SENADO DE LA REPÚBLICA
DEL H. CONGRESO DE LA UNIÓN
LXV LEGISLATURA

De las **Senadoras Alejandra Lagunes Soto Ruíz**, **Xóchitl Gálvez Ruiz y los Senadores Jorge Carlos Ramírez Marín, Gustavo Madero Muñoz** y **Miguel Ángel Mancera Espinoza** integrantes de la LXV Legislatura del H. Congreso de la Unión, de conformidad con lo previsto en los artículos 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos; 8, numeral 1, fracción I, 164 y 169 del Reglamento del Senado de la República, someto a la consideración de esta Soberanía el siguiente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA LA FRACCIÓN XVII, AL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, EN MATERIA DE INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD Y NEURODERECHOS** con base en las siguientes:

EXPOSICIÓN DE MOTIVOS

En un estudio realizado por la Universidad de Pensilvania[1], se investigan las posibles implicaciones que los modelos Generative Pre-trained Transformer (GPT) y otras tecnologías relacionadas pueden tener en el mercado laboral.

Se utilizaron nuevas métricas para evaluar las ocupaciones en función de su correspondencia con las capacidades de GPT, incorporando tanto la experiencia humana como las clasificaciones de GPT-4. Los resultados indican que aproximadamente el 80% de la fuerza laboral estadounidense podría ver afectado al menos el 10% de sus tareas laborales con la introducción de GPT, mientras que alrededor del 19% de los trabajadores podrían ver afectado al menos el 50% de sus tareas.

La influencia abarca todos los niveles salariales, y los trabajos de ingresos más altos podrían enfrentar una mayor exposición. Cabe destacar que el impacto no se limita a las industrias con un mayor crecimiento reciente de la productividad. Se concluye que los Generative Pre-trained Transformers presentan características de tecnologías de propósito general (GPT), lo que sugiere que estos modelos podrían tener notables implicaciones económicas, sociales y políticas.

[1] Eloundou, T., Manning, S., Mishkin, P., & Rock, D. (2023, 21 marzo). GPTs are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models. arxiv.org. Recuperado 23 de marzo de 22d. C., de https://arxiv.org/pdf/2303.10130.pdf

Por otro lado, la inteligencia artificial puede representar grandes riesgos a la privacidad. De manera inicial, la IA requiere grandes cantidades de datos para entrenar y mejorar su rendimiento, por lo que la recopilación de estos datos puede poner en riesgo la privacidad de las personas, si esta se realiza sin su consentimiento o se utiliza para fines distintos a los establecidos originalmente.

Asimismo, una vez obtenidos los datos es importante asegurarse de que los datos se almacenen de manera segura y se protejan de posibles amenazas de seguridad. De modo que es importante que los sistemas de IA sean transparentes y comprensibles para los usuarios finales, para que estos puedan entender cuál es el uso que se le da a sus datos. Hasta el 49% de los trabajadores podrían tener expuestas la mitad o más de sus tareas a Modelos de Lenguaje de Aprendizaje Profundo (LLM).

Los hallazgos muestran que la mayoría de las ocupaciones presentan cierto grado de exposición a LLM, con niveles de exposición variables en diferentes tipos de trabajo. Las ocupaciones con salarios más altos generalmente presentan una alta exposición, un resultado contrario a evaluaciones similares de exposición general al aprendizaje automático.

Se descubrió que los roles que dependen en gran medida de habilidades científicas y de pensamiento crítico muestran una correlación negativa con la exposición, mientras que las habilidades de programación y escritura están positivamente asociadas con la exposición a LLM. Además, se descubrió que la exposición ocupacional a LLM aumenta débilmente con la dificultad de la preparación del trabajo.

