesional.

8.6 Fortalecimiento de la privacidad y la protección de datos

Finalmente, en un mundo donde los datos personales son un objetivo constante de los ciberdelincuentes, México debe fortalecer las políticas de privacidad y protección de datos. La inclusión de la ciberseguridad en la Constitución podría implicar una modificación del artículo 16, que se refiere a la protección de la privacidad, para incorporar explícitamente la protección de la información digital en un contexto de amenazas cibernéticas.

La ciberseguridad debe ser abordada como una prioridad nacional en México, y la legislación debe evolucionar para adaptarse a las nuevas realidades digitales. La creación de un marco legal integral que regule la ciberseguridad no solo protegerá las infraestructuras críticas y los datos personales, sino que también garantizará el derecho de los ciudadanos a un entorno digital seguro. A través de la cooperación internacional, el fortalecimiento de las capacidades nacionales y la integración de la ciberseguridad en los marcos constitucionales y legales, México podrá avanzar en la protección de su ciberespacio y en la defensa de los derechos fundamentales de sus ciudadanos.

8.7 Responsabilidad de los actores privados y públicos en la protección de datos digitales

En el contexto actual, donde la digitalización y el uso de tecnologías avanzadas son una constante en la vida cotidiana, la responsabilidad de los actores privados y públicos en la protección de los datos digitales se ha convertido en un tema central. Esto no solo implica el manejo y resguardo de la infor-

mación de los usuarios, sino también la adopción de medidas proactivas para evitar que se vean comprometidos datos sensibles. La responsabilidad de proteger los datos recae tanto en entidades públicas como privadas, con cada sector teniendo un papel esencial en la creación de un entorno digital seguro y confiable.

8.8 Responsabilidad de los actores públicos

Los actores públicos, en su rol como reguladores y supervisores, tienen la obligación de garantizar que las leyes y políticas relacionadas con la protección de datos sean claras, eficaces y estén alineadas con las mejores prácticas internacionales. En este sentido, los gobiernos deben implementar marcos regulatorios robustos y adaptativos que aborden las amenazas emergentes y permitan a las organizaciones públicas y privadas responder de manera efectiva ante incidentes de seguridad.

En México, por ejemplo, la Ley General de Protección de Datos Personales en Posesión de los Particulares establece obligaciones claras para las empresas en cuanto al manejo de la información personal, pero también impone responsabilidades a las entidades públicas. La autoridad encargada de supervisar el cumplimiento de esta ley, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), tiene la tarea de fiscalizar y garantizar que se respete el derecho de los ciudadanos a la privacidad y la seguridad de sus datos.

El gobierno también debe ser responsable de formar a los funcionarios públicos en los riesgos y mejores prácticas de ciberseguridad, asegurando que los sistemas y plataformas públicas sean resistentes a ciberataques. Además, tiene el deber de fomentar una cultura de transparencia y rendición de cuentas en el manejo de la información personal. Esto es crucial, especialmente cuando se manejan datos sensibles, como los relacionados con la salud o la justicia, ya que cualquier vulnerabilidad podría tener consecuencias devastadoras para los individuos afectados.

8.9 Responsabilidad de los actores privados

Por otro lado, las empresas y actores privados también juegan un papel crucial en la protección de los datos digitales. La responsabilidad privada se centra principalmente en la implementación de medidas de seguridad adecuadas para proteger los datos personales de sus clientes y empleados. Esto incluye, entre otras cosas, la adopción de prácticas como el cifrado de datos,

el uso de redes seguras, el monitoreo constante de los sistemas y la implementación de protocolos de respuesta ante incidentes.

Un aspecto fundamental que debe ser considerado es la necesidad de que las empresas realicen auditorías periódicas sobre la seguridad de sus sistemas, con el objetivo de identificar posibles vulnerabilidades. El cumplimiento de normativas internacionales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, es un ejemplo de cómo las empresas deben adoptar estándares que garanticen la privacidad de los datos. Si bien en México existen disposiciones legales como la Ley Federal de Protección de Datos Personales, el cumplimiento de estas normas aún es incipiente y muchas empresas carecen de los recursos para implementarlas adecuadamente.

En este sentido, se puede argumentar que las empresas deben ir más allá de lo estipulado por las normativas, adoptando una postura ética frente al manejo de la información. Esto no solo ayuda a proteger a los usuarios, sino que también refuerza la reputación y confianza en la marca, lo cual tiene un impacto positivo en el largo plazo.

