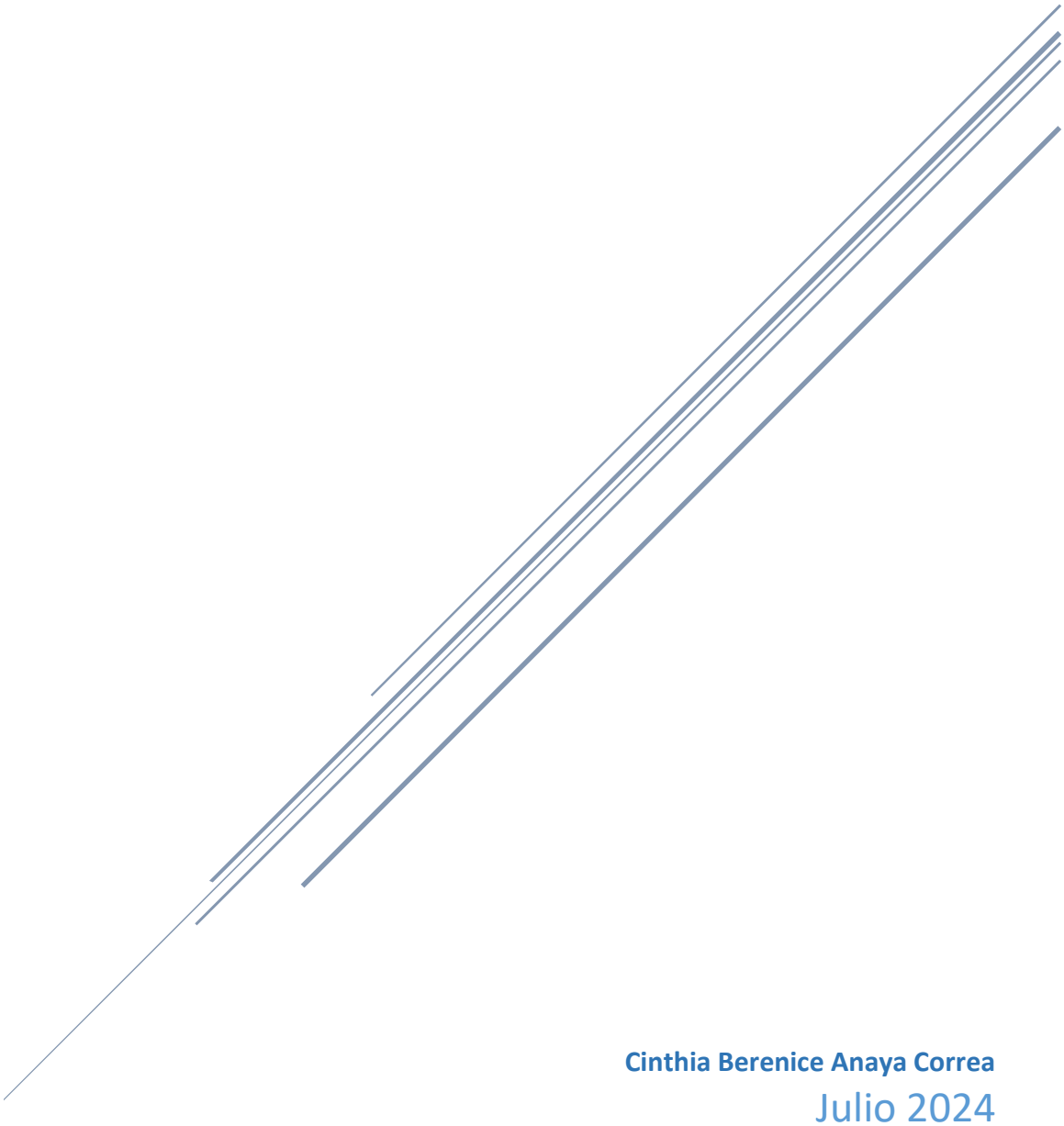
# Inteligencia artificial y violencia de género



**Cinthia Berenice Anaya Correa**

Julio 2024




## Resumen

La regulación de la inteligencia artificial y otras tecnologías digitales debe incluir una perspectiva de género que garantice la protección de las mujeres contra el acoso, la vigilancia no consentida, la manipulación de información y otras formas de abuso digital. Esto no solo implica la creación de leyes específicas, sino también la implementación de políticas públicas que promuevan la educación digital, la alfabetización en derechos digitales y el fortalecimiento de las capacidades institucionales para enfrentar estos desafíos.

La prevención y atención de la violencia de género no solo es un imperativo de derechos humanos, sino que también es esencial para la creación de sociedades más justas, equitativas y prósperas. En el contexto actual de México, es fundamental avanzar en la implementación efectiva de las leyes existentes, así como en la creación de nuevas regulaciones que aborden las formas emergentes de violencia, incluidas aquellas mediadas por tecnologías como la inteligencia artificial. Solo a través de un enfoque integral y coordinado se podrá avanzar en la erradicación de la violencia de género y en la construcción de una sociedad verdaderamente igualitaria.

**Índice**

I. Introducción……1

II. Justificación de la realización de la investigación……2

III. Objeto de la investigación……6

IV. Planteamiento y delimitacion del problema……6

V. Marco teórico conceptual de referencia……8

VI. Hipótesis……31

VII. Pruebas empíricas o cualitativas de la hipótesis……31

VIII. Conclusiones y nueva agenda de investigación……51

IX. Bibliografía……55

## I. Introducción

La violencia de género es un fenómeno multidimensional que afecta profundamente la vida de las mujeres en todo el mundo. Este tipo de violencia se manifiesta en diversas formas, desde la violencia física y psicológica hasta la violencia económica y simbólica. Con la creciente digitalización de nuestras sociedades, la violencia de género también ha encontrado nuevas formas de manifestarse a través de las tecnologías, incluyendo la inteligencia artificial (IA). Este tema cobra una relevancia particular en el contexto actual de México, donde las tasas de violencia contra las mujeres siguen siendo alarmantemente altas y donde las estructuras sociales y legales se encuentran en constante evolución para enfrentar este problema.

El mundo digital y en particular la inteligencia artificial ha transformado numerosos aspectos de la vida cotidiana, desde la automatización de procesos hasta la creación de nuevas oportunidades en diversos campos. Si bien, existen beneficios, esta tecnología también plantea desafíos importantes, particularmente en lo que respecta a la violencia de género, pues para algunas mujeres el uso de la red puede representar un peligro, lo últimos datos registrados por el Instituto Nacional de Estadística y Geografía permite conocer la forma en que la violencia digital se ha incrementado conforme se desarrollan nuevas tecnologías afectando en mayor medida a la población femenina, sin importar la clase social, raza, identidad de género, ni residencia, ya que este tipo de violencia se reproduce en cualquier espacio del mundo.

La violencia de género perpetrada al utilizar la inteligencia artificial, puede manifestarse de múltiples maneras, entre la más comunes encontramos el acoso cibernético, la difusión de contenido íntimo sin consentimiento, deepfake, deepnude y la utilización de algoritmos que perpetúan estereotipos y discriminación. Estas conductas no solo violan los derechos fundamentales de las mujeres víctimas, sino que también reflejan vacíos en la legislación actual que no está suficientemente actualizada para enfrentar las complejidades

tecnológicas del presente. Para comprender esta realidad que evoluciona rápidamente, es imperativo realizar un análisis que permita conocer que es la inteligencia artificial e identificar cuáles son las manifestaciones de este fenómeno en la violencia de género, así mismo, cómo regula México este tipo de conductas y por consecuencia si cuenta con la normativa necesaria para atender dicho fenómeno, es por ello, que el presente análisis se realizará utilizando un método mixto, es decir, cuantitativo y cualitativo que nos arrojen mediante estadísticas proporcionadas por dependencias gubernamentales y asociaciones especializadas en el tema, datos sobre la forma e incidencia de la violencia de género en la que se emplea la inteligencia artificial, así como, casos conocidos, doctrina existente en el tema y experiencias a nivel internacional.

## II. Justificación

La violencia de género mediada por inteligencia artificial puede definirse como cualquier acto de violencia basado en el género que es facilitado o perpetuado a través del uso de tecnologías de inteligencia artificial (AI). Esto incluye, pero no se limita a, el acoso digital, la manipulación de datos personales, la creación y difusión de deepfakes con contenido sexual no consentido, y la discriminación algorítmica que refuerza estereotipos de género y marginaliza a las mujeres en diversas esferas, como el empleo y el acceso a servicios.

El origen de esta violencia radica en una combinación de factores. Primero, la falta de diversidad de género en los equipos de desarrollo de IA conduce a la creación de sistemas que replican y amplifican sesgos de género preexistentes. Además, la insuficiencia de marcos regulatorios y éticos sólidos permite que estas tecnologías sean utilizadas de maneras que vulneran los derechos de las mujeres sin consecuencias significativas para los perpetradores. Como señala Cathy O'Neil en su libro *Weapons of Math Destruction* (2016), los algoritmos, cuando no son diseñados y aplicados con un enfoque ético y crítico, pueden perpetuar injusticias a gran escala.

Las consecuencias de esta violencia son profundas y multifacéticas. En el plano personal, las mujeres que son víctimas de esta violencia sufren daños psicológicos, sociales y, en algunos casos, económicos irreparables. En un contexto más amplio, esta violencia perpetúa las desigualdades de género, socavando los esfuerzos hacia la equidad y limitando el potencial de las mujeres para participar plenamente en la sociedad. Además, la normalización de estas formas de violencia a través de la tecnología puede desensibilizar a la sociedad, dificultando la identificación y respuesta efectiva a estas agresiones.

La atención efectiva a la violencia de género mediada por inteligencia artificial es crucial por varias razones. Primero, es una cuestión fundamental de derechos humanos. Según la Declaración Universal de Derechos Humanos, toda persona tiene derecho a la seguridad, la privacidad y a no ser objeto de discriminación. Cuando la IA se utiliza para perpetuar la violencia de género, se infringen estos derechos, poniendo en riesgo la dignidad y la autonomía de las mujeres.

Desde una perspectiva social, la atención a este problema es esencial para avanzar hacia una sociedad más equitativa e inclusiva. La violencia de género, cuando se perpetúa a través de tecnologías avanzadas, refuerza las estructuras de poder que marginan a las mujeres, impidiéndoles acceder a oportunidades y participar plenamente en la vida pública. Abordar este problema de manera proactiva es indispensable para romper estos ciclos de exclusión y empoderar a las mujeres en todos los niveles de la sociedad.

Económicamente, la violencia de género mediada por inteligencia artificial tiene un costo significativo. Las mujeres afectadas por esta violencia pueden experimentar una disminución en su capacidad para trabajar y contribuir económicamente, lo que a su vez afecta la productividad y el crecimiento económico general. Además, los costos asociados con la atención a las víctimas, incluyendo servicios de salud mental y asistencia legal, representan una carga económica considerable para los sistemas de salud y justicia.

La apuesta por prevenir y atender la violencia de género mediada por inteligencia artificial trae consigo multiples beneficios, pues contribuye a la protección de los derechos humanos de las mujeres, garantizando que puedan vivir en un entorno seguro, tanto en el mundo físico como digital. Esto es esencial para el desarrollo de sociedades más justas y equitativas.

Asimismo, la prevención de esta violencia puede tener un impacto positivo en la economía. Al reducir las barreras que enfrentan las mujeres en el ámbito digital, se facilita su plena participación en el mercado laboral y en otras esferas de la vida pública, lo que puede conducir a un crecimiento económico más inclusivo. Según un estudio de McKinsey Global Institute (2015), avanzar hacia la igualdad de género podría añadir hasta 12 billones de dólares al PIB global para 2025.

Desde una perspectiva global, la atención efectiva a esta forma de violencia también puede posicionar a México y otros países como líderes en la promoción de los derechos digitales y la equidad de género, estableciendo un ejemplo para otras naciones en desarrollo.

Por otro lado, la falta de atención adecuada a la violencia de género mediada por inteligencia artificial puede tener consecuencias devastadoras, ya que, perpetúa la desigualdad de género, permitiendo que las estructuras de poder existentes se mantengan intactas y que las mujeres continúen siendo marginadas en múltiples esferas. Además, la impunidad de los actos de violencia digital puede desincentivar a las víctimas a buscar justicia, perpetuando un ciclo de violencia y victimización.

La falta de atención a este problema puede llevar a una pérdida significativa de talento y potencial humano, afectando negativamente la productividad y el crecimiento económico. Socialmente, puede contribuir a la desintegración del tejido social, creando un entorno de desconfianza y temor que afecta a toda la sociedad.

En atención a los desafíos que plantea la violencia de género perpetrada por inteligencia artificial, se han llevado a cabo diversas acciones tanto a nivel gubernamental como social. En México, por ejemplo, la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia ha sido un paso importante para proteger los derechos de las mujeres. Sin embargo, ¿esta legislación aún no aborda de manera específica la violencia facilitada por tecnologías de IA?, lo que implicaría la necesidad de actualizar el marco legal.

A nivel internacional, instrumentos como la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer (CEDAW) y la Convención de Belém do Pará establecen obligaciones claras para los Estados en la protección de los derechos de las mujeres, incluyendo en el ámbito digital. Sin embargo, es necesario que estos tratados se complementen con legislación específica que aborde los desafíos únicos que plantea la inteligencia artificial.

Dado el carácter emergente y complejo de la violencia de género mediada por inteligencia artificial, ¿Es imperativo desarrollar un marco legal que aborde este fenómeno?. Esta legislación debe incluir provisiones específicas para la protección de los derechos digitales de las mujeres, así como mecanismos de responsabilidad para los desarrolladores y usuarios de tecnologías de IA. Además, debe promover la diversidad y la inclusión en el desarrollo de estas tecnologías, asegurando que se diseñen de manera que no perpetúen ni amplifiquen los sesgos de género existentes.

En resumen, la violencia de género mediada por inteligencia artificial es un problema complejo y multifacético que requiere una atención urgente y coordinada desde múltiples frentes. La prevención y atención efectiva de este tipo de violencia no solo es una cuestión de justicia y derechos humanos, sino que también tiene implicaciones profundas para el desarrollo social y económico de las sociedades. En el contexto actual de México y del mundo, ¿es esencial avanzar en la implementación de políticas y leyes que aborden estas nuevas formas de violencia, asegurando que las mujeres puedan vivir y participar plenamente en una sociedad digital que respete su dignidad y derechos?.