Se analiza la exposición por industria y se descubre que las industrias de procesamiento de información exhiben una alta exposición, mientras que la fabricación, la agricultura y la minería muestran una exposición más baja. La conexión entre el crecimiento de la productividad en la última década y la exposición general a LLM parece débil. En resumen, los impactos de LLM como GPT-4 son probablemente generalizados y su efecto económico se espera que persista y aumente incluso si detenemos el desarrollo de nuevas capacidades hoy en día. Los LLM son una tecnología de propósito general (GPT) y, como con otras tecnologías de propósito general, gran parte de su potencial surgirá en una amplia gama de casos de uso económicamente valiosos.

Se presentan varias conclusiones sobre la relación entre los salarios, el empleo y las habilidades requeridas en los trabajos y la exposición a los modelos de lenguaje de IA. Se muestra la intensidad de la exposición en la economía en términos de trabajadores y ocupaciones. Se observa que la concentración de trabajadores en ciertas ocupaciones no tiene una fuerte correlación con la exposición a los modelos de lenguaje de IA. Además, se encontró que los trabajos con salarios más altos tienden a estar más expuestos a estos modelos.

En la sección "Importancia" se examina la relación entre la importancia de una habilidad para una ocupación (según lo anotado en el conjunto de datos de O*NET) y las medidas de exposición a los modelos de lenguaje de IA. Se encontró que las habilidades de ciencias y pensamiento crítico tienen una fuerte asociación negativa con la exposición, mientras que las habilidades de programación y escritura tienen una fuerte asociación positiva con la exposición.

En la sección "Educación requerida", se analiza la relación entre el nivel de educación requerido para ingresar a un trabajo y la exposición a los modelos de lenguaje de IA. Se encontró que las personas con títulos universitarios y de posgrado están más expuestas a estos modelos que aquellas sin credenciales educativas formales. Además, los trabajos que requieren menos capacitación en el trabajo tienen una mayor exposición a los modelos de lenguaje de IA.

En resumen, este estudio ofrece un examen del impacto potencial de los LLMs, específicamente los GPTs, en varias ocupaciones e industrias dentro de la economía de Estados Unidos. Al aplicar una nueva herramienta para entender las capacidades de los LLMs y sus posibles efectos en los trabajos, se observa que la mayoría de las ocupaciones tienen cierto grado de exposición a los GPTs, siendo las ocupaciones de mayor salario las que presentan más tareas con alta exposición. El análisis indica que aproximadamente el 19% de los trabajos tienen al menos el 50% de sus tareas expuestas a los GPTs, considerando tanto las capacidades actuales de los modelos como el software impulsado por GPTs anticipado.

El objetivo de la investigación es resaltar el potencial de los GPTs y sus posibles implicaciones para los trabajadores estadounidenses. Los hallazgos confirman la hipótesis de que estas tecnologías pueden tener impactos generalizados en una amplia variedad de ocupaciones en Estados Unidos, y que los avances adicionales respaldados por GPTs, principalmente a través de software y herramientas digitales, pueden tener efectos significativos en diversas actividades económicas.

Sin embargo, aunque la capacidad técnica de los GPTs para hacer que el trabajo humano sea más eficiente parece evidente, es importante reconocer que factores sociales, económicos, regulatorios y otros pueden influir en los resultados reales de la productividad laboral. A medida que las capacidades sigan evolucionando, es probable que el impacto de los GPTs en la economía persista y aumente, planteando desafíos para los responsables de políticas al predecir y regular su trayectoria.

El 21 de marzo de 2018, se presentó el informe **"En miras hacia una Estrategia de Inteligencia Artificial (IA) en México: Aprovechando la Revolución de IA"**[2], realizado por Oxford Insights, C-Minds y comisionado por la Embajada Británica en México en cooperación con el Gobierno de la República. Este estudio contenía un análisis sobre las ventajas,

[2] Disponible en: https://datos.gob.mx/blog/estrategia-de-inteligencia-artificial-mx-2018

oportunidades y desafíos de México en la materia, así como recomendaciones en el corto, mediano y largo plazo para todos los sectores de la sociedad.