8.10 Recomendaciones para la armonización internacional de normativas sobre ciberseguridad

La ciberseguridad es un tema que, por su naturaleza global, requiere de esfuerzos coordinados a nivel internacional. Los ciberataques no conocen fronteras, y las amenazas a la seguridad digital afectan a países de todo el mundo, independientemente de su nivel de desarrollo. Como resultado, la creación de normativas armonizadas en todo el mundo es fundamental para establecer una defensa coherente contra las amenazas cibernéticas.

8.11 Crear un marco regulatorio global consistente

Uno de los mayores desafíos en la ciberseguridad es la diversidad de marcos legales existentes en distintas jurisdicciones. Si bien países como la Unión Europea han logrado avances significativos con el RGPD, otros países aún carecen de un marco regulatorio que proteja adecuadamente a sus ciudadanos. Para promover la armonización internacional, sería necesario crear un tratado internacional que establezca directrices comunes sobre el manejo de datos, la respuesta ante ciberataques y la cooperación entre países.

Este tratado podría basarse en principios como la protección de la privacidad, la transparencia en el manejo de datos, la obligación de notificar las

violaciones de seguridad y la cooperación internacional en la lucha contra los cibercrímenes. Además, se podría establecer una plataforma internacional para compartir información sobre ciberamenazas y mejores prácticas, similar a lo que ya existe en el ámbito de la lucha contra el terrorismo.

8.12 Fomentar la colaboración público-privada

La colaboración entre los sectores público y privado es esencial para fortalecer la ciberseguridad global. Las empresas tienen acceso a información vital sobre amenazas cibernéticas y vulnerabilidades en sus sistemas, mientras que los gobiernos pueden ofrecer apoyo en términos de políticas públicas, recursos y legislación. Por lo tanto, es fundamental crear mecanismos que faciliten el intercambio de información y la colaboración en la identificación y mitigación de ciber amenazas.

A nivel internacional, organizaciones como la Organización de las Naciones Unidas (ONU) y la Interpol ya están promoviendo esta colaboración. No obstante, es necesario que los gobiernos impulsen políticas más ágiles y abiertas para facilitar la cooperación entre empresas, gobiernos y otras organizaciones internacionales.

8.13 Establecer estándares técnicos comunes

La armonización de las normativas sobre ciberseguridad también debe ir acompañada de la creación de estándares técnicos comunes. Estos estándares deben abordar aspectos clave como la protección de datos, la autenticación de usuarios, la encriptación de la información y la seguridad en las comunicaciones. La cooperación entre organismos internacionales como la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) es fundamental para establecer estos estándares.

Un ejemplo de esto es la norma ISO/IEC 27001, que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Esta norma es ampliamente adoptada por empresas y gobiernos en todo el mundo, pero su implementación debe ser promovida de manera más activa, especialmente en países en desarrollo que no han implementado mecanismos de seguridad adecuados.

8.14 Aumentar la capacitación y la conciencia global sobre ciberseguridad

Por último, es fundamental que a nivel internacional se promuevan programas de educación y concientización sobre ciberseguridad. Los gobiernos deben invertir en la formación de ciudadanos, funcionarios públicos y empresas para que comprendan la importancia de la ciberseguridad y las mejores prácticas para protegerse de amenazas cibernéticas.

En este contexto, México debería seguir el ejemplo de países como Estonia, que ha implementado un programa nacional de educación en ciberseguridad, que forma tanto a estudiantes como a profesionales. Esto no solo fortalecerá la seguridad interna, sino que también contribuirá a un entorno digital global más seguro.

La responsabilidad de proteger los datos digitales no solo recae en los actores públicos, sino también en las entidades privadas, que deben tomar medidas proactivas para garantizar la seguridad de la información. Para fortalecer la ciberseguridad global, es necesario que se armonicen las normativas y se fomente la cooperación internacional. Esto permitirá que se enfrenten de manera más efectiva las amenazas cibernéticas, que son cada vez más complejas y sofisticadas. México, en particular, debe avanzar en la implementación de leyes más robustas y promover una cultura de ciberseguridad tanto en el sector público como privado.

8.15 Reflexión sobre la necesidad de un marco jurídico actualizado para proteger la identidad digital en la era de la inteligencia artificial

En la era digital, la protección de la identidad digital se ha convertido en una prioridad para gobiernos, empresas y ciudadanos. A medida que las tecnologías evolucionan rápidamente, la ciberseguridad enfrenta retos nunca antes vistos, especialmente con el auge de la inteligencia artificial (IA), que promete transformar industrias, pero también representa un riesgo significativo para la privacidad y la seguridad de los individuos. La identidad digital, entendida como el conjunto de datos que nos representan en el mundo virtual, se ha vuelto uno de los activos más valiosos y, al mismo tiempo, más vulnerables.