## III. Objetivo de la investigación

El objetivo principal de esta investigación es: (i) identificar el fenómeno de la violencia de género perpetrada a través de la inteligencia artificial en México y otros países, (ii) las formas de perpetuarse y (iii) analizar si el marco jurídico federal vigente en nuestro país, protege de manera efectiva los derechos de las mujeres en el entorno digital asegurando que las tecnologías emergentes se utilicen de manera que promuevan la equidad de género y respeten los derechos humanos. (iv) Esta investigación también busca contribuir al desarrollo de un marco jurídico actualizado que proteja de manera efectiva los derechos de las mujeres en el entorno digital.

## IV. Planteamiento y delimitación del problema

A pesar de los avances en el reconocimiento de la violencia de género como un problema prioritario en México, los esfuerzos por abordar las formas emergentes de esta violencia, particularmente las facilitadas por la inteligencia artificial, son aún incipientes e insuficientes. Las políticas públicas y marcos regulatorios actuales no abordan de manera específica los riesgos que la IA representa para las mujeres, lo que deja una brecha significativa en la protección de sus derechos en el entorno digital.

Aunque se han realizado esfuerzos importantes, como la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y la implementación de las Alertas de Violencia de Género contra las Mujeres (AVGM), estas iniciativas no han sido adaptadas para enfrentar las nuevas formas de violencia facilitadas por tecnologías avanzadas. Además, los tratados internacionales a los que México está adherido, como la Convención de Belém do Pará y la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW), proporcionan un marco general para la protección de los derechos de las

mujeres, pero no abordan de manera específica los desafíos que plantea la inteligencia artificial.

La investigación se delimita a analizar la violencia de género facilitada por la inteligencia artificial en el contexto mexicano, con un enfoque en las manifestaciones más comunes de esta violencia, como la discriminación algorítmica, el acoso digital (ciberacoso), y la creación de deepfakes. Se considerarán tanto las implicaciones sociales, económicas y educativas como los desafíos específicos que enfrenta México en la creación de un marco legal y regulatorio adecuado para abordar este problema.

Si bien, se han realizado avances importantes en la lucha contra la violencia de género en México, como la implementación de políticas públicas y la creación de leyes enfocadas en proteger a las mujeres, incluyendo las recientes reformas conocidas como la Ley Olimpia estos esfuerzos son insuficientes para abordar la violencia mediada por inteligencia artificial. Las leyes actuales no contemplan las complejidades de la tecnología moderna ni los nuevos tipos de violencia que esta puede facilitar. Por lo tanto, es imperativo actualizar y expandir el marco jurídico y político para que incluya mecanismos de protección específicos contra la violencia de género facilitada por IA.

Además, es necesario fortalecer la colaboración entre el gobierno, la sociedad civil, el sector privado y la academia para desarrollar soluciones efectivas y sostenibles. Esto incluye la promoción de investigaciones que ofrezcan nuevas perspectivas y soluciones innovadoras, así como la creación de alianzas estratégicas para la implementación de políticas integrales que combatan esta forma emergente de violencia de género.

El planteamiento y delimitación del problema de la violencia de género facilitada por inteligencia artificial en México resalta la urgencia de abordar esta problemática desde múltiples perspectivas, incluyendo la social, económica, educativa y de igualdad de género. A pesar de los avances realizados, queda un largo camino por recorrer para garantizar que las mujeres estén protegidas en el entorno digital. La presente investigación busca

contribuir a cerrar esta brecha, proponiendo soluciones que no solo sean efectivas a corto plazo, sino que también aseguren un futuro donde la tecnología sea una herramienta para la igualdad, y no para la perpetuación de la violencia y la discriminación.

Por ello, con datos nacionales proporcionados por instancias oficiales se identificarán las formas de violencia de género perpetradas por IA que se están presentando en México. ¿En qué medida las leyes actuales en México son adecuadas para abordar la violencia de género perpetrada a través de la IA? y ¿Qué acciones legislativas a nivel federal han sido propuestas para enfrentar la violencia de género asistida por IA?

## V. Marco teórico conceptual de referencia

La inteligencia artificial como campo de estudio formal comenzó en la década de 1950, cuando Alan Turing, matemático británico, planteó la idea de que las máquinas podrían ser capaces de pensar de manera autónoma. Turing es conocido por proponer el "Test de Turing", un experimento diseñado para evaluar la capacidad de una máquina para exhibir un comportamiento indistinguible del de un ser humano. Durante las décadas de 1960 y 1970, la IA se centró en el desarrollo de sistemas expertos, programas de computadora diseñados para emular la toma de decisiones humanas en áreas específicas como la medicina y la ingeniería.

A lo largo de las décadas de 1980 y 1990, la IA experimentó un crecimiento más lento, pero se mantuvo en desarrollo, principalmente en laboratorios de investigación. Fue durante la década de 2010, con la explosión del aprendizaje automático (*machine learning*) y el acceso a grandes volúmenes de datos, que la IA resurgió con fuerza, encontrando aplicaciones en una amplia gama de sectores, desde la tecnología hasta las finanzas.

Ahora bien, la violencia de género es un fenómeno antiguo, profundamente enraizado en las estructuras patriarcales de la sociedad. A lo largo de la historia, las mujeres han sido objeto de violencia física, psicológica, económica y sexual. Con la llegada de la era digital,

estas formas de violencia comenzaron a trasladarse al ciberespacio, dando lugar a nuevas formas de abuso que, aunque menos visibles, son igualmente devastadoras.

Esta violencia de género ha evolucionado con la aparición de la inteligencia artificial, introduciendo nuevas formas de abuso que son menos visibles, pero igualmente dañinas. Inicialmente, la violencia digital se limitaba a formas de acoso en línea, como el *ciberacoso*, *cyberbullying* y la difusión no autorizada de imágenes íntimas. Sin embargo, con la incorporación de la inteligencia artificial, estas formas de violencia se han vuelto más sofisticadas y difíciles de detectar.

En la violencia de género facilitada por IA, encontramos que esta comenzó a manifestarse de manera más clara en la última década, a medida que las tecnologías algorítmicas se integraron cada vez más en la vida cotidiana. Uno de los primeros incidentes documentados de discriminación algorítmica ocurrió en el ámbito de la contratación, donde los sistemas automatizados, entrenados con datos históricos, penalizaban a las mujeres debido a sesgos de género en los datos utilizados para entrenar los algoritmos.

Otro ejemplo significativo es el surgimiento de los *deepfakes* a mediados de la década de 2010. Estos videos, creados con técnicas avanzadas de IA, a menudo eran utilizados para crear contenido sexual explícito no consentido de mujeres, lo que representa una forma nueva y extremadamente perturbadora de violencia sexual digital.

Los citados *deepfakes* son videos o imágenes falsificadas generadas por inteligencia artificial, que a menudo se utilizan para crear contenido sexual explícito no consensuado de mujeres. En muchos casos, estos videos son difundidos en plataformas en línea, donde se convierten en herramientas de acoso y humillación pública.

Bañuelos Capistrán define al deepfake como “documentos falsos o falsificados que se hacen pasar por auténticos, y que pueden tener un amplio alcance mediático. Se trata de un fenómeno emergente en el campo del audiovisual y por lo mismo plantea problemáticas,

también emergentes, que no habían sido tecnológicamente gestionadas, culturalmente asimiladas o legisladas".

Es decir, el deepfake puede definirse como una tecnología que captura ciertas características físicas, expresiones y movimientos de una persona, y así su rostro, cuerpo o voz puede recrearse o superponerse en otras imágenes o videos y sonidos, dando paso de manera más específica al deepface, deepvoice, fake nudes o deepnudes.

De igual forma existe el deepnude, tecnología similar a la utilizada en el deepfake, en la que en lugar de sobreponer rostros o expresiones faciales lo que hace es que, se recopilan en la red partes desnudas del cuerpo, típicamente femenino, y se sobreponen en fotografías o imágenes de otras mujeres para desnudarlas.

También encontramos que no solo la imagen se ve comprometida en estas falsificaciones, pues la voz también puede ser imitada por esta tecnología, dando paso al deepvoice, que no se encuentra tan desarrollado como el deepface, pero peligrosamente se prevé que en próximos años se desarrolle y más usuarios tengan acceso a la misma. Se ha dado a conocer que el deepvoice ha sido utilizado para generar fraudes millonarios a usuarios bancarios, solicitando a través de voces falseadas el retiro de grandes cantidades de dinero, haciéndose pasar por la víctima. Esta técnica, a diferencia de los mensajes falsos utilizados por medio escrito como phishing, que usualmente tienen faltas ortográficas o algún elemento extraño en su redacción que podrían dar indicios de su falsedad y detectarlos, reproduce de forma muy similar la voz de la persona suplantada a través de la inteligencia artificial, por lo que corroborar su autenticidad requiere de gran expertis.

Como ejemplo de esta evolución, Estados Unidos fue uno de los primeros países en enfrentar casos de discriminación algorítmica, especialmente en sectores como la tecnología y las finanzas, donde los algoritmos comenzaron a ser ampliamente utilizados

para decisiones automatizadas. Por ejemplo, en 2018[1], se descubrió que un sistema de contratación desarrollado por Amazon, presentaba un sesgo de género que penalizaba sistemáticamente a las mujeres que aplicaban a puestos de tecnología, debido a que el sistema había sido entrenado con datos de currículos predominantemente masculinos.

Los *deepfakes* también se originaron en Estados Unidos, con plataformas como Reddit siendo utilizadas para difundir videos manipulados de mujeres. Esta práctica pronto se extendió a otros países, convirtiéndose en un problema global.

En Europa han experimentado un aumento en los casos de violencia de género facilitada por IA. Un artículo The Unseen Biases: *How AI is Perpetuating Gender Inequality in Hiring Practices.*" Journal of Ethics in Technology *publicado* en el Journal of Ethics in Technology señala que en Alemania, se documentó un caso donde un algoritmo utilizado para la contratación en el sector tecnológico mostraba una clara preferencia por los candidatos masculinos. Esto se debió a que el sistema fue entrenado con datos de currículos anteriores en los que predominaban los hombres, lo que llevó al algoritmo a asociar ciertas características de éxito profesional con el género masculino. Como resultado, las candidaturas femeninas fueron sistemáticamente subvaloradas, perpetuando la desigualdad de género en el acceso a empleos bien remunerados y de alta demanda

En Reino Unido en la European Financial Review se publicó el *articulo* Algorithmic Discrimination and the Gender Divide in Digital Finance, en que se han documentado casos de discriminación algorítmica en sectores como la vivienda y los seguros. En este país un estudio similar reveló que un sistema de IA utilizado por una empresa financiera internacional tendía a descartar automáticamente a candidatas femeninas para roles en tecnología y finanzas, basándose en patrones históricos que reflejaban un sesgo de género.

[1] Dastin, J. (2018). "Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women." Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

Estos casos subrayan cómo la IA, cuando no se diseña y supervisa adecuadamente, puede replicar y amplificar las desigualdades de género existentes.

La revista Review of Central and East European Law (RCEEL) publicó un caso muy conocido ocurrió en Polonia donde una periodista fue víctima de un deepfake que mostraba un video sexual explícito en el que se había manipulado su imagen. A pesar de que el video era falso, su difusión en redes sociales tuvo un impacto devastador en su reputación y bienestar psicológico. Este tipo de violencia de género digital es particularmente dañino porque es difícil de controlar y combatir, y las mujeres afectadas a menudo carecen de recursos legales eficaces para defenderse.

La revista Journal of Cybersecurity Studie dio a conocer que en Rumanía, se reportaron varios incidentes en los que mujeres jóvenes fueron víctimas de *deepfakes* creados y difundidos por compañeros de clase o exparejas. Estos videos se utilizan para extorsionar o acosar a las mujeres, amenazándolas con hacer públicos los videos falsos si no cumplen con ciertas demandas. Este fenómeno ha generado una gran preocupación en la región, ya que las leyes no siempre están equipadas para abordar eficazmente este tipo de violencia digital.

En Asia, particularmente en India, por ejemplo, las mujeres han sido víctimas de acoso digital facilitado por IA, así como de discriminación algorítmica que ha sido identificada como una forma significativa de violencia de género facilitada por IA, especialmente en el sector financiero. Las mujeres en India a menudo enfrentan dificultades para acceder a crédito y servicios financieros debido a algoritmos utilizados por bancos y empresas de tecnología financiera (*fintech*), que tienden a favorecer a los hombres.

Un estudio realizado en 2019, reveló que los algoritmos utilizados por varias plataformas de préstamos en línea en India penalizaban a las mujeres debido a factores como su historial laboral, que en muchos casos reflejaba brechas debido a responsabilidades de cuidado no remuneradas, y su menor acceso histórico al crédito. Como resultado, las mujeres recibían

calificaciones crediticias más bajas y se les ofrecían peores condiciones de préstamo en comparación con sus contrapartes masculinas. Este tipo de discriminación algorítmica perpetúa las desigualdades de género en el acceso a recursos financieros esenciales, limitando las oportunidades económicas de las mujeres.

En Asia, los *deepfakes* también han sido una herramienta predominante para perpetrar violencia de género, especialmente en países como Corea del Sur y Japón. En Corea del Sur, el uso de *deepfakes* se ha convertido en un problema tan extendido que el término "molka" (que originalmente se refería a cámaras ocultas utilizadas para grabar mujeres sin su consentimiento) ha comenzado a abarcar también estos videos manipulados.

Un caso muy conocido en Corea del Sur involucró a una actriz que fue víctima de un *deepfake* que mostraba su rostro en un video pornográfico. A pesar de que el video era falso, su difusión en línea tuvo consecuencias terribles para su carrera y bienestar personal. La falta de una respuesta legal adecuada para abordar estos casos en Corea del Sur llevó a una fuerte movilización social que exigió una regulación más estricta contra el uso de *deepfakes* y otros tipos de violencia sexual digital.

En Japón, la Japanese Journal of Law and Society señala que los deepfakes también han sido utilizados para acosar y humillar a mujeres, con casos en los que se manipularon imágenes de celebridades y personas públicas para crear contenido pornográfico falso. Este tipo de violencia digital ha resaltado la necesidad urgente de regulaciones específicas que aborden el uso de IA en la creación de contenido no consensuado y la protección de las víctimas de este tipo de abusos.

Aunque Estados Unidos ha liderado el desarrollo de tecnologías de IA, la regulación específica para abordar la violencia de género facilitada por estas tecnologías aún es limitada. No obstante, se han realizado esfuerzos significativos para abordar la discriminación algorítmica, como la propuesta de la Ley de Responsabilidad Algorítmica

(Algorithmic Accountability Act) de 2019, que exige que las empresas evalúen los impactos éticos y sociales de sus sistemas de IA.

La Unión Europea ha adoptado un enfoque más proactivo en la regulación de la inteligencia artificial. La propuesta del Reglamento de Inteligencia Artificial (AI Act) de 2021 establece un marco para la supervisión y regulación de los sistemas de IA, con un enfoque en mitigar los riesgos de discriminación y proteger los derechos fundamentales. Además, el Reglamento General de Protección de Datos (GDPR) proporciona una sólida protección contra el uso indebido de datos personales, lo que es crucial para prevenir la violencia de género en el entorno digital.