La estrategia contemplaba el desarrollo de un marco de gobernanza adecuado para fomentar el diálogo multisectorial, el mapeo de los usos y necesidades en la industria, el impulso del liderazgo internacional de México en la materia, la publicación de las recomendaciones realizadas por el informe a consulta pública y el trabajo con expertos y ciudadanos mediante la Subcomisión de Inteligencia Artificial para alcanzar la continuidad de estos esfuerzos durante la siguiente administración.[3]

Con el lanzamiento de este informe y la Estrategia IA-MX, **México se convirtió en uno de los primeros 10 países en contar con acciones claras para fomentar el desarrollo, adopción y uso de la Inteligencia Artificial en el mundo.[4]**

Desde la presentación de la Estrategia de Inteligencia Artificial de México en 2018, se han conseguido diversos avances legislativos en el país para fomentar, regular, adoptar y aprovechar la Inteligencia Artificial. Algunos de estos avances son:

- **Ley de Fomento a la Confianza Ciudadana:** En 2019, se promulgó la Ley de Fomento a la Confianza Ciudadana, que establece la creación de un Comité Nacional de Ética y Tecnologías Emergentes, encargado de promover el uso responsable y ético de las tecnologías emergentes, incluyendo la Inteligencia Artificial.[5]
- **Ley de Protección de Datos Personales:** En 2020, se promulgó la Ley Federal de Protección de Datos Personales en Posesión de Particulares, que establece medidas para proteger la privacidad de las personas en el contexto de la recopilación, procesamiento y uso de datos personales, incluyendo aquellos generados por sistemas de Inteligencia Artificial.[6]
- **Estrategia Nacional de Inteligencia Artificial:** En 2018, se presentó la Estrategia Nacional de Inteligencia Artificial, que tiene como objetivo promover el desarrollo y la adopción de la Inteligencia Artificial en el país, a través de la inversión en investigación, el desarrollo de capacidades, la colaboración público-privada y la promoción de un marco ético y regulatorio.
- **Laboratorio Nacional de Inteligencia Artificial:** En 2021, se inauguró el Laboratorio Nacional de Inteligencia Artificial, con el objetivo de promover la investigación, el desarrollo y la transferencia de tecnología en el campo de la Inteligencia Artificial, así

[3] Zapata, E. (2017, marzo). Estrategia de Inteligencia Artificial MX 2018. Gobierno de México.

[4] Ibid

[5] (Ley de Fomento a la Confianza Ciudadana, 2023). 2020, México.

[6] (Ley Federal de Protección de Datos Personales, 2023). 2010, México.

como de fomentar la colaboración entre el sector público, el sector privado y la academia.[7]

En general, si bien aún queda mucho por realizar en materia de Inteligencia Artificial en México, estos avances legislativos son un paso importante hacia la promoción de un uso responsable, ético y beneficioso de la tecnología en el país.

Por otro lado, el día 15 de marzo de 2023, la Comisión de Ciencia y Tecnología del Senado de la República realizó el primer conversatorio sobre inteligencia artificial titulado **"Conversatorio sobre Inteligencia Artificial: Retos, riesgos y oportunidades"**, donde se discutió el tema con diversos legisladores y personas expertas en la materia.

Espacio en el que se habló sobre la responsabilidad y rendición de cuentas, los sesgos y discriminación en las diversas Inteligencias Artificiales, privacidad y seguridad, educación y fuerza laboral, y cooperación internacional.

En este conversatorio se registraron diversas conclusiones tendientes a que es urgente y necesario promover el uso y estudio de la inteligencia artificial en México, bajo un enfoque ético, responsable y sostenible de esta tecnología.

Asimismo, se mencionó que es esencial para una política en materia de IA contar con alta conectividad, educación y alta velocidad en el ámbito tecnológico. Para poder llegar a esto es esencial entender cuál es el papel que México quiere jugar en la IA.

Más allá, dentro de la mención de desafíos se presentaron tres limitaciones éticas a la IA. En primer lugar se comentó que aquellas personas que se dedican a la ciberdelincuencia pueden crear contenido malicioso de forma automática y generar correos de phishing mucho más reales.