Los avances en IA han abierto nuevas posibilidades, pero también han generado un escenario en el que la manipulación de datos personales y la creación de perfiles digitalizados son mucho más fáciles, rápidos y, a menudo, menos detectables. La velocidad con la que se procesan los datos, la capacidad de predicción y personalización de los sistemas basados en IA,

junto con la creciente interconexión de dispositivos, hace que la protección de la identidad digital sea una tarea sumamente compleja.

Los marcos jurídicos tradicionales, establecidos en su mayoría en un contexto donde las tecnologías digitales y los riesgos cibernéticos eran menos sofisticados, han quedado desactualizados. Es imprescindible crear un marco jurídico robusto y adaptable, capaz de abordar tanto las amenazas emergentes como las regulaciones internacionales. Este marco debe proteger el derecho a la privacidad y la integridad de la identidad digital, pero también debe incentivar la innovación y el desarrollo tecnológico responsable, sin frenar el progreso.

8.16 Desafíos actuales en la protección de la identidad digital

Uno de los principales desafíos es la falta de regulación unificada a nivel global. Mientras que regiones como la Unión Europea han avanzado significativamente con el Reglamento General de Protección de Datos (RGPD), en otras partes del mundo, como América Latina y Asia, la legislación en ciberseguridad y protección de datos personales es fragmentada y, en muchos casos, insuficiente. En México, aunque existen normativas como la Ley General de Protección de Datos Personales en Posesión de los Particulares, estas leyes aún no abarcan adecuadamente los nuevos riesgos planteados por las tecnologías emergentes, especialmente la IA. Esto crea un vacío legal en el que tanto las instituciones públicas como las empresas privadas tienen escasos incentivos para proteger de manera efectiva los datos sensibles de los usuarios.

Además, la inteligencia artificial, que cada vez está más presente en el análisis de grandes volúmenes de datos, puede utilizarse para crear perfiles detallados de individuos sin su consentimiento, y manipular estos datos con fines comerciales, políticos o de vigilancia. La capacidad de la IA para predecir comportamientos y tomar decisiones autónomas en base a datos personales exige una revisión crítica de las normativas existentes, ya que la privacidad ya no es una cuestión solo de control de acceso a la información, sino también de cómo esa información es utilizada para influir o predecir comportamientos.

8.17 Propuestas de estrategias legislativas y regulatorias para prevenir vulneraciones en ciberseguridad

La creación de un marco jurídico actualizado y coherente debe centrarse en varios ejes clave que garanticen una protección efectiva de la identidad digital. A continuación se presentan algunas estrategias legislativas y regulatorias fundamentales:

8.18 Establecimiento de normas internacionales unificadas

Es esencial que las normativas de protección de datos y ciberseguridad estén alineadas a nivel internacional para facilitar la cooperación transfronteriza. La creación de una normativa global sobre ciberseguridad, similar al Reglamento General de Protección de Datos de la Unión Europea (RGPD), podría establecer principios comunes que aseguren la protección de la identidad digital en todos los países. Esto permitiría evitar la fragmentación legal, promoviendo la interoperabilidad de los sistemas de seguridad a nivel global y reduciendo las brechas en la protección de datos entre jurisdicciones.

México, como parte activa de las organizaciones internacionales, debe trabajar hacia la creación de un acuerdo multilateral que establezca normas mínimas de ciberseguridad, con mecanismos de control, sanciones y cooperación internacional.

8.19 Fortalecimiento de la protección en la inteligencia artificial

La legislación debe evolucionar para abordar específicamente los desafíos planteados por la inteligencia artificial. Esto incluye la creación de principios claros sobre el uso ético de la IA, especialmente cuando se trata del procesamiento de datos personales. Las normativas deben exigir la transparencia en los algoritmos utilizados por las empresas y gobiernos, asegurando que los sistemas de IA sean auditables, y que los ciudadanos tengan acceso a la información sobre cómo sus datos son procesados y utilizados.

Además, debe garantizarse la existencia de mecanismos de control y auditoría que permitan evaluar el impacto de las decisiones tomadas por IA en los derechos de los individuos, en particular en lo que respecta a la privacidad y la no discriminación. Las leyes deben regular los casos en los que los sistemas de IA pueden generar perfiles detallados de individuos, y establecer límites claros sobre la automatización de decisiones que afectan a la vida de las personas.