El Reino Unido ha avanzado en la regulación de la IA y la protección contra la discriminación algorítmica. En 2018, se estableció un Comité de IA para examinar las implicaciones éticas y sociales de estas tecnologías, lo que resultó en la creación de pautas para asegurar la equidad algorítmica. La Ley de Igualdad de 2010 también proporciona una base legal para combatir la discriminación en el uso de tecnologías avanzadas.

Canadá ha sido líder en la incorporación de principios éticos en el desarrollo y uso de la IA. El Consejo Asesor de Inteligencia Artificial de Canadá ha promovido la creación de marcos de responsabilidad para el desarrollo de IA, y el país ha sido pionero en la inclusión de la perspectiva de género en la ética de la tecnología.

Por lo que hace al marco legal nuestro país, es parte de varios instrumentos internacionales que, aunque no tratan específicamente la violencia de género mediante IA, establecen principios que son relevantes para su regulación.

En este sentido, se destaca que México es parte de la Convención de Belém do Pará[2], esta convención interamericana en su artículo primero establece la obligación de los Estados de

[2]**Tratados Multilaterales.** ***Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la mujer "Convención De Belem Do Para"*** **Recuperado de** https://www.oas.org/juridico/spanish/tratados/a-61.html

prevenir, sancionar y erradicar la violencia contra las mujeres, un principio que se puede aplicar a la violencia digital. Define la violencia contra la mujer, como “cualquier acción o conducta, basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado”.

Señalando además que para prevenir, sancionar y erradicar la violencia contra las mujeres los Estados Partes de la citada Convención, entre ellos México, convinieron adoptar, políticas orientadas a tal fin, así como llevar a cabo entre otras, las siguientes medidas:

- Incluir en su legislación interna normas penales, civiles y administrativas, así como las de otra naturaleza que sean necesarias para prevenir, sancionar y erradicar la violencia contra la mujer y adoptar las medidas administrativas apropiadas que sean del caso.
- Establecer procedimientos legales justos y eficaces para la mujer que haya sido sometida a violencia, que incluyan, entre otros, medidas de protección, un juicio oportuno y el acceso efectivo a tales procedimientos.

De igual forma la Convención sobre todas las formas de Discriminación contra la Mujer (CEDAW) obliga a los Estados a eliminar la discriminación contra las mujeres en todas sus formas, lo que incluye la discriminación facilitada por la tecnología, señalando en su artículo 2 que se entenderá que la violencia contra la mujer abarca los siguientes actos, aunque sin limitarse a ellos:

a) La violencia física, sexual y sicológica que se produzca en la familia, incluidos los malos tratos, el abuso sexual de las niñas en el hogar, la violencia relacionada con la dote, la violación por el marido, la mutilación genital femenina y otras prácticas tradicionales nocivas para la mujer, los actos de violencia perpetrados por otros miembros de la familia y la violencia relacionada con la explotación.
b) La violencia física, sexual y sicológica perpetrada dentro de la comunidad en general, inclusive la violación, el abuso sexual, el acoso y la intimidación sexuales en el trabajo, en instituciones educacionales y en otros lugares, la trata de mujeres

y la prostitución forzada.

Por su parte, uno de los Objetivos de Desarrollo Sostenible de la Agenda 2030 de la Organización de las Naciones Unidas es el Objetivo 5 Lograr la igualdad entre los géneros y empoderar a todas las mujeres y niñas, el cual en el apartado 5.b establece como una de las metas, mejorar el uso de las de la tecnología instrumental, en particular la tecnología de la información y las comunicaciones, para promover el empoderamiento de las mujeres.

Asimismo, los Principios Rectores sobre Empresas y Derechos Humanos de la ONU (2011), aunque no es un tratado vinculante, estos principios establecen que las empresas, incluidas las de tecnología, tienen la responsabilidad de respetar los derechos humanos, lo que incluye evitar la perpetuación de la violencia de género mediante IA.

Pese a la existencia de estos preceptos, surgió la discusión sobre su ámbito de tutela, es decir, si aplicaba para el mundo real (offline) o el mundo digital (online) parecieran claros y suficientes para obviar la discusión sobre si estos instrumentos protegen o tutelan la violencia contra las mujeres, pues la violencia digital es resultado de la evolución en los medios comisivos pero los fines y daños tienen el mismo impacto o incluso mayor.

A esta deliberación, le siguió otra, consistente en la construcción del concepto o definición de la violencia digital. Pronunciándose en 2018 la Organización de las Naciones Unidas (ONU), la Relatora Especial sobre la Violencia contra las Mujeres, al señalar que la violencia en línea contra las mujeres es “todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada además de estar en constante cambio”[3].

[3] Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias (REVM-ONU) (14 de Junio de 2018). A/HRC/38/47. *Informe acerca de la violencia en línea contra las mujeres*

En este ámbito encontramos el Convenio de Budapest que es el principal marco internacional para combatir los delitos cibernéticos, que incluye aspectos de la violencia digital, sin embargo, México aún no es parte del mismo, pese a que se han presentado diversos exhortos por parte del Poder Legislativo para su suscripción.

En cuanto a la legislación nacional, el ámbito federal la suma de esfuerzos por diversos actores impulsaron diversas reformas denominadas Ley Olimpia y lograron que las mismas fueran aprobadas por el Congreso de la Unión y el primero de junio de 2021 se publicara en el Diario Oficial de la Federación la reforma que incluía la violencia digital y mediática en Ley General de Acceso de las Mujeres a una Vida Libre de Violencia[4] definiéndolas, de la siguiente forma:

*Artículo 20 Quáter.-* ***Violencia digital*** *es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.*

*Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación.*

*Para efectos del presente Capítulo se entenderá por Tecnologías de la Información y la Comunicación aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos.*

*La violencia digital será sancionada en la forma y términos que establezca el Código Penal Federal*.

*Artículo 20 Quinquies.-* ***Violencia mediática*** *es todo acto a través de cualquier medio de comunicación, que de manera directa o indirecta promueva estereotipos sexistas, haga apología de la violencia contra las mujeres y las niñas, produzca o permita la producción y difusión de discurso de odio sexista, discriminación de género o desigualdad entre mujeres y hombres, que cause daño a las mujeres y niñas de tipo psicológico, sexual, físico, económico, patrimonial o feminicida.*

---

*y las niñas desde la perspectiva de los derechos humanos*. Recuperado de https:// www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

[4] Cámara de Diputados. (2022). *Ley General de Acceso de las Mujeres a una Vida Libre de Violencia*. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf

*La violencia mediática se ejerce por cualquier persona física o moral que utilice un medio de comunicación para producir y difundir contenidos que atentan contra la autoestima, salud, integridad, libertad y seguridad de las mujeres y niñas, que impide su desarrollo y que atenta contra la igualdad.*

Además de reconocer e incorporar estas modalidades de violencia, establece obligaciones para las autoridades del ámbito de la procuración e impartición de justicia tendientes a proteger a la víctima, como se plasman a continuación.

*Artículo 20 Sexies.- Tratándose de violencia digital o mediática para garantizar la integridad de la víctima, la o el Ministerio Público, la jueza o el juez, ordenarán de manera inmediata, las medidas de protección necesarias, ordenando vía electrónica o mediante escrito a las empresas de plataformas digitales, de medios de comunicación, redes sociales o páginas electrónicas, personas físicas o morales, la interrupción, bloqueo, destrucción, o eliminación de imágenes, audios o videos relacionados con la investigación previa satisfacción de los requisitos de Ley.*

*En este caso se deberá identificar plenamente al proveedor de servicios en línea a cargo de la administración del sistema informático, sitio o plataforma de Internet en donde se encuentre alojado el contenido y la localización precisa del contenido en Internet, señalando el Localizador Uniforme de Recursos.*

*La autoridad que ordene las medidas de protección contempladas en este artículo deberá solicitar el resguardo y conservación lícita e idónea del contenido que se denunció de acuerdo a las características del mismo.*

*Las plataformas digitales, medios de comunicación, redes sociales o páginas electrónicas darán aviso de forma inmediata al usuario que compartió el contenido, donde se establezca de forma clara y precisa que el contenido será inhabilitado por cumplimiento de una orden judicial.*

*Dentro de los cinco días siguientes a la imposición de las medidas de protección previstas en este artículo deberá celebrarse la audiencia en la que la o el juez de control podrá cancelarlas, ratificarlas o modificarlas considerando la información disponible, así como la irreparabilidad del daño.*

Esta reforma a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia se realizó de forma conjunta con una adición al Código Penal Federal[5] a efecto de establecer tipos penales y sancionar el delito de violación a la intimidad sexual, de la siguiente forma:

[5] Cámara de Diputados. (2022). *Código Penal Federal*. México. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

*Artículo 199 Octies.- Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.*

*Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.*

*Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización.*

*Artículo 199 Nonies.- Se impondrán las mismas sanciones previstas en el artículo anterior cuando las imágenes, videos o audios de contenido íntimo sexual que se divulguen, compartan, distribuyan o publiquen no correspondan con la persona que es señalada o identificada en los mismos.*

*Artículo 199 Decies.- El mínimo y el máximo de la pena se aumentará hasta en una mitad:*

*I.- Cuando el delito sea cometido por el cónyuge, concubinario o concubina, o por cualquier persona con la que la víctima tenga o haya tenido una relación sentimental, afectiva o de confianza;*

*II.- Cuando el delito sea cometido por un servidor público en ejercicio de sus funciones;*

*III.- Cuando se cometa contra una persona que no pueda comprender el significado del hecho o no tenga la capacidad para resistirlo;*

*IV.- Cuando se obtenga algún tipo de beneficio no lucrativo;*

*V.- Cuando se haga con fines lucrativos, o*

*VI.- Cuando a consecuencia de los efectos o impactos del delito, la víctima atente contra su integridad o contra su propia vida.*

No es de obviarse que esta reforma conocida en nuestro país como Ley Olimpia, se debe al activismo que ha llevado por años Olimpia Coral Melo, después de ser víctima de violencia digital por parte de su ex pareja quien difundió un video sexual en redes sociales sin su consentimiento, sin que dicho hecho pudiera ser sancionado debido a que nuestro marco legal no preveía el tipo penal y por ende la sanción.

La citada reforma, tiene por objeto que nuestro país cuente con un marco legal federal que permita a las autoridades proteger a las víctimas, investigar, y sancionar conductas de esta

naturaleza evitando así la impunidad y erradicando estas prácticas que causan graves daños a las mujeres y si bien, representa un avance para sancionar la violencia de género digital, es importante señalar que la misma, si bien constituye una forma de sanción de la violencia digital, dicha normativa solo se limita a sancionar el contenido digital de carácter sexual no autorizado en sus diversas modalidades dejando de lado aquellas imágenes, audios y videograbaciones manipuladas por la inteligencia artificial alterando el contenido para fines indebidos, por ende no cubre todas las formas de violencia de género facilitadas por IA, como la discriminación algorítmica o el acoso automatizado, entre otros.

Otro aspecto importante a regular es, el derecho a la Protección de Datos Personales, este derecho parte del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en el cual se establece que no solo toda persona tiene derecho a proteger su información personal, sino también a acceder a ella, a rectificar, a cancelarla e incluso a oponerse a determinados tratamientos. Este derecho tiene un doble ámbito de aplicación, al vincular tanto a las autoridades en el sector público, como a los particulares en el sector privado. La tutela efectiva de este derecho en México hasta el momento está garantizada por el un organismo autónomo garante nacional y de 32 organismos garantes locales.

El numeral 16 de la Constitución Política de los Estados Unidos Mexicanos en su segundo párrafo establece:

*"…Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros…"*

En cuanto al reconocimiento y evolución de este derecho[6], es relevante señalar que la Ley Federal de Transparencia y Acceso a la Información Gubernamental, promulgada en 2002,

[6] InfoCdMex. (2024, 19 junio). #ENVIVO 📽 FORO: «ConcienCIA Digital» Inteligencia artificial y privacidad. [Vídeo]. YouTube. https://www.youtube.com/watch?v=J4f3qeQ7ZQ0

inicialmente contempló la protección de datos personales como un componente del derecho de acceso a la información, restringiendo la difusión de información pública y permitiendo únicamente que los individuos pudieran acceder y corregir sus datos personales en manos de las autoridades.

Años más tarde, con la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en 2010, se designó al entonces Instituto Federal de Acceso a la Información y Protección de Datos como la instancia responsable de salvaguardar este derecho.

Posteriormente, con la reforma constitucional de 2014, todos los Institutos de Transparencia se convirtieron en órganos constitucionales autónomos, asumiendo la responsabilidad de garantizar el derecho a la protección de datos personales.

Esta reforma también amplió el catálogo de sujetos obligados en materia de transparencia, facilitando la identificación de aquellos responsables del cumplimiento de la protección de datos personales, y se sentaron las bases para la creación del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, un mecanismo de coordinación interinstitucional que define las políticas públicas en estos ámbitos.

Con la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en 2016, se establecieron un conjunto de obligaciones específicas para todas las autoridades con el fin de cumplir con los principios y deberes en la materia y garantizar los derechos de acceso, rectificación, cancelación y oposición, comúnmente conocidos por su acrónimo ARCO.

De esta forma, el derecho a la protección de datos personales es reconocido como un derecho autónomo, distinto del derecho de acceso a la información pública. Según la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la

autodeterminación informativa se puede ejercer ante diversas autoridades de los ámbitos nacional, estatal y municipal:

• Poderes Ejecutivo, Legislativo y Judicial;

• Órganos autónomos;

• Partidos políticos;

• Fideicomisos y fondos públicos;

• Sindicatos; y,

• Personas físicas y morales que reciban y ejerzan recursos públicos o realicen actos de autoridad.

Este reconocimiento de sujetos obligados establece que tales autoridades deben de realizar acciones para promover, proteger, respetar y garantizar al interior de la institución, los derechos de acceso, rectificación, cancelación, oposición y la protección de toda información personal.

En este sentido, es fundamental que las y los usuarios conozcan qué es un dato personal, definido como la información concerniente a una persona física identificada o identificable. Entre esta, se distingue la información personal sensible, que se relaciona con aquellos datos personales que deben de ser protegidos con mayor intensidad para evitar situaciones y consecuencias que no favorezcan a las personas titulares y que de divulgarse, pueden afectarles severamente.