Esto puede provocar que las personas sean más propensas a caer en fraudes o engaños que les hagan proporcionar sus datos personales. En segundo lugar, está la preocupación por la generación de desinformación. No cabe duda de que la Inteligencia Artificial genera respuestas muy acertadas, sin embargo, porque aún el sistema se está entrenando, aún se presentan inconsistencias en la investigación y verificación de los hechos. Por último, los sesgos de información pueden fomentar ideas basadas en preferencias específicas de género, política, economía, entre otras. No cabe duda de que la IA genera respuestas muy acertadas, sin embargo, porque aún el sistema se está entrenando, se presentan inconsistencias en la investigación y verificación de los hechos que la IA genera.

[7] Laboratorio de Inteligencia Artificial Microsoft. (s. f.). http://www.ai.unam.mx/

Ciberseguridad

Incorporar el concepto de ciberseguridad en nuestra Carta Magna es de suma importancia en la era digital actual por varias razones fundamentales:

- Protección de datos personales: Crear leyes sobre ciberseguridad permitirá garantizar la privacidad y la protección de los datos personales de los individuos. Con la creciente cantidad de información sensible que se almacena y transmite en línea, las regulaciones de ciberseguridad ayudan a establecer estándares para la recopilación, el almacenamiento y el uso adecuado de estos datos.
- Prevención de ciberataques: Las leyes de ciberseguridad establecen medidas de seguridad y requisitos para organizaciones y proveedores de servicios en línea, lo que puede ayudar a prevenir ciberataques. Al hacer cumplir políticas de seguridad sólidas, se reduce la probabilidad de brechas de seguridad y se protegen los sistemas y datos críticos.
- Responsabilidad legal: Establecer leyes relacionadas con la ciberseguridad también define responsabilidades legales claras en caso de incidentes cibernéticos. Esto puede ayudar a determinar quién es responsable de los daños y las pérdidas en caso de que ocurra un ciberataque, lo que facilita la aplicación de la ley y la compensación a las víctimas.
- Protección de la infraestructura crítica: Las leyes de ciberseguridad pueden estar dirigidas a proteger la infraestructura crítica, como sistemas de energía, transporte y salud. Esto es crucial para garantizar el funcionamiento continuo de servicios esenciales y la seguridad nacional.
- Prevención del cibercrimen: La legislación en ciberseguridad también puede ayudar en la lucha contra el cibercrimen al establecer penas y sanciones para actividades ilegales en línea, como el robo de datos, el fraude cibernético y los ataques informáticos maliciosos.
- Fomento de la confianza en línea: Cuando los usuarios tienen la confianza de que sus datos están protegidos y sus actividades en línea son seguras, es más probable que participen activamente en la economía digital y utilicen servicios en línea, lo que beneficia a la sociedad en general.

La ciberseguridad es una de las principales preocupaciones alrededor del mundo. Cada día hay más plataformas digitales y el ciberespacio se ha convertido en el mercado objetivo de muchas empresas internacionales por su potencial de crecimiento y capacidad. Por otro lado, jóvenes de todo el mundo consumen información con solo un click. Además, los gobiernos y sus infraestructuras críticas dependen enormemente del Internet. Esto aumenta el riesgo de ciberataques para todas las organizaciones e instituciones privadas o públicas.

De todos los crímenes, el cibercrimen es el que se está propagando más rápido. Por lo que la protección de brechas de datos, ataques de ransomware, phishing, usurpación de identidad, entre otros, se han convertido en uno de los principales objetivos tanto de empresas como de instituciones de gobierno. Algunos investigadores predijeron que la ciberdelincuencia será la causa de la próxima guerra mundial y que el país que logre combatirla será la próxima potencia mundial.

Pero, no solo empresas y gobiernos se ven afectados por este fenómeno. El cibercrimen también afecta a las personas usuarias de Internet. Cisco, prevé que para el año 2023 habrá 30,000 millones de dispositivos conectados a Internet. Cada dispositivo conectado ya sea una cámara, computadora portátil, celular, bocina o televisión inteligente, representa una superficie de ataque en la que hackers pueden acceder sin autorización y extraer nuestra información.