8.20 Desarrollo de una cultura de ciberseguridad y privacidad digital

La prevención de vulneraciones en ciberseguridad requiere un enfoque integral, que involucre tanto a los actores públicos como privados. Es necesario que se promueva una cultura de ciberseguridad y privacidad en el ámbito empresarial, académico y gubernamental. Las empresas deben estar obligadas a implementar medidas de seguridad adecuadas, como la encriptación de datos, la autenticación multifactor, y el monitoreo constante de sus sistemas.

A nivel gubernamental, deben impulsarse campañas educativas para sensibilizar a los ciudadanos sobre la importancia de proteger su identidad digital, cómo evitar ser víctima de fraudes cibernéticos, y cómo manejar su información personal en plataformas en línea.

8.21 Implementación de sistemas de respuesta y recuperación rápida ante ciberincidentes

Otro componente crítico en la protección de la identidad digital es la capacidad de respuesta ante incidentes. Las leyes deben exigir que tanto las empresas como los organismos públicos cuenten con protocolos claros y eficaces para la gestión de incidentes de ciberseguridad. Esto incluye la notificación temprana de brechas de seguridad y la creación de sistemas de recuperación ante desastres que permitan mitigar los efectos de cualquier ataque cibernético.

Además, se debe incentivar la cooperación entre las distintas partes involucradas: empresas, gobiernos y organismos internacionales, para intercambiar información sobre amenazas emergentes y soluciones eficaces, mejorando así la respuesta global ante ciberincidentes.

8.22 Fortalecimiento de la autonomía y control de los ciudadanos sobre sus datos personales

Finalmente, es esencial que los ciudadanos cuenten con herramientas claras y accesibles para gestionar y proteger su identidad digital. Las leyes deben garantizar que las personas puedan ejercer el control sobre sus datos, decidiendo cómo, cuándo y con quién compartirlos. Esto incluye la implementación de derechos adicionales, como el derecho a la portabilidad de los datos y el derecho a la rectificación o eliminación de información incorrecta o desactualizada.

La creación de plataformas transparentes que permitan a los usuarios monitorear cómo se utilizan sus datos personales en tiempo real podría ser una de las soluciones tecnológicas más eficaces para lograr este objetivo. Además, las empresas y gobiernos deberían ser obligados a informar a los usuarios sobre sus derechos y garantizar un acceso fácil y gratuito a mecanismos de reclamación y resolución de disputas.

Conclusión

La ciberseguridad dejó de ser un asunto técnico o exclusivo de expertos: hoy es una condición indispensable para ejercer derechos fundamentales en un mundo profundamente digitalizado. Vivimos en una época en la que nuestras identidades, relaciones, trabajo y decisiones cotidianas transitan por plataformas digitales, sin embargo, el marco jurídico no ha evolucionado al mismo ritmo que las amenazas. Reconocer la ciberseguridad como un derecho humano emergente no es una exageración, es una necesidad urgente. A lo largo de este análisis quedó claro que el sistema legal mexicano presenta vacíos importantes en la protección de la identidad digital, especialmente frente a fenómenos complejos como los *deepfakes*, el *phishing*, o el uso indebido de *datos biométricos*. La desaparición del INAI no solo representa un retroceso institucional, sino que evidencia una falta de compromiso con la defensa de la privacidad como valor democrático.

Frente a este panorama, se vuelve imprescindible construir un marco jurídico integral, adaptable y con visión de futuro. Uno que incorpore principios de justicia digital, educación tecnológica y enfoque de derechos humanos. La ciberseguridad debe dejar de ser una preocupación aislada para convertirse en una política pública transversal. Solo así podremos garantizar que el entorno digital no solo sea innovador, sino también seguro, justo y verdaderamente humano.

Bibliografía

Agencia Española de Protección de Datos (AEPD), *Guía sobre el uso de tecnologías de reconocimiento facial*, 2021. www.aepd.es/guias/guia-control-presencia-biometrico.pdf (fecha de consulta: 6 de abril de 2025).

California State Legislature, *California Consumer Privacy Act (CCPA)*, 2018. https://oag.ca.gov/privacy/ccpa (fecha de consulta: 30 de marzo de 2025).

Constitución Política de los Estados Unidos Mexicanos, art. 6° y 16°. (fecha de consulta: 1 de abril de 2025).

De Hert, Paul y Papakonstantinou, Vagelis, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, vol. 28, núm. 2, 2012, pp. 130–142. https://doi.org/10.1016/j.clsr.2012.01.006

Deepfakes: el nuevo reto legal y ético en la era de la desinformación, 2025. blog.cipi.es/blog2-nntt/item/263-deepfakes-el-nuevo-reto-legal-y-etico-en-la-era-de-la-desinformacion (fecha de consulta: 2 de abril de 2025).