Los datos personales que se comparten con más frecuencia dentro del contexto planteado son el domicilio, el número de teléfono, la dirección de correo electrónico, alguna huella digital o los rasgos del rostro. Ciertamente, el frecuente uso de las Tecnologías de la Información y Comunicación ha implicado que se normalice el compartir información personal sin conocer los parámetros de regulación de los sitios en los que se navega en

Internet. Ello, porque el acceso a servicios que brindan las plataformas digitales, está condicionado a la entrega "voluntaria" de información personal. La posibilidad de que toda persona pueda tener control para conocer, recuperar o restituir su información personal, en relación al uso de tecnologías, en primer lugar, depende de que haya una identificación del tipo de información que se entrega y, en segundo término, que se conozca la política de privacidad de cada plataforma que se utiliza, precisamente porque las circunstancias en las que vivimos el trámite o transacción más sencilla recopila información personal que convierte a nuestra información en una huella digital de quiénes somos, qué hacemos, cómo nos movemos, qué consumimos, etc.

Finalmente es de resaltarse que esta normativa protege los datos personales y la privacidad, aspectos cruciales en el contexto de la IA, especialmente en lo que respecta a la manipulación de datos para perpetuar la violencia de género. No obstante, su aplicación específica en casos de violencia de género mediada por IA, no es específica.

Por lo que hace al Programa Nacional para la Igualdad entre Mujeres y Hombres[7] (PROIGUALDAD) 2020-2024 incluye la violencia digital en sus objetivos, pero aún no se han realizado reformas específicas que aborden la violencia de género mediante IA. Esto demuestra una necesidad urgente de actualizar el marco jurídico para proteger a las mujeres en el entorno digital.

Como hemos visto la inteligencia artificial tiene una función social significativa, ya que puede influir en decisiones cotidianas y en las estructuras sociales de manera profunda. Sin embargo, cuando se utiliza sin una perspectiva de género, la IA puede perpetuar desigualdades y reforzar los estereotipos de género existentes. La capacidad de la IA para automatizar decisiones y procesar grandes volúmenes de datos significa que los sesgos

[7] INMUJERES. Programa Nacional para la Igualdad entre Mujeres y Hombres 2020 2024. gob.mx. https://www.gob.mx/inmujeres/acciones-y-programas/programa-nacional-para-la-igualdad-entre-mujeres-y-hombres

incorporados en estos sistemas pueden amplificar desigualdades a una escala sin precedentes.

El peligro radica en la invisibilidad de estas formas de violencia. Dado que los algoritmos y los sistemas de IA suelen ser opacos, es difícil para las víctimas y para la sociedad en general reconocer cuándo están siendo objeto de discriminación o abuso. Esto puede llevar a una normalización de la violencia de género mediada por IA, dificultando aún más su identificación y erradicación.

Derivado del constante avance tecnológico y diversidad de técnicas que emplea la IA para a comisión de violencia de género es necesario la expedición de la normativa que para evitar los vacíos legales dando una respuesta legal integral que responda a las problemáticas que plantea el rápido desarrollo de la inteligencia artificial.

En este sentido, en el Congreso de la Unión se han planteado diversas iniciativas con la intención de regular las tecnologías entre ellas, la creación de la Comisión de Derechos Digitales del Senado de la República, conformada el 9 de noviembre de 2023, cuyo objetivo es, abordar con responsabilidad todos los aspectos relacionados con la regulación, uso, aprovechamiento e implementación de las herramientas y plataformas tecnológicas, con un enfoque centrado en la inclusión digital.

Es así, como encontramos que, de las 16 iniciativas presentadas en esta Comisión, destaca la Iniciativa que pretende regular la violencia digital sexual presentada por la diputada Ruth Alejandra López Hernández de Movimiento Ciudadano, y presidenta de la Comisión de Derechos Digitales, que propone reformas significativas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal. Esta propuesta de reforma busca abordar los desafíos emergentes relacionados con la violencia digital y el uso de inteligencia artificial (IA), con el objetivo de fortalecer la protección de las mujeres contra la violencia de género en el ámbito digital.

La propuesta se centra en varios aspectos clave:

Tipificación de la Violencia Digital: La iniciativa propone ampliar la definición de violencia de género en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia para incluir la violencia digital. Esto abarca cualquier forma de agresión, acoso, difusión no consentida de imágenes o información personal, y uso de IA para generar contenidos que atenten contra la dignidad y privacidad de las mujeres.

Reformas al Código Penal Federal: La iniciativa incluye modificaciones al Código Penal Federal para tipificar de manera específica delitos relacionados con el uso de IA para perpetuar violencia de género. Esto incluye la creación, distribución o utilización de deepfakes, contenido falso generado por IA, con el propósito de dañar la reputación, chantajear o acosar a una persona.

Medidas Preventivas y Punitivas: Se propone la implementación de medidas tanto preventivas como punitivas. Por un lado, la iniciativa sugiere la creación de campañas de sensibilización y programas educativos sobre los riesgos y consecuencias de la violencia digital. Por otro lado, establece sanciones más severas para aquellos que utilicen tecnologías digitales, incluyendo IA, para cometer actos de violencia de género.

Protección de Datos Personales y Privacidad: La iniciativa también hace hincapié en la protección de los datos personales y la privacidad de las mujeres, proponiendo mayores controles y regulaciones sobre el uso de tecnologías que puedan facilitar la violencia de género digital.

A pesar de las buenas intenciones detrás de la propuesta, la iniciativa ha sido objeto de varias críticas por parte de expertos en derecho digital, inteligencia artificial y derechos humanos, siendo las principales:

Falta de Claridad en la Definición de Violencia Digital: Algunos expertos han señalado que la iniciativa carece de claridad en cuanto a la definición y alcance de lo que constituye

violencia digital. La definición propuesta es considerada demasiado amplia y podría llevar a la criminalización de conductas que no necesariamente implican violencia de género, generando incertidumbre jurídica.

Posibles Impactos en la Libertad de Expresión: Una crítica recurrente es que las reformas propuestas podrían tener implicaciones negativas para la libertad de expresión. La tipificación de delitos relacionados con el uso de IA, como la creación de deepfakes, podría llevar a una regulación excesiva que afecte la creación y distribución de contenidos legítimos, incluyendo aquellos con fines artísticos o satíricos.

Desafíos en la Aplicación Práctica: Los críticos también han señalado que la implementación de estas reformas podría enfrentar desafíos significativos, especialmente en términos de la capacidad de las autoridades para identificar y perseguir delitos cometidos en el entorno digital. La tecnología evoluciona rápidamente, y existe la preocupación de que las reformas propuestas puedan quedar desactualizadas o ser difíciles de aplicar de manera efectiva.

Riesgo de Criminalización de Conductas No Intencionales: Otra crítica importante es que la iniciativa podría llevar a la criminalización de conductas que, si bien pueden ser perjudiciales, no fueron realizadas con la intención de causar daño. Esto podría afectar a usuarios de tecnologías digitales que desconocen el potencial impacto de sus acciones o que no tenían intención de cometer un delito.

Necesidad de un Enfoque Multidisciplinario: Algunos expertos han argumentado que la iniciativa debería ser parte de un enfoque más amplio y multidisciplinario que incluya no solo reformas legales, sino también esfuerzos educativos, tecnológicos y de políticas públicas para abordar de manera integral la violencia digital de género.

En conclusión, la iniciativa presentada por la diputada Ruth Alejandra López Hernández es un esfuerzo valioso para adaptar el marco legal mexicano a los desafíos que plantea la violencia de género en el entorno digital, especialmente en relación con el uso de

tecnologías de inteligencia artificial. Sin embargo, como lo destacan las críticas, es fundamental que cualquier reforma legal esté respaldada por definiciones claras, un análisis profundo de las implicaciones para los derechos humanos, y un enfoque equilibrado que proteja tanto la integridad y privacidad de las mujeres como la libertad de expresión.

Otra iniciativa que ha tomado relevancia es la presentada por el senador Ricardo Monreal en marzo de 2023 para regular la inteligencia artificial (IA) la cual pretende abordar las complejidades y desafíos que emergen con el rápido avance de esta tecnología. Esta propuesta legislativa tiene como objetivo establecer un marco normativo que asegure el desarrollo, implementación y uso ético de la inteligencia artificial en el país. A continuación, se presenta un análisis del alcance de la iniciativa, así como las principales críticas que ha recibido por parte de expertos en la materia.

La propuesta busca crear un marco regulatorio para la inteligencia artificial que aborde varios aspectos clave:

Transparencia y Rendición de Cuentas: La iniciativa propone la creación de mecanismos para asegurar que los desarrolladores y usuarios de IA sean transparentes en cuanto a los algoritmos y procesos utilizados. Además, se busca establecer responsabilidades claras para quienes implementen sistemas de IA, especialmente en casos de fallos o decisiones controversiales.

Protección de Derechos Humanos: Un enfoque central de la propuesta es asegurar que el uso de IA respete los derechos humanos, evitando discriminación, sesgo y violaciones a la privacidad. Esto incluye la protección de datos personales y la no discriminación en el uso de algoritmos.

Fomento a la Innovación: La iniciativa también busca promover la innovación tecnológica, al mismo tiempo que establece controles que prevengan posibles abusos o mal uso de la inteligencia artificial.

Supervisión y Regulación: La creación de un organismo especializado en la supervisión y regulación de la inteligencia artificial en México es una de las propuestas más destacadas. Este organismo estaría encargado de emitir directrices, monitorear el cumplimiento de las normativas, y sancionar prácticas que contravengan el marco legal propuesto.

Ahora bien, las principales críticas a la iniciativa, han sido:

Falta de Especificidad Técnica: Muchos expertos han señalado que la propuesta carece de una comprensión técnica detallada sobre cómo funciona la inteligencia artificial y sus aplicaciones. La falta de especificidad técnica puede llevar a regulaciones que sean difíciles de implementar o que no aborden adecuadamente los problemas complejos asociados con la IA.

Posibles Obstáculos a la Innovación: Aunque la iniciativa busca promover la innovación, algunos críticos argumentan que la implementación de regulaciones estrictas podría sofocar el desarrollo de la inteligencia artificial en México. La burocratización del proceso de innovación podría desalentar a startups y empresas tecnológicas, que podrían optar por trasladar sus actividades a países con regulaciones más flexibles.

Desafíos en la Implementación y Supervisión: Otro punto de crítica es la viabilidad de crear un organismo especializado con la capacidad técnica y recursos suficientes para supervisar y regular de manera efectiva la inteligencia artificial. Algunos expertos señalan que esto podría ser una tarea difícil de llevar a cabo, especialmente considerando los recursos limitados y la falta de expertos en IA dentro del gobierno mexicano.

Preocupaciones sobre la Eficiencia y la Efectividad: Varios analistas han expresado dudas sobre si el marco propuesto realmente podrá mitigar los riesgos asociados con la inteligencia artificial, como los sesgos algorítmicos o la automatización que conduce a la pérdida de empleos. La efectividad de la regulación dependerá en gran medida de la capacidad del nuevo organismo para adaptarse rápidamente a los cambios tecnológicos y de mercado.

Regulación Prematura: Algunos expertos argumentan que la regulación podría ser prematura y podría ser más prudente esperar a que se desarrollen marcos regulatorios internacionales más robustos antes de implementar regulaciones a nivel nacional. Esto evitaría que México se quede atrás en términos de competitividad tecnológica a nivel global.

En suma, la iniciativa del senador Ricardo Monreal para regular la inteligencia artificial en México es un esfuerzo necesario para abordar los desafíos y riesgos que presenta esta tecnología emergente. Sin embargo, como lo indican las críticas de expertos, es crucial que cualquier marco regulatorio sea cuidadosamente diseñado para evitar obstáculos innecesarios a la innovación y garantizar que se pueda implementar de manera efectiva. Es esencial que la regulación de la IA en México no solo proteja los derechos humanos y fomente la transparencia, sino que también permita un entorno dinámico donde la tecnología pueda desarrollarse y prosperar.

Para que esta iniciativa tenga éxito, será fundamental un diálogo continuo entre legisladores, expertos técnicos, y actores de la industria, asegurando que las regulaciones estén alineadas con las mejores prácticas internacionales y adaptadas a las necesidades específicas de México.

A todo ello se suman lo señalado por la organización Luchadoras[8] resultado de la creación y trabajo de esta comisión, en donde realizan las siguientes reflexiones:

Tomando en cuenta lo anterior, resulta necesario mirar de forma crítica a esta Comisión y las iniciativas y reformas que emergen de ella. Por eso vale la pena tomar en cuenta que:

- Las comisiones necesitan asesorarse sobre los temas que pretender abordar en sus agendas, la vinculación o consultorías con organizaciones de la sociedad civil o institutos expertos en digitalidad y derechos humanos.

- Estas comisiones necesitan partir del reconocimiento del estado actual de los derechos digitales en México.

- No debe incitar a la censura, el temor, el prohibicionismo o ambigüedades en sus iniciativas y evitar provocar incertidumbres en torno a la digitalidad en las personas usuarias.

- No debe crear mecanismos de espionaje disfrazados de ciberseguridad.

Si bien las iniciativas en violencia de género, pretenden proteger a las mujeres del mal uso de las tecnologías (como la IA) resulta necesario recordar que “más leyes no significa más justicia” y tampoco más prevención. En este sentido, algunos puntos sobre las reformas que no deberíamos perder de vista son:

- El abordaje legislativo más allá de priorizar el punitivismo debe poner al centro de sus iniciativas los derechos humanos de grupos vulnerables basándose en el consentimiento, privacidad, equidad, agencia y promover un entorno digital más seguro.

- Nombrar la respectiva responsabilidad que las empresas desarrolladoras de tecnología (incluyendo a las plataformas de redes sociales) tienen en la construcción de espacios

[8] Avendaño, Elizabeth. Luchadoras.mx La Comisión de Derechos Digitales del Senado y sus iniciativas de regulación de tecnologías e inteligencia artificial. https://luchadoras.mx/quienes-somos/

digitales seguros y exigir su cooperación con las autoridades para identificar daños, agresores y medidas de respuesta.

- En lugar de promover la creación de nuevos delitos, se necesita priorizar, capacitar y sensibilizar a autoridades para una mejor interpretación legal, donde se contemplen las repercusiones *offline* (en los espacios físicos) de los comportamientos *online* (en los espacios digitales).

- Es necesario que la legislación y los procedimientos de acceso a la justicia sean claros para las víctimas y contemplen una perspectiva de reparación del daño.

- Realizar acuerdos expeditos y disponibles en español, considerando que la mayor parte de documentación sobre tecnología se genera en inglés, entre autoridades y plataformas para garantizar el acceso a la justicia penal o cualquier otra.

- El lenguaje que se utiliza debe ser crítico sin promover estigmas o alarmar a las personas usuarias. Por ejemplo, nombrar como “medios de falsificación” a las herramientas tecnológicas como la IA puede llegar a ser tendencioso y sugestivo.

  De ser necesario un abordaje punitivo, éste debe plantearse de forma responsable y nombrar consigo la garantía de un adecuado acceso a la justicia, políticas públicas y mecanismos de prevención.

  Es necesario pensar y construir iniciativas desde la prevención, no desde la censura, la sobrerregulación punitiva y posturas prohibicionistas alimentadas de miedo. Lo digital es real, por ello, debemos estar muy alertas sobre las propuestas que busquen regular el espacio digital.

## VI. Hipótesis

Las hipótesis en las que se basa esta investigación son las siguientes: i. El marco jurídico actual cuenta con los mecanismos suficientes y adecuados para prevenir y atender la

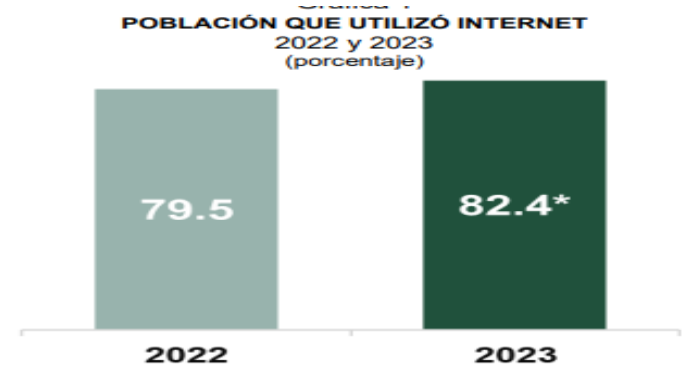
violencia de género perpetuada mediante inteligencia artificial; ii. Puede afirmarse que el proceso y evolución de las tecnologías ha traído como consecuencia la existencia de diversas formas de violencia de género contra mujeres con igual gravedad; iii. Es relevante, pertinente y necesario la voluntad política para implementar acciones a partir de la experiencia adquirida en otros países a fin de regular el empleo de esta tecnología y evitar la incidencia en este tipo de violencia.

## VII. Pruebas empíricas o cualitativas de la hipótesis

En la actualidad, no existe una base de datos oficial y específica que cuantifique de manera precisa la violencia de género facilitada por inteligencia artificial (IA) en México. Sin embargo, se pueden encontrar estadísticas y datos relevantes sobre violencia digital y violencia de género en general, que pueden incluir casos donde la IA ha sido un factor.

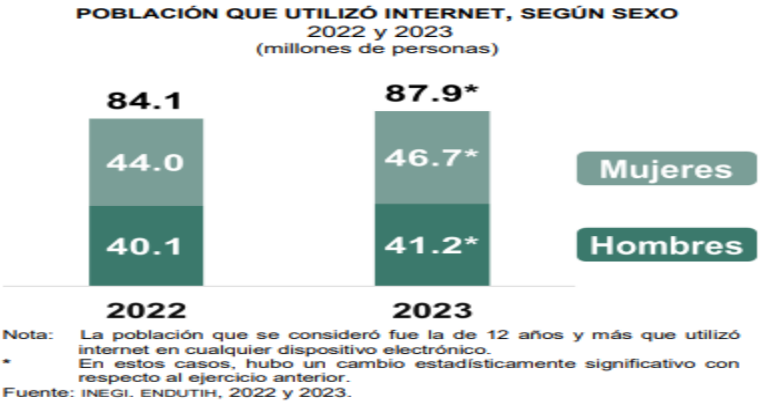
En este sentido encontramos la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH) 2023[9] la cual nos proporciona información referente al uso de internet por parte de la población hasta especificar los casos de violencia digital. En esta lógica a fin de identificar la población que utiliza la red y que puede ser víctima de este fenómeno, plasmamos los datos generales contenido en la citada encuesta y es así como encontramos que la población de 12 años y más que utilizó internet fue de 106.7 millones de personas.

[9] INEGI. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023. https://www.inegi.org.mx/programas/endutih/2023/




Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. ENDUTIH, 2022 y 2023.

De ese total, entre marzo y agosto de 2023, 87.9 millones de personas (82.4 %) utilizaron internet en cualquier dispositivo: 46.7 millones fueron mujeres y 41.2 millones, hombres. La población usuaria de internet utilizó este servicio en promedio 4.7 horas al día.

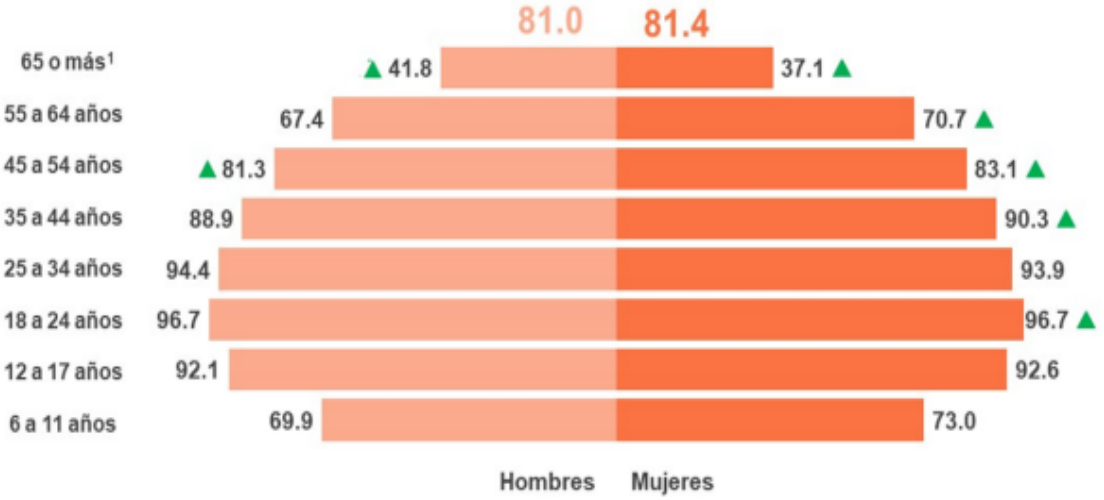



Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. ENDUTIH, 2022 y 2023.

En 2023, el grupo de 18 a 24 años presentó el mayor porcentaje de personas usuarias de internet, con 96.7 por ciento. Entre 2022 y 2023, el grupo con mayor incremento fue el de 55 a 64 años, que aumentó 6.9 puntos porcentuales su uso de internet. El grupo de 12 a 17 años presentó la misma participación (92.4 %) en este periodo.

En 2023, por primera vez, el porcentaje de mujeres usuarias de internet fue superior al de los hombres. La diferencia fue de 0.4 puntos porcentuales: 81.4 % correspondió a mujeres y 81.0 %, a hombres.

**PERSONAS USUARIAS DE INTERNET, SEGÚN GRUPOS DE EDAD Y SEXO**
2023
(porcentaje)

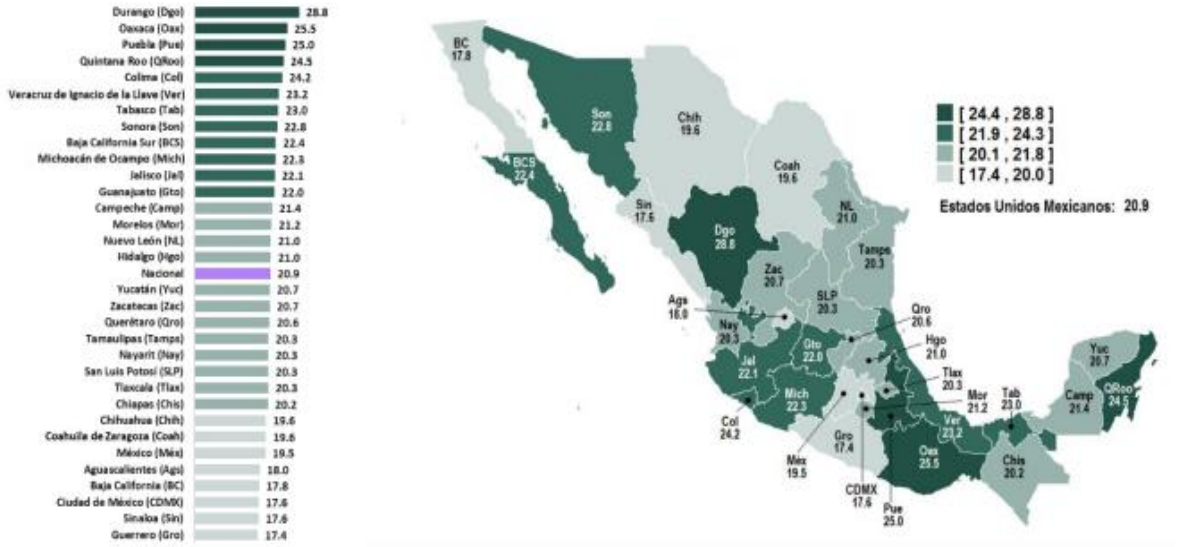



Nota: Los porcentajes se calcularon respecto al total de la población de referencia.
1 Incluye a las personas que no especificaron su edad.
▲ Incremento estadísticamente significativo respecto al año anterior.
Fuente: INEGI. ENDUTIH, 2023.

Ahora bien, en cuanto al ciberacoso,[10] el módulo sobre ciberacoso 2023 realizado por INEGI, proporciona información sobre este fenómeno, y es así como encontramos que a nivel nacional, 20.9 % de la población usuaria de internet vivió alguna situación de acoso cibernético. El porcentaje representa 18.4 millones de personas de 12 años y más. La mayor prevalencia de ciberacoso se registró en Durango, con 28.8 por ciento. Siguieron Oaxaca y Puebla, con 25.5 y 25.0 %, respectivamente. Las entidades con menor prevalencia fueron Guerrero, con 17.4 % y Sinaloa y Ciudad de México, ambas con 17.6 %

[10] INEGI, Módulo sobre Ciberacoso 2023. (2024, 6 agosto). https://www.inegi.org.mx/rnm/index.php/catalog/999

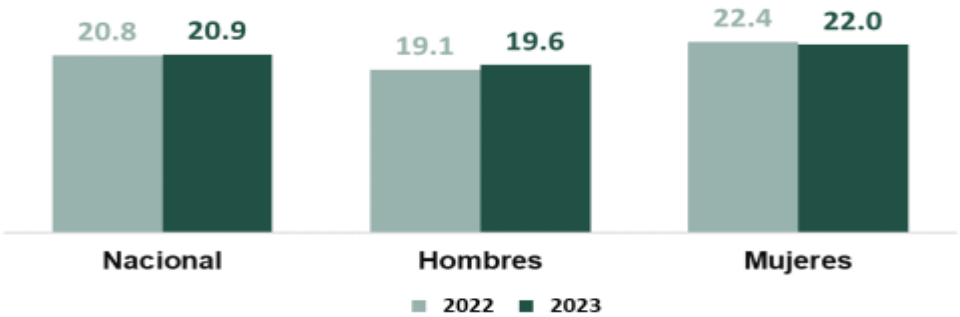
**POBLACIÓN QUE VIVIÓ CIBERACOSO, SEGÚN ENTIDAD FEDERATIVA**
2022 a 2023[1]
(porcentaje)




[1] La información se refiere al periodo de julio de 2022 a agosto de 2023.
Fuente: INEGI. MOCIBA, 2023.

A nivel nacional, 20.9 % de la población usuaria de internet vivió alguna situación de acoso cibernético, porcentaje que representa 18.4 millones de personas de 12 años y más. Para la población de mujeres usuarias, se estima que 22.0 % fue víctima de ciberacoso y para el caso de la población de hombres usuarios, fue de 19.6 %.

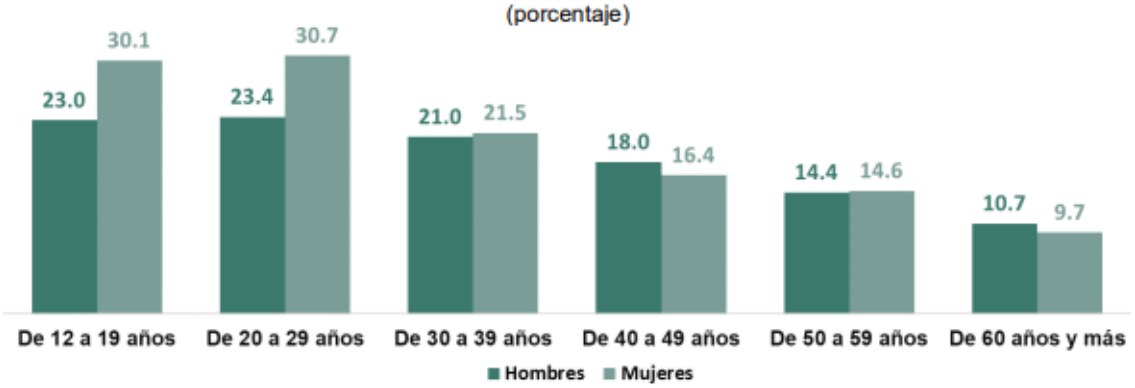
**POBLACIÓN USUARIA DE INTERNET QUE EXPERIMENTÓ ALGUNA SITUACIÓN DE CIBERACOSO[1]**
2022 y 2023
(porcentaje)




Notas: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
Fuente: INEGI. MOCIBA, 2022 y 2023.

En 2023, 30.7 % de las mujeres de 20 a 29 años y 23.4 % de los hombres de 20 a 29 años que utilizaron internet fueron víctimas de ciberacoso, en los últimos 12 meses.

**POBLACIÓN VÍCTIMA DE CIBERACOSO,[1] SEGÚN RANGO DE EDAD**
2022 a 2023
(porcentaje)




Notas: La población que se consideró fue la que utilizó internet en cualquier dispositivo electrónico.
[1] La información se refiere al periodo de julio de 2022 a agosto de 2023.
Fuente: INEGI. MOCIBA, 2023.

**MUJERES VÍCTIMAS DE CIBERACOSO,[1] SEGÚN RANGO DE EDAD**
2022 y 2023
(porcentaje)




Notas: Se consideró a mujeres de 12 años y más que utilizaron internet en cualquier dispositivo electrónico.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. MOCIBA, 2022 y 2023.

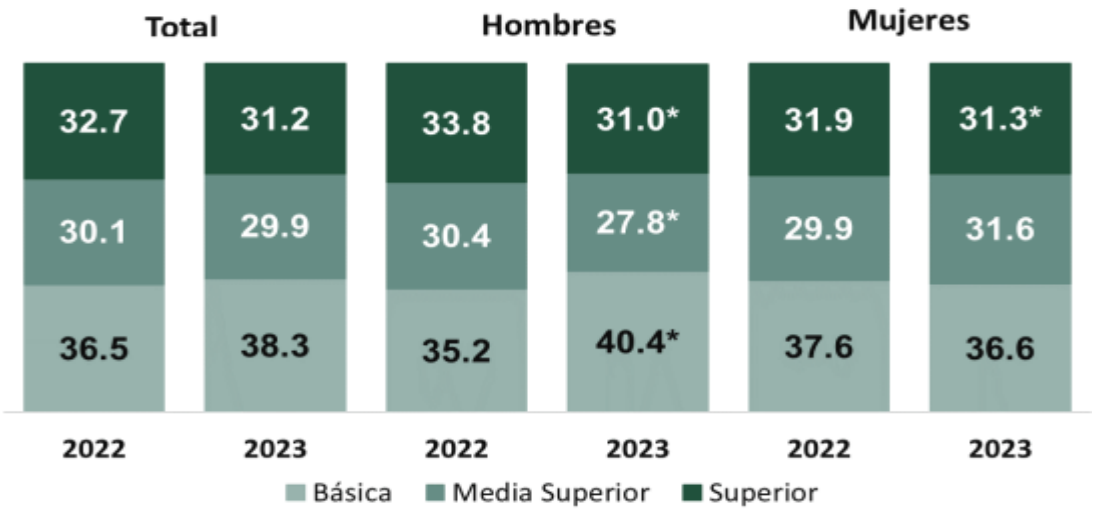
**HOMBRES VÍCTIMAS DE CIBERACOSO,[1] SEGÚN RANGO DE EDAD**
(porcentaje)
2022 y 2023




Notas: Se consideró a hombres de 12 años y más que utilizaron internet en cualquier dispositivo electrónico.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. MOCIBA, 2022 y 2023.

En 2023, de la población usuaria que fue víctima de ciberacoso, 38.3 % contó con estudios de nivel básico. Para la población de hombres, este porcentaje fue de 40.4 % y, para la población de mujeres, de 36.6 %.

**POBLACIÓN QUE EXPERIMENTÓ ALGUNA SITUACIÓN DE CIBERACOSO,[1] SEGÚN NIVEL DE ESCOLARIDAD**
2022 y 2023
(porcentaje)




Nota: Los porcentajes de mujeres y hombres se calcularon con relación al total nacional, según nivel educativo. Se excluyó información de la población *sin escolaridad* y *no especificado*. La población que se consideró fue la de 12 años y más que utilizó internet en algún dispositivo electrónico.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. MOCIBA, 2022 y 2023.

La prevalencia más alta de ciberacoso hacia las mujeres se detectó en Durango, con 33.0 por ciento. Siguieron Puebla, con 26.6 % y Colima, con 25.7 por ciento. Por otra parte, las entidades con menor prevalencia de ciberacoso hacia las mujeres fueron Guerrero, Ciudad de México y Coahuila, con 18.1, 18.4 y 18.9 %, respectivamente. En el caso de los hombres, la prevalencia más alta se presentó en Oaxaca, con 28.2 por ciento. Siguieron Quintana Roo, con 26.1 % y Tabasco, con 24.1 por ciento. En contraste, las entidades con menor prevalencia de ciberacoso a hombres fueron Aguascalientes, Sinaloa y Baja California, con 14.7, 15.7 y 16.2 %, respectivamente.

**PERSONAS USUARIAS DE INTERNET QUE EXPERIMENTARON ALGUNA SITUACIÓN DE CIBERACOSO EN LOS ÚLTIMOS 12 MESES, SEGÚN ENTIDAD FEDERATIVA[1]**
2022 y 2023
(porcentaje)

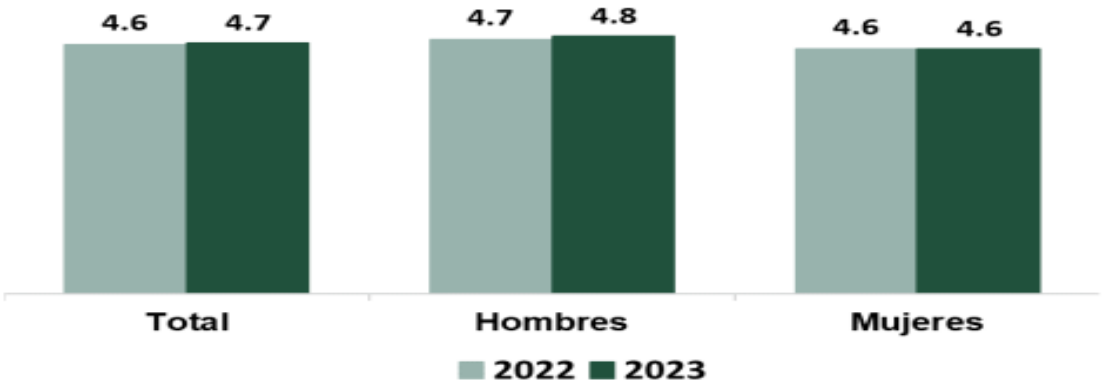
**Entidades federativas** ▼ A la baja **9** ▲ Al alza **3** ▬ Sin cambio **20**

| Entidad | 2022 | 2023 | Cambio (Δ %) | Entidad | 2022 | 2023 | Cambio (Δ %) |
|---|---|---|---|---|---|---|---|
| NACIONAL | 20.8 | 20.9 | - 0.5 | | | | |
| Aguascalientes | 21.3 | 18.0 | ▼ -15.5 | Morelos | 17.2 | 21.2 | ▲ 23.3 |
| Baja California | 21.8 | 17.8 | ▼ -18.3 | Nayarit | 23.7 | 20.3 | ▼ -14.3 |
| Baja California Sur | 24.9 | 22.4 | - -10.0 | Nuevo León | 20.9 | 21.0 | - 0.5 |
| Campeche | 24.8 | 21.4 | ▼ -13.7 | Oaxaca | 27.0 | 25.5 | - -5.6 |
| Coahuila de Zaragoza | 22.9 | 19.6 | ▼ -14.4 | Puebla | 22.0 | 25.0 | - 13.6 |
| Colima | 21.4 | 24.2 | - 13.1 | Querétaro | 19.3 | 20.6 | - 6.7 |
| Chiapas | 20.1 | 20.2 | - 0.5 | Quintana Roo | 18.7 | 24.5 | ▲ 31.0 |
| Chihuahua | 22.4 | 19.6 | - -12.5 | San Luis Potosí | 20.0 | 20.3 | - 1.5 |
| Ciudad de México | 16.9 | 17.6 | - 4.1 | Sinaloa | 17.4 | 17.6 | - 1.1 |
| Durango | 27.9 | 28.8 | - 3.2 | Sonora | 23.0 | 22.8 | - -0.9 |
| Guanajuato | 19.4 | 22.0 | - 13.4 | Tabasco | 27.9 | 23.0 | ▼ -17.6 |
| Guerrero | 26.2 | 17.4 | ▼ -33.6 | Tamaulipas | 21.5 | 20.3 | - -5.6 |
| Hidalgo | 23.5 | 21.0 | - -10.6 | Tlaxcala | 30.4 | 20.3 | ▼ -33.2 |
| Jalisco | 16.9 | 22.1 | ▲ 30.8 | Veracruz de Ignacio de la Llave | 23.4 | 23.2 | - -0.9 |
| México | 17.3 | 19.5 | - 12.7 | Yucatán | 27.9 | 20.7 | ▼ -25.8 |
| Michoacán de Ocampo | 24.2 | 22.3 | - -7.9 | Zacatecas | 21.5 | 20.7 | - -3.7 |

▼▲ De acuerdo con las pruebas de hipótesis correspondientes, en estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
Fuente: INEGI. MOCIBA, 2022 y 2023.

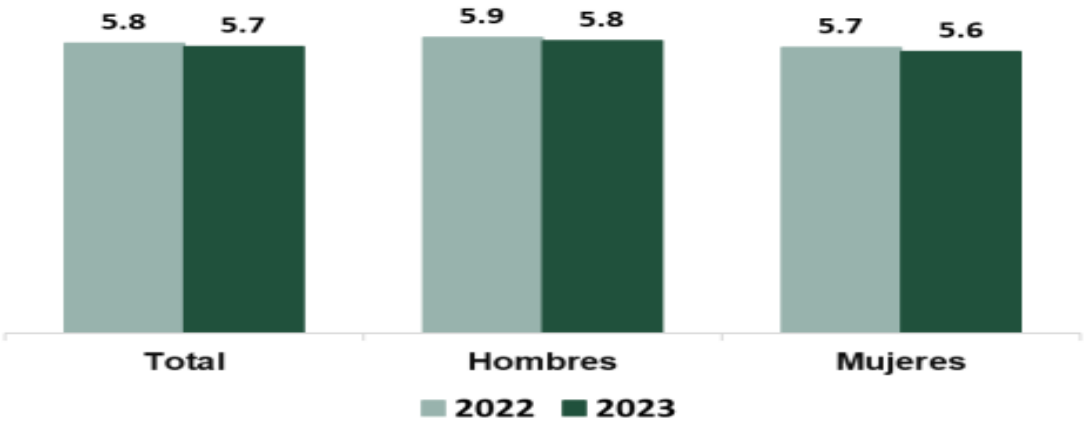
En promedio, la población que experimentó ciberacoso utilizó internet 5.7 horas al día, lo que significa que quienes vivieron esta experiencia pasaron mínimo una hora más en internet que quienes no la vivieron. En el caso específico, de las mujeres que sufrieron ciberacoso, el promedio de tiempo de conexión fue de 5.6 horas, mientras que para los hombres que vivieron ciberacoso, fue de 5.8 horas.

**PROMEDIO DE HORAS DE USO DIARIO DE INTERNET DE LA POBLACIÓN USUARIA**
2022 y 2023
(horas)




Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico en los últimos 3 meses con respecto al periodo de captación de los datos. Para 2022 y 2023, la información fue de junio a agosto.
Fuente: INEGI. MOCIBA, 2022 y 2023.

Gráfica 10
**PROMEDIO DE HORAS DE USO DIARIO DE INTERNET DE LA POBLACIÓN QUE VIVIÓ CIBERACOSO**
2022 y 2023
(horas)




Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico en los últimos 3 meses con respecto al periodo de captación de información. Para 2022 y 2023, los datos fueron de junio a agosto.
Fuente: INEGI. MOCIBA, 2022 y 2023.

El mayor tiempo de uso de internet en la población que vivió ciberacoso se registró en Coahuila, con 7.3 horas. Siguieron Nuevo León y Ciudad de México, con 6.8 y 6.6 horas, respectivamente. Las entidades con menor tiempo de uso de internet fueron Tlaxcala, con 4.3 horas; Guerrero, con 4.5 y Oaxaca, con 4.7.

**PROMEDIO DE HORAS DE USO DIARIO DE INTERNET DE LA POBLACIÓN QUE VIVIÓ CIBERACOSO, SEGÚN ENTIDAD FEDERATIVA**
2023
(horas)




Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico en los últimos 3 meses con respecto al periodo de captación de información (junio-agosto de 2023).
Fuente: INEGI. MOCIBA, 2023.

Durante los últimos 12 meses, 35.8 % de las mujeres y 35.9 % de los hombres víctimas de ciberacoso experimentaron contacto mediante identidades falsas. Asimismo, 31.0 % de las mujeres víctimas de ciberacoso recibió contenido sexual y 30.8 %, insinuaciones o propuestas sexuales. Para los hombres, estos porcentajes fueron 19.6 y 14.7 %, respectivamente.

**SITUACIONES DE CIBERACOSO EXPERIMENTADAS SEGÚN SEXO**
2022 a 2023[1]
(distribución porcentual)




Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico.
[1] La información se refiere al periodo de julio de 2022 a agosto de 2023.
Fuente: INEGI. MOCIBA, 2023.

**SITUACIONES DE CIBERACOSO EXPERIMENTADAS POR MUJERES**
2022 y 2023[1]
(distribución porcentual)




Nota: La población que se consideró corresponde a mujeres de 12 años y más que utilizaron internet en cualquier dispositivo electrónico.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022.
Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. MOCIBA, 2022 y 2023.

**SITUACIONES DE CIBERACOSO EXPERIMENTADAS POR HOMBRES**
2022 y 2023[1]
(distribución porcentual)




Nota: La población que se consideró corresponde a hombres de 12 años y más que utilizaron internet en cualquier dispositivo electrónico.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. MOCIBA, 2022 y 2023.

En cuanto a las situaciones experimentadas, según frecuencia y distinción por sexo, en 2023, la situación de ciberacoso que las mujeres experimentaron con mayor frecuencia fue rastreo de cuentas o sitios web, con 40.3 por ciento. Para los hombres, lo más común fue publicar o vender imágenes o videos de contenido sexual, con 37.4 %

**POBLACIÓN DE MUJERES QUE VIVIERON SITUACIONES DE CIBERACOSO, SEGÚN FRECUENCIA**
2022 a 2023[1]
(porcentaje)




Nota: La población que se consideró fue la de 12 años y más de edad que utilizó internet en cualquier dispositivo electrónico.
[1] La información se refiere al periodo de julio de 2022 a agosto de 2023.
Fuente: INEGI. MOCIBA, 2023.

**POBLACIÓN DE HOMBRES QUE VIVIERON SITUACIONES DE CIBERACOSO, SEGÚN FRECUENCIA**
2022 a 2023[1]
(porcentaje)

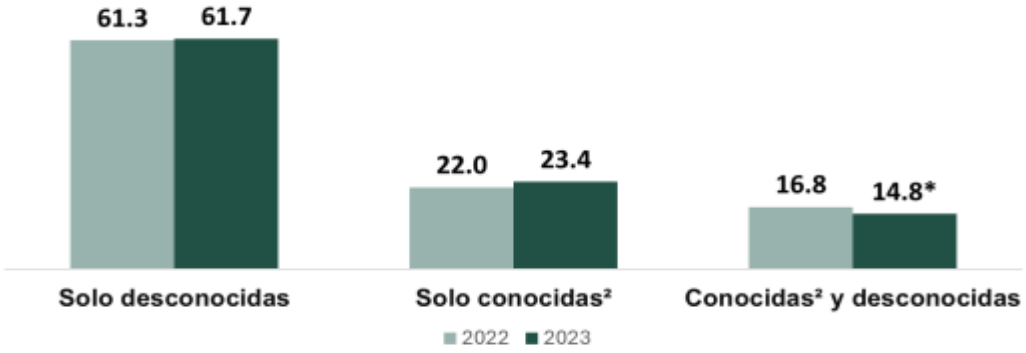



Nota: La población que se consideró fue la de 12 años y más de edad que utilizó internet en cualquier dispositivo electrónico.
[1] La información se refiere al periodo de julio de 2022 a agosto de 2023.
Fuente: INEGI. MOCIBA, 2023.

En cuanto a la identidad de la persona ciberacosadora, durante 2023, 61.7 % de la población de 12 años y más víctima de ciberacoso desconocía a la persona acosadora; 23.4 % identificó solo a personas conocidas y 14.8 % sufrió ciberacoso tanto de personas conocidas como desconocidas.

Gráfica 16

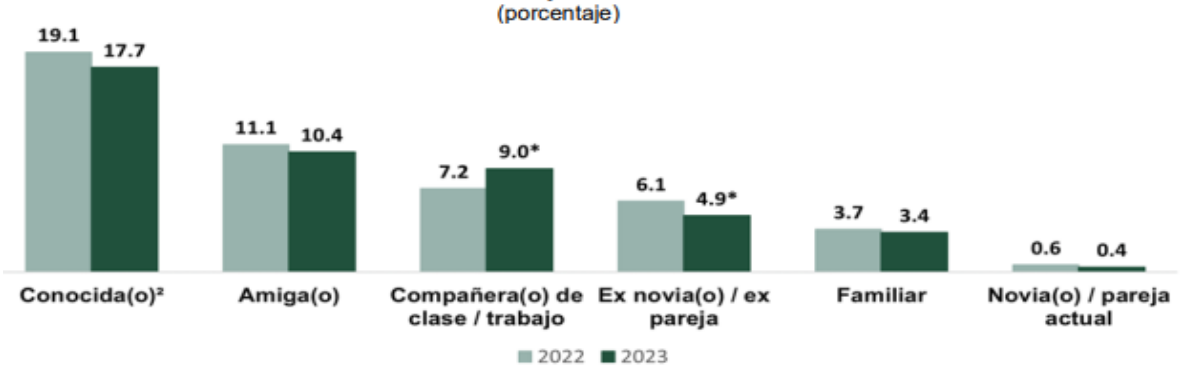
**POBLACIÓN QUE VIVIÓ CIBERACOSO, SEGÚN SU RELACIÓN CON LA PERSONA AGRESORA**
2022 y 2023[1]
(porcentaje)




Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico.
[1] Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
[2] Incluyó las opciones de respuesta *novia(o) / pareja actual*, *exnovia(o) / expareja*, *familiar*, *amiga(o)*, *compañera(o) de clase / trabajo*, *conocida(o) de poco trato* y *conocida(o) solo de vista*.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. MOCIBA, 2022 y 2023.

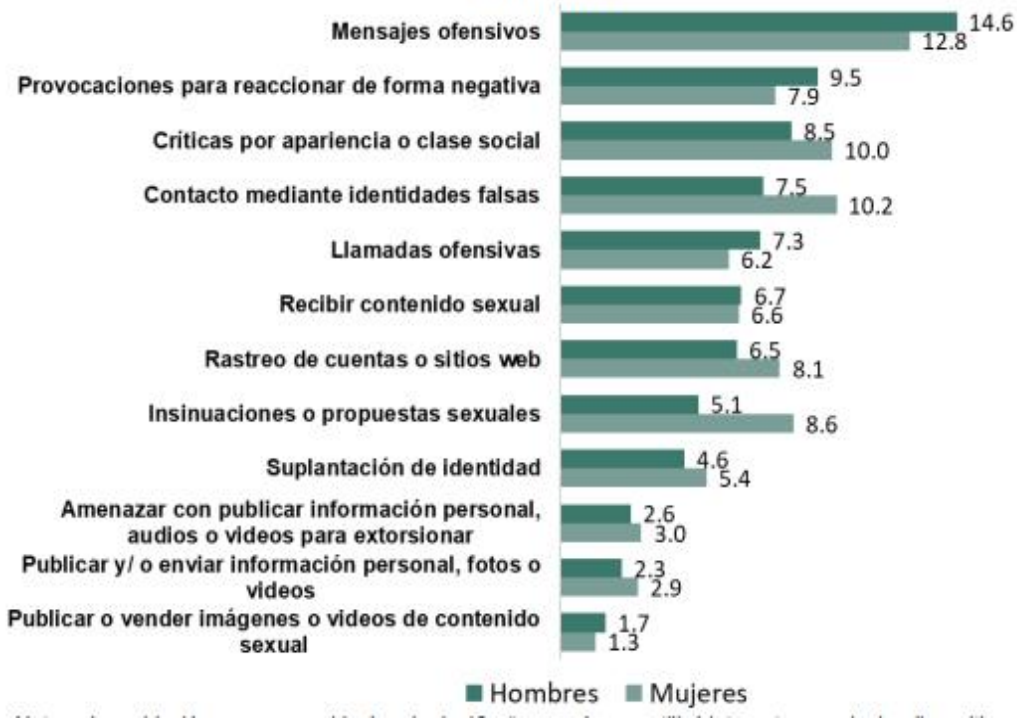
De la población que sufrió ciberacoso por parte de una persona conocida, 17.7 % no tenía una relación directa con la o el acosador.

**POBLACIÓN QUE VIVIÓ CIBERACOSO POR PARTE DE UNA PERSONA CONOCIDA, SEGÚN IDENTIDAD DE LA PERSONA ACOSADORA**
2022 y 2023[1]
(porcentaje)




Entre julio de 2022 y agosto de 2023, de las mujeres víctimas de ciberacoso por parte de personas conocidas, 12.8 % recibió mensajes ofensivos. Para los hombres víctimas de ciberacoso por parte de personas conocidas, este porcentaje fue de 14.6 %.

**POBLACIÓN QUE VIVIÓ SITUACIONES DE CIBERACOSO POR PARTE DE PERSONAS CONOCIDAS, SEGÚN TIPO DE SITUACIÓN Y SEXO DE LA VÍCTIMA**
2022 a 2023[1]
(porcentaje)



De la población de hombres de 12 años y más que fueron víctimas de ciberacoso y que pudieron identificar el sexo de las personas agresoras, 60.4 % indicó que la agresión la realizaron solo hombres. Por su parte, de la población de mujeres que fueron víctimas de ciberacoso y que pudieron identificar el sexo de las personas agresoras, 53.0 % manifestó que la agresión provino únicamente de hombres.

**POBLACIÓN QUE VIVIÓ CIBERACOSO, SEGÚN SEXO DE LA VÍCTIMA Y SEXO DE QUIEN EFECTUÓ EL CIBERACOSO**
2022 y 2023
(porcentaje)

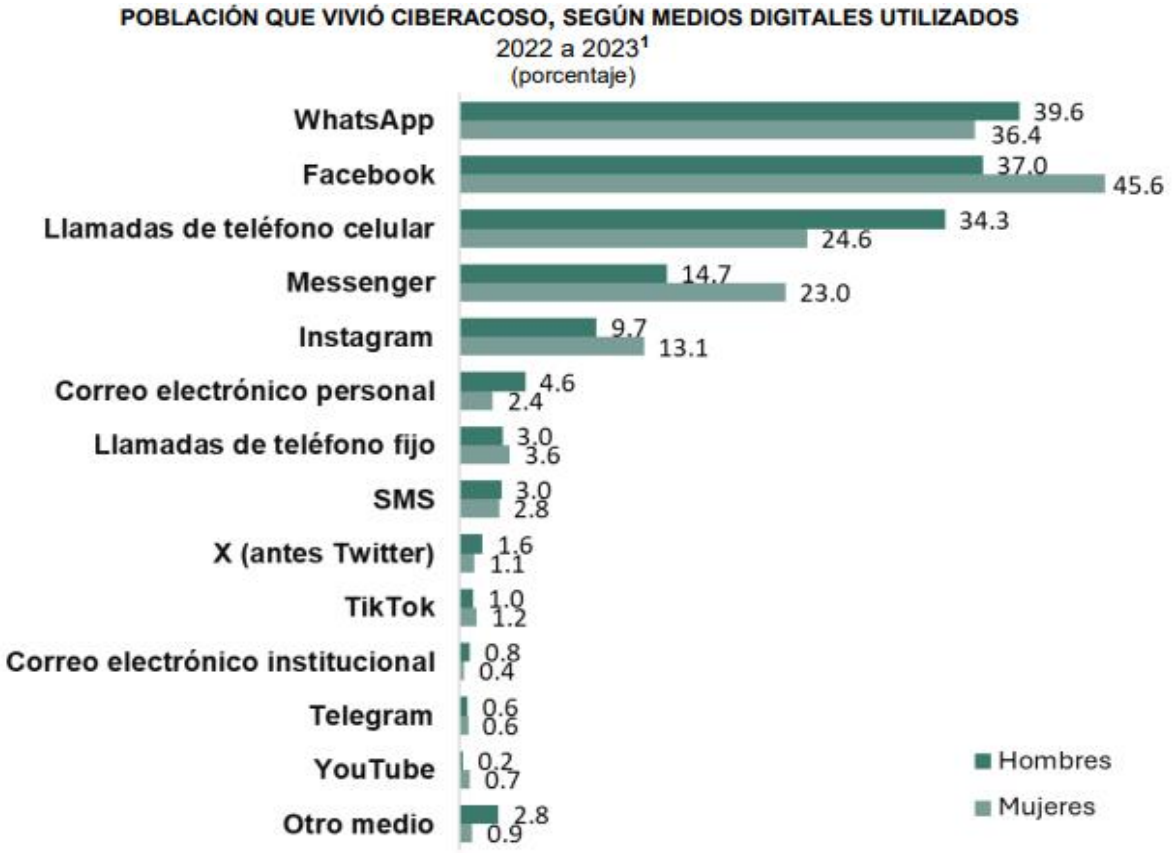
| Sexo de la víctima | Sexo de la persona acosadora | | | | | |
|---|---|---|---|---|---|---|
| | Hombres | | Mujeres | | Hombres y mujeres | |
| | 2022 | 2023 | 2022 | 2023 | 2022 | 2023 |
| **Hombres** | 58.1 | 60.4 | 15.6 | 13.3* | 26.2 | 26.3 |
| **Mujeres** | 56.1 | 53.0* | 17.6 | 20.5* | 26.3 | 26.5 |

Nota: La población que se consideró fue la de 12 años y más que utilizó internet en cualquier dispositivo electrónico. Para el caso de 2022, la información se refiere al periodo de julio de 2021 a agosto de 2022. Para 2023, los datos fueron de julio de 2022 a agosto de 2023.
* En estos casos, hubo un cambio estadísticamente significativo con respecto al ejercicio anterior.
Fuente: INEGI. MOCIBA, 2022 y 2023.

En 2023, de la población de mujeres de 12 años y más que experimentaron alguna situación de ciberacoso, 45.6 % sufrió el acoso mediante Facebook. De la población de hombres de 12 años y más que experimentaron alguna situación de ciberacoso, 39.6 % lo sufrió mediante WhatsApp.

El medio más frecuente que se utilizó para realizar ciberacoso en la modalidad de llamadas ofensivas fue llamadas de teléfono celular, con 59.5 por ciento. Para esta misma modalidad, el segundo medio más frecuente que se utilizó fue WhatsApp, con 30.3 %.

Respecto a los efectos del ciberacoso, la población de 12 años y más que fue víctima de ciberacoso, 60.9 % manifestó haber experimentado enojo ante esta situación. Siguieron desconfianza e inseguridad, con 37.6 y 30.1 %, respectivamente. Asimismo, 54.5 % de los hombres y 66.0 % de las mujeres que fueron víctimas de ciberacoso dijeron haber experimentado enojo.



Lo anterior, constituyen los datos más recientes en cuanto al ciberacoso que se vive en nuestro país, la forma de comisión, las posibles victimas e incluso los sujetos activos que lo cometen.

Aunado a lo anterior, Jumio[11] organización conocida como el proveedor líder de soluciones automatizadas de verificación de identidad, señales de riesgo y cumplimiento impulsadas por IA, publicó en mayo de este año la tercera entrega de su investigación global anual de consumidores. Los resultados de este año ponen de manifiesto la gran preocupación de los consumidores por los riesgos asociados a la IA generativa y las deepfakes, incluido el potencial aumento de la ciberdelincuencia y el fraude de identidad.

El estudio examinó las opiniones de más de 8.000 consumidores adultos, repartidos por igual entre el Reino Unido, Estados Unidos, Singapur y México. Los resultados sugieren que nueve de cada 10 consumidores mexicanos (89%) se preocupan diariamente de ser engañados por un deepfake para entregar información sensible o dinero, comparado con el 72% en general. Sólo el 15% de los consumidores globales afirma que nunca se ha encontrado con un vídeo, audio o imagen falsificada, mientras que el 60% ha estado expuesto a una deepfake en el último año.

Una mayoría significativa (60%) de los consumidores pide una mayor regulación gubernamental de la IA para abordar estos problemas. Sin embargo, la confianza en la regulación varía de un país a otro: el 69% de los consumidores de Singapur confía en la capacidad de su gobierno para regular la IA, frente al 26% del Reino Unido, el 31% de Estados Unidos y el 44% de México.

El fraude es un problema demasiado conocido para muchos consumidores de todo el mundo, ya que el 68% de los encuestados afirma saber o sospechar que ha sido víctima de fraude en línea o usurpación de identidad, o que conoce a alguien que lo ha sido. Casi la

[11] Jumio. (2023, 19 diciembre). Validación de identidad, KYC y biometria | Tecnología con IA. Jumio: End-to-End ID, Identity Verification And AML Solutions. https://www.jumio.com/es/tecnologia/

mitad de los encuestados mexicanos (47%) conoce a alguien que ha sido víctima de fraude en línea o robo de identidad, mientras que el 31% reportó saber o sospechar que ellos mismos han sido víctimas.

Mientras que casi la mitad (43%) de los consumidores mexicanos que fueron o sospecharon que fueron víctimas de fraude en línea o robo de identidad dijeron que la experiencia fue un inconveniente menor, el 33% dijo que causó problemas significativos y varias horas de trabajo administrativo para resolverlo, y el 19% llegó a calificarlo como una experiencia traumática.

Independientemente de si han sido víctimas de un fraude o de un robo de identidad, la mayoría de los consumidores mexicanos se preocupan diariamente por ser víctimas de filtraciones de datos (91%) y de ataques de robos de cuentas (91%).

A medida que navegamos por las complejidades introducidas por la IA generativa, el papel de los sistemas de seguridad sofisticados se vuelve crucial," dijo Philipp Pointner, jefe de identidad digital de Jumio. "Para contrarrestar el aumento de las deepfakes y el engaño cibernético, es imperativo incorporar sistemas de verificación multimodales y basados en la biometría. Estas tecnologías son clave para garantizar que las empresas puedan proteger sus plataformas y a sus clientes de las amenazas online emergentes, y son significativamente más fuertes que las contraseñas y otros métodos tradicionales y obsoletos de identificación y autenticación.

Por otra parte "La infodemia y su impacto en la vida digital" publicado en mayo de 2021[12], elaborada por Kaspersky y CORPA, señala que el 70% de los usuarios de las tecnologías en América Latina desconocen qué es el deepfake; siendo Perú el país donde más se le

[12] Diazgranados, H. (2021, 25 mayo). Investigación: la infodemia y su impacto en la vida digital. Blog Oficial de Kaspersky. https://latam.kaspersky.com/blog/investigacion-la-infodemia-y-su-impacto-en-la-vida-digital/21992/

desconoce con un 75%, seguido de México y Chile sólo 3 puntos porcentuales abajo, y Argentina con 67 %.

Según el Reporte Sensity AI[13] The State of deepfake 2024, proporciona varios puntos significativos sobre el uso de la inteligencia artificial (IA) en la comisión de delitos, particularmente en el contexto de la violencia de género. Un área muy utilizada en las campañas de influencia con deepfakes, empleadas para manipular la opinión pública, desacreditar a oponentes políticos e influir en elecciones. Estas campañas a menudo tienen como objetivo a figuras públicas y se difunden a través de redes sociales y plataformas digitales, lo que dificulta su detección y contrarrestación efectiva.

También señala que la comercialización de la IA ha reducido las barreras de entrada para la creación de deepfakes sofisticados, que ahora son utilizados por diversos actores, incluidos ciberdelincuentes, agencias adversarias y hacktivistas. Estas entidades utilizan la IA para llevar a cabo ciberguerra, ataques de phishing y difundir desinformación, todo lo cual puede desestabilizar las estructuras sociales, económicas y políticas

Destaca que las campañas de influencia y las estafas con deepfakes no están confinadas a una sola región, sino que son un fenómeno global. El uso generalizado de estas tecnologías tiene implicaciones significativas para la confianza pública, la estabilidad económica y la integridad de las comunicaciones en todo el mundo.

Estos hallazgos subrayan la importancia de abordar el uso indebido de la IA en los cibercrímenes, particularmente en el contexto de la violencia de género, ya que estas tecnologías pueden ser utilizadas como armas para perpetuar aún más el daño contra poblaciones vulnerables.

[13] Team, S. (2024, 4 julio). Reports - Sensity AI. Sensity. https://sensity.ai/reports/

Por otro lado un estudio realizado por el Centro de Estudios de Género de la Universidad Nacional Autónoma de México[14] (UNAM) señala la preocupante realidad de la violencia digital que afecta a las mujeres en México. Según los hallazgos, una gran mayoría de las mujeres que son víctimas de violencia digital no denuncian los incidentes. Este fenómeno de subregistro tiene varias causas, entre las cuales se destaca la falta de claridad sobre cómo las tecnologías emergentes, como la inteligencia artificial (IA), están involucradas en estos delitos.

Una de las principales razones por las que las mujeres no denuncian la violencia digital es la falta de comprensión sobre cómo la IA contribuye a estos actos de violencia. Muchas víctimas no están al tanto de que tecnologías como los algoritmos de inteligencia artificial pueden estar detrás del acoso automatizado que reciben en redes sociales, o de la creación de *deepfakes* que manipulan su imagen para generar contenido sexual no consensuado. Esta falta de conocimiento no solo impide que las víctimas identifiquen correctamente la naturaleza del delito, sino que también dificulta su capacidad para buscar justicia y protección.

Por ejemplo, en el caso de *deepfakes*, muchas mujeres no entienden cómo se crean estos videos falsos ni que están generados por IA. Esto les lleva a sentirse desconcertadas y avergonzadas, lo que a menudo resulta en su silencio y en la falta de denuncia. Además, la sofisticación de estas tecnologías hace que las víctimas duden de la capacidad de las autoridades para intervenir de manera efectiva, lo que refuerza la percepción de impunidad.

Otra razón crítica es la falta de capacitación de las autoridades para manejar casos que involucran tecnologías avanzadas como la IA. El estudio de la UNAM señala que muchas veces, cuando las mujeres intentan denunciar, se encuentran con un sistema legal que no está preparado para lidiar con las complejidades de la violencia facilitada por IA. Los

[14] CIEG - UNAM. (s. f.). https://cieg.unam.mx/

funcionarios encargados de recibir las denuncias a menudo carecen del conocimiento técnico necesario para comprender cómo la IA está implicada en estos delitos, lo que puede llevar a que las denuncias sean desestimadas o tratadas de manera inadecuada.

Esta falta de preparación institucional no solo desincentiva a las víctimas a denunciar, sino que también perpetúa la sensación de vulnerabilidad e indefensión entre las mujeres. Como resultado, la violencia digital facilitada por IA sigue creciendo, mientras que las respuestas legales y de protección permanecen ineficaces.

El impacto psicológico de la violencia digital es profundo, y cuando está facilitada por tecnologías avanzadas como la IA, este impacto puede ser aún más severo. El estudio de la UNAM resalta que muchas mujeres experimentan una profunda angustia emocional al enfrentarse a situaciones en las que su privacidad ha sido violada a través de la manipulación tecnológica. Este daño psicológico se ve exacerbado por la falta de apoyo adecuado, ya que las víctimas sienten que no existen recursos o vías efectivas para resolver su situación.

La vergüenza, el miedo a ser juzgadas y la sensación de impotencia contribuyen a que las mujeres opten por no denunciar. Esto no solo perpetúa el ciclo de violencia, sino que también genera una cultura de silencio que beneficia a los perpetradores, quienes continúan utilizando estas tecnologías sin temor a represalias.

El estudio subraya la necesidad urgente de implementar programas de educación y sensibilización tanto para las mujeres como para las autoridades sobre la naturaleza de la violencia digital facilitada por IA. Es crucial que las víctimas comprendan cómo estas tecnologías pueden ser utilizadas en su contra y que sepan que tienen el derecho de buscar protección y justicia. Asimismo, es fundamental que las instituciones encargadas de la aplicación de la ley y la protección de los derechos humanos estén debidamente capacitadas para manejar estos casos.

La creación de campañas de concienciación que expliquen cómo funciona la IA en el contexto de la violencia digital, y cómo denunciar estos incidentes, podría empoderar a las mujeres y aumentar el número de denuncias. Además, la implementación de políticas públicas que promuevan la capacitación de las autoridades y la mejora de los mecanismos de denuncia es esencial para garantizar que las víctimas reciban el apoyo y la justicia que merecen.

## VIII. Conclusión

La inteligencia artificial, aunque ofrece enormes beneficios, también ha exacerbado las desigualdades de género en México. Las tecnologías como los *deepfakes*, la discriminación algorítmica, y el acoso automatizado en línea son formas emergentes de violencia de género que afectan gravemente a las mujeres. Estas tecnologías perpetúan estereotipos y amplifican la violencia existente, lo que subraya la necesidad urgente de desarrollar un marco legal y regulatorio que integre una perspectiva de género. Sin una regulación adecuada, la IA continuará siendo una herramienta para perpetuar la violencia de género, lo que exacerbará las desigualdades sociales y afectará negativamente la participación de las mujeres en la sociedad.

La discriminación algorítmica en sectores como el empleo y el acceso a servicios financieros ha limitado significativamente las oportunidades económicas para las mujeres en México. Los algoritmos, al estar entrenados con datos sesgados, perpetúan desigualdades históricas, lo que reduce la participación económica de las mujeres y perpetúa la brecha de género. Es esencial implementar políticas públicas que regulen el diseño y uso de algoritmos con una perspectiva de género para garantizar que estas tecnologías no perpetúen la desigualdad económica.

La falta de conocimiento y comprensión sobre cómo la IA puede facilitar que la violencia de género sea un problema significativo. Es crucial desarrollar programas educativos y de sensibilización tanto para el público general como para los responsables de la formulación

de políticas y la aplicación de la ley. Estos programas deben incluir información sobre los riesgos asociados con la IA y la violencia de género, así como la formación en el uso seguro y ético de estas tecnologías. Además, las instituciones educativas deben incorporar la enseñanza de la ética de la IA y la igualdad de género en sus currículos, para preparar a las futuras generaciones para enfrentar estos desafíos.

**Perspectiva Jurídica y Necesidad de Reformas Legales.** Aunque México ha avanzado en la legislación para proteger a las mujeres contra la violencia digital, como la Ley Olimpia, las leyes actuales no son suficientes para abordar los desafíos específicos que plantea la inteligencia artificial. Es necesario reformar y actualizar el marco jurídico para incluir disposiciones específicas sobre la violencia de género facilitada por IA, tales como la creación de *deepfakes*, la discriminación algorítmica y el acoso automatizado. La falta de una legislación adecuada no solo deja a las mujeres vulnerables, sino que también dificulta la aplicación efectiva de la ley y la protección de sus derechos.

**Programas Gubernamentales y la Implementación de Políticas Públicas.** Es fundamental que el gobierno mexicano desarrolle e implemente programas específicos que aborden la violencia de género en el entorno digital. Estos programas deben incluir la creación de unidades especializadas dentro de las instituciones de justicia que estén capacitadas para manejar casos relacionados con la IA y la violencia de género. Además, el gobierno debe trabajar en colaboración con organizaciones de la sociedad civil y el sector privado para desarrollar políticas que promuevan el uso ético de la IA y protejan los derechos de las mujeres en el entorno digital.

**Nueva Agenda de Investigación**

**Desarrollo de Marcos Regulatorios para la IA con Perspectiva de Género**. La actual legislación mexicana no es suficiente para regular la violencia de género mediante IA. Es esencial desarrollar una agenda de investigación que explore cómo crear marcos regulatorios que incorporen una perspectiva de género en el desarrollo y uso de la IA. Esta

investigación debe analizar experiencias internacionales, identificar mejores prácticas, y adaptar soluciones a las realidades y necesidades de México.

**Evaluación de Algoritmos y Mitigación de Sesgos**. Es necesario llevar a cabo investigaciones que evalúen los algoritmos utilizados en diversas industrias en México, identificando y mitigando los sesgos de género. Estas investigaciones deben incluir el desarrollo de metodologías para auditar y corregir los algoritmos, asegurando que las tecnologías se utilicen de manera justa y equitativa.

**Impacto Psicológico y Social de la Violencia de Género Facilitada por IA**. Otra área crucial de investigación es el impacto psicológico y social de la violencia de género facilitada por IA en las mujeres. Esta investigación debe explorar cómo las tecnologías emergentes afectan el bienestar emocional de las víctimas y cuáles son las mejores prácticas para brindar apoyo psicológico y social a las mujeres afectadas.

**Colaboración Internacional para Enfrentar la Violencia de Género Mediante IA**. México debe fomentar la colaboración internacional en la investigación de la violencia de género facilitada por IA. Esto incluye participar en estudios comparativos, compartir datos y mejores prácticas, y colaborar en la creación de normativas internacionales que aborden esta forma de violencia de manera integral.

**Innovación Tecnológica para la Protección de las Mujeres**. Finalmente, es fundamental que la nueva agenda de investigación explore cómo la tecnología puede ser utilizada para proteger a las mujeres en lugar de perjudicarlas. Esto incluye el desarrollo de herramientas de IA que puedan detectar y prevenir la violencia de género en línea, así como aplicaciones que ayuden a las mujeres a mantenerse seguras en el entorno digital.

En suma, toda investigación que aborde la violencia de género facilitada por inteligencia artificial en México revela no solo la urgente necesidad de actualizar y expandir el marco jurídico, si no de forma transversal y simultanea desarrollar políticas públicas integrales, y

promover una educación y sensibilización profunda en todos los niveles de la sociedad. La IA tiene el potencial de ser una herramienta poderosa para el bien, pero sin una regulación adecuada y una perspectiva de género clara, también puede perpetuar y amplificar las desigualdades existentes. La nueva agenda de investigación debe enfocarse en la creación de soluciones innovadoras y sostenibles que protejan los derechos de las mujeres y promuevan la igualdad de género en la era digital.

## IX. Bibliografía

Almarza, Oscar. (2020). La tecnología que realiza los deep fakes podría contribuir en el sector de la medicina. https://urbantecno.com/tecnologia/ tecnologia-deep-fakes-medicina.

Avendaño, Elizabeth. Luchadoras.mx La Comisión de Derechos Digitales del Senado y sus iniciativas de regulación de tecnologías e inteligencia artificial. https://luchadoras.mx/quienes-somos/

Barrera, Lulú V.(10 de diciembre de 2019). *Violencia contra las mujeres en medios digitales del Conversatorio Violencia contra las mujeres en espacios digitales*. Ciudad de México. Luchadoras. Recuperado de https://www.youtube.com/watch?v=rBaNZtD_ueg&t=7811s

Bañuelos Capistrán, Jacob. (2020). Deepfake: la imagen en tiempos de la posverdad. Revista Panamericana de Comunicación, Año 2, N. 1, enero-junio 2020, Recuperado: https://revistas.up.edu.mx.

Biurrun, Alfredo. (2021). Deep Voice: tecnología que falsifica la voz y con la que han robado 35 millones de dólares en La Razón. Recuperado de: larazon.es/ tecnologia/20211016/ivt7yazbmzb7lmxknhf2hz2fma.html.

CORPA y Kaspersky. (2021). La infodemia y su impacto en la vida digital de 2021. Recuperado: https:// latam.kaspersky.com/blog/investigacion-la-infodemia-y-suimpacto-en-la-vida-digital/21992/. Pérez, Enrique. (2019).

CIEG - UNAM. (s. f.). https://cieg.unam.mx/

Dastin, J. (2018). "Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women." Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

Diazgranados, H. (2021, 25 mayo). Investigación: la infodemia y su impacto en la vida digital. Blog Oficial de Kaspersky. https://latam.kaspersky.com/blog/investigacion-la-infodemia-y-su-impacto-en-la-vida-digital/21992/

DeepNude: la polémica aplicación que "desnuda" a cualquier mujer mediante inteligencia artificial en Xataca. Recuperado de: https://www.xataka. com/privacidad/deepnude-polemica-aplicacion-que-desnuda-acualquier-mujer-mediante-inteligencia-artificial.

García Celis, Frida . (2022). *¿Qué datos sobre género hay en México?*. México. Tecnología Digital para el Cambio Social Recuperado de https://escueladedatos.online/que-datos-sobre-genero-hay-en-mexico/

Gómez, Fernanda. (16 de diciembre de 2019). *Violencia sexual digital. Un balance de la ley Olimpia en CDMX*. México. Luchadoras.mx Recuperado de https://luchadoras.mx/un-balance-de-la-ley-olimpia-en-cdmx/

Instituto de Investigaciones Jurídicas de la UNAM. (2021). La violencia digital contra las mujeres un problema de género. México. UNAM. Recuperado de https://archivos.juridicas.unam.mx

InfoCdMex. (2024, 19 junio). #ENVIVO 📽 FORO: «ConcienCIA Digital» Inteligencia artificial y privacidad