De ahí la importancia de aprender a cuidarnos de terceras personas que buscan acceder a nuestro contenido sin nuestra autorización. Y, aunque la prevención es sumamente importante para prevenir ciberdelitos, debemos actualizar e innovar en materia legislativa.

En México, el panorama de la ciberdelincuencia es preocupante. En 2019 Pemex sufrió un ciberataque, en 2022 la Secretaría de la Función Pública (Condusef) fue hackeada y expuso las declaraciones patrimoniales de 830 mil funcionarios públicos, la Lotería Nacional, el SAT y Banxico son otras instituciones que han sido víctimas del cibercrimen. En fechas más recientes, la SEDENA dejó expuesta la frágil y débil política de ciberseguridad de México, al haber experimentado el hackeo más grande de la historia de nuestro país.

Necesitamos adoptar una visión de largo plazo que resuelva los problemas a los que nos enfrentamos en materia de tecnología y seguridad. Si protegemos los entornos digitales, estaremos protegiendo la seguridad de todas las personas usuarias de Internet, de empresas y de las instituciones públicas. Además, México se estaría convirtiendo en un país con una visión innovadora y como referente en América Latina.

La ciberseguridad no se limita al gobierno o a las infraestructuras críticas, cibercriminales atacan a las y los mexicanos todos los días, y la ciberseguridad consiste en protegerlos a ustedes y los servicios de los que dependemos. Esta semana nacional de ciberseguridad, les invito a que aumenten su ciberseguridad en casa, en el trabajo y en las escuelas, tomando medidas como el uso de la autenticación multifactorial, el uso de un gestor de contraseñas de confianza y de contraseñas seguras, el reconocimiento y la denuncia de la suplantación de identidad y la actualización periódica del software.

Neuroderechos

Los neuroderechos son un concepto emergente en el campo de la ética y los derechos humanos que se centra en la protección de la integridad y la autonomía de los individuos en relación con sus cerebros y sus sistemas nerviosos. Estos derechos buscan abordar las cuestiones éticas y legales relacionadas con avances en neuro tecnología[8] y neurociencia que pueden tener un impacto profundo en la privacidad, la identidad y la autodeterminación de las personas.

En 2019, el neurocientífico Rafael Yuste[9], director del Centro de Neuro tecnología de la Universidad de Columbia de Estados Unidos y principal impulsor del proyecto BRAIN[10], publicó un experimento en el que mediante electrodos implantados en el cerebro de ratas podía hacer que los animales vieran cosas que en realidad no estaban ahí. En otras palabras, los investigadores estaban controlando la actividad de su cerebro. Según Yuste, y otros científicos en todo el mundo, es solo cuestión de tiempo que se pueda hacer algo similar con seres humanos y por eso es urgente definir y reconocer los neuro derechos de las personas.

La estimulación cerebral profunda mediante electrodos implantados en el cerebro es un avance en el campo de la biotecnología que ya se ha usado con éxito para, por ejemplo, mejorar los síntomas de las personas que sufren de Parkinson o epilepsia. El proyecto Neuralink[11] de Elon Musk, tiene como objetivo desarrollar una interfaz bidireccional capaz no sólo de estimular partes del cerebro, sino también de recibir e interpretar las señales que provienen de él.

Una vez establecida esta conexión, y mediante el uso de inteligencia artificial, sería posible identificar emociones, controlar dispositivos o inducir estados. Algunos científicos consideran que una versión futura muy sofisticada de este sistema, u otro similar, podría leer los pensamientos de una persona, acceder a su memoria e, incluso, controlar ambos, lo que ven como un peligro potencial para la humanidad.

Los neuro derechos se pueden definir como un nuevo marco jurídico internacional de derechos humanos destinados específicamente a proteger el cerebro y su actividad a medida que se produzcan avances en neuro tecnología. El concepto ha sido desarrollado por la plataforma NeuroRights Initiative[12], se abre en ventana nueva., liderada por la ya citada Universidad de Columbia en Nueva York e impulsada por una comunidad internacional de neurocientíficos.

---

[8] Ética de la neurotecnología, UNESCO disponible en: https://www.unesco.org/es/ethics-neurotech

[9] Consultar: https://www.elmundo.es/tecnologia/innovacion/working-progress/2023/03/26/641dc4e221efa078638b45d5.html

[10] Proyecto BRAIN: qué es y cómo pretende mapear el cerebro humano. Disponible en: https://psicologiaymente.com/neurociencias/proyecto-brain

[11] Sitio oficial de Neuralink, disponible: https://neuralink.com/

[12] Sitio oficial disponible en: https://neurorightsfoundation.org/

Se entiende por neuro tecnología cualquier tecnología que registre información procedente de la actividad cerebral o interfiera con ella. Combinada con la inteligencia artificial, tiene el potencial de alterar la sociedad de manera fundamental, según afirman los científicos al frente de la iniciativa. El trabajo de la organización se centra, por tanto, en desarrollar un código deontológico para los científicos implicados en neuro tecnología y en el reconocimiento internacional de los cinco neuro derechos:

1. **Identidad personal** Consiste en limitar cualquier neuro tecnología que permita alterar el sentido del yo de las personas y en evitar que la identidad personal se pierda con la conexión a redes digitales externas.

2. **Libre albedrío** Se refiere a preservar la capacidad de las personas de tomar decisiones de forma libre y autónoma, es decir, sin manipulación alguna mediada por parte de las neuro tecnologías.

3. **Privacidad mental** Protege a las personas del uso de los datos obtenidos durante la medición de su actividad cerebral sin su consentimiento y prohíbe expresamente cualquier transacción comercial con esos datos.

4. **Acceso equitativo** Busca la regulación en la aplicación de las neuro tecnologías para aumentar las capacidades cerebrales, de manera que no queden solo al alcance de unos pocos y generen desigualdad en la sociedad.

5. **Protección contra los sesgos** Evita que las personas sean discriminadas por cualquier factor, como pudiera ser un mero pensamiento, que se pueda obtener mediante el uso de las neuro tecnologías.

En los últimos años, la regulación de los neuro derechos ha registrado avances en varios lugares del mundo. Chile fue el primer país del mundo en aprobar una modificación en su constitución para incluir los derechos digitales y la protección de la "integridad mental" ante el avance de las neuro tecnologías. Muchos otros países están adoptando los ciber derechos en un contexto de transformación digital con el objeto de que dicho proceso ponga a las personas en el centro.

Algunos aspectos que esta reforma constitucional se podrán considerar bajo el paraguas de los neuro derechos incluyen:

- Privacidad cerebral: La protección de la privacidad de la información generada por el cerebro, como las señales neuronales, las imágenes cerebrales y los datos de neuro tecnología. Esto es especialmente relevante en un mundo donde la neuro vigilancia y la capacidad de leer o influir en la mente de una persona están en constante evolución.

- Autonomía cognitiva: Garantizar que las personas tengan control sobre sus procesos mentales y decisiones cognitivas, incluso cuando están interfiriendo con la ayuda de neuro tecnologías como la estimulación cerebral profunda o la modificación cognitiva.
- Consentimiento informado: Asegurarse de que las personas comprendan completamente los riesgos y las implicaciones de cualquier procedimiento o tecnología relacionada con el cerebro antes de dar su consentimiento para su uso.
- Identidad y autoexpresión: Proteger la integridad de la identidad personal y la expresión de uno mismo frente a intervenciones que puedan alterar la personalidad, la memoria o la cognición.
- No discriminación: Evitar la discriminación basada en características cerebrales o neurológicas, y garantizar que las personas con discapacidades neurológicas tengan igualdad de oportunidades.
- Acceso equitativo a beneficios: Asegurarse de que los avances en neurociencia y neuro tecnología estén disponibles para todos y no creen desigualdades sociales o económicas.

Estos derechos son relevantes para abordar las cuestiones éticas y sociales en evolución relacionadas con la neurociencia y la neuro tecnología.

Si se continúa con esta tendencia, todos los pensamientos deconstruidos respecto a los roles de género o las comunidades afrodescendientes, se verán reforzados nuevamente por el simple hecho de que existen algoritmos entrenados con esos estereotipos.

I. CONTENIDO DE LA INICIATIVA

Dotar al Congreso de la Unión la facultad de legislar sobre ciberseguridad, inteligencia artificial y neuro derechos es de vital importancia en la era digital y tecnológica en la que vivimos. Si bien, se han incorporado las tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, resulta de vital importancia reconocer que:

La ciberseguridad se ha convertido en un elemento fundamental para proteger la infraestructura crítica, los datos personales y la estabilidad de las naciones. Permitir al Congreso legislar en este ámbito garantiza la creación de leyes y regulaciones adecuadas para hacer frente a las amenazas cibernéticas cada vez más sofisticadas y para proteger la privacidad de los ciudadanos.

La inteligencia artificial está transformando profundamente la economía y la sociedad. La regulación en este campo es esencial para abordar cuestiones éticas, como la discriminación

algorítmica, y para garantizar la seguridad y la responsabilidad en el desarrollo y su uso. El Congreso tiene el deber de establecer marcos legales que promuevan la innovación y al mismo tiempo protejan los derechos y la equidad de las personas.

Los neuro derechos son un campo emergente que se refiere a la protección de la integridad mental y la privacidad del individuo en un mundo cada vez más conectado a la neuro tecnología. Con la creciente capacidad de leer y manipular la mente humana, es esencial que el Congreso establezca límites y garantías legales para proteger los derechos fundamentales de las personas en este ámbito.

Esta actualización constitucional para incorporar la facultad de legislar sobre ciberseguridad, inteligencia artificial y neuro derechos es esencial para proteger los intereses y derechos de los mexicanos en la era digital. Estas áreas están en constante evolución y plantean desafíos únicos que requieren una regulación adecuada para garantizar la seguridad, la privacidad y la equidad en un mundo cada vez más tecnológico.

Para mayor referencia, a continuación se ilustra la modificación constitucional planteada.

Texto vigente	Texto propuesto
Artículo 73. El Congreso tiene facultad:	**Artículo 73**. …
I a la XVI. …	I a la XVI. …
XVII. Para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal.	XVII. Para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, **así como sobre inteligencia artificial y sus aplicaciones, ciberseguridad, neuro derechos,** postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal.
XVIII a la XXXI. …	XVIII a la XXXI. …

En atención a lo anteriormente expuesto, sometemos a consideración de este Honorable Pleno la siguiente iniciativa, con proyecto de:

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA LA FRACCIÓN XVII, AL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, EN MATERIA DE INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD Y NEURODERECHOS

ARTÍCULO ÚNICO. – Se reforma la fracción XVII, al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73.-

I a la XVI. …

XVII. Para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, así como sobre inteligencia artificial y sus aplicaciones, ciberseguridad, neuro derechos, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal.

XVIII a la XXXI. …

TRANSITORIOS

PRIMERO. El presente decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO. El Congreso de la Unión deberá realizar las reformas a la legislación secundaria correspondiente que regulen la inteligencia artificial, ciberseguridad y neuro derechos, a más tardar en un plazo de 180 días a partir de la entrada en vigor del presente decreto.

Salón de Sesiones de la Cámara de Senadores del H. Congreso de la Unión, sede de la Comisión Permanente, 20 de septiembre de 2023.

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA LA FRACCIÓN XVII, AL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, EN MATERIA DE INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD Y NEURO DERECHOS

Sen. Alejandra Lagunes Soto Ruiz	Sen. Xóchitl Gálvez Ruiz
Sen. Jorge Carlos Ramírez Marín	Sen. Gustavo Madero Muñoz
Sen. Miguel Ángel Mancera Espinoza	