Derechos Digitales América Latina, "Ciberseguridad: más allá de la concientización", 2024. https://www.derechosdigitales.org/24488/ciberseguridad-mas-alla-de-la-concientizacion/ (fecha de consulta: 8 de abril de 2025).

Derechos Digitales, *Agencia Nacional de Ciberseguridad en Chile: panorama normativo e institucional*, s.f. www.derechosdigitales.org/wp-content/uploads/Ciberseguridad-en-Chile-panorama-normativo-e-institucional.pdf (fecha de consulta: 1 de abril de 2025).

El Economista, "México enfrenta desafíos sin precedentes en ciberseguridad", 2025. www.eleconomista.com.mx/tecnologia/Ciberseguridad-en-Mexico-entre-la-inmadurez-y-la-conciencia--20240503-0095.html (fecha de consulta: 1 de abril de 2025).

El País, "La CURP con datos biométricos: ¿avance o riesgo?", 2025. https://elpais.com (fecha de consulta: 2 de abril de 2025).

El Universal, "Adiós al INAI tras 22 años desaparece en medio de escándalos", 2024. www.eluniversal.com.mx/nacion/adios-al-inai-tras-22-anos-desaparece-en-medio-de-escandalos/com (fecha de consulta: 2 de abril de 2025).

Floridi, Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford, Oxford University Press, 2014.

Mejía, Laura, "El fin del INAI y sus repercusiones en el derecho a la información", *Revista Digital de Derecho Público*, 2025. https://revistaderechopublico.org (fecha de consulta: 4 de abril de 2025).

Meristation, "Hackers explotan inteligencia artificial para vulnerar redes de empresas", 2025. https://as.com/meristation (fecha de consulta: 6 de abril de 2025).

Microsoft, *Informe anual de defensa digital 2024*. https://www.microsoft.com/es-es/security/business/digital-defense-report (fecha de consulta: 6 de abril de 2025).

Organización de los Estados Americanos (OEA), *Estudio sobre la protección de datos personales en las Américas*, 2022. https://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp (fecha de consulta: 8 de abril de 2025).

Parlamento Europeo y Consejo de la Unión Europea, *Reglamento (UE) 2016/679*..., Diario Oficial de la Unión Europea, 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679 (fecha de consulta: 8 de abril de 2025).

Rodríguez, Luis Fernando, "La protección de la privacidad frente a los algoritmos", *Revista Latinoamericana de Derecho y Tecnología*, año 2, núm. 4, 2020, pp. 99–124. (fecha de consulta: 8 de abril de 2025).

Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, Nueva York, W. W. Norton & Company, 2015.

Solove, Daniel J., "A taxonomy of privacy", *University of Pennsylvania Law Review*, vol. 154, núm. 3, 2006, pp. 477–560.

Stark, Michael, "Artificial intelligence and cybersecurity threats", *Cyberlaw Review*, vol. 34, núm. 2, 2024, pp. 77–89.

Suprema Corte de Justicia de la Nación (SCJN), *Criterios del Poder Judicial de la Federación en materia de Protección de Datos Personales y otros conceptos relacionados*. https://www.scjn.gob.mx/sites/default/files/pagina_transparencia/documento/2018-11/CriteriosPJF_Proteccion_Datos_2a_Ed_Digital_2018.pdf (fecha de consulta: 8 de abril de 2025).

Tufekci, Zeynep, "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency", *Colorado Technology Law Journal*, vol. 13, 2015. https://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf (fecha de consulta: 8 de abril de 2025).

Welivesecurity, "Tendencias en ciberseguridad 2025: uso malicioso de la IA generativa y tecnologías operativas en la mira", 2025. https://mundoti.net (fecha de consulta: 8 de abril de 2025).

World Compliance Association, "El impacto de la inteligencia artificial en la protección de datos personales", 2020. www.worldcomplianceassociation.com/2767/articulo-el-impacto-de-la-inteligencia-artificial-en-la-proteccin-de-datos-personales.html (fecha de consulta: 2 de abril de 2025).

World Economic Forum, *Global Cybersecurity Outlook 2023*. https://www.weforum.org/reports/global-cybersecurity-outlook-2023 (fecha de consulta: 9 de abril de 2025).

Sobre la autora

Olga Patricia Chávez Ávila. Investigadora independiente.
https://orcid.org/0009-0004-5797-5922 *olgapatriciachavezavila@gmail.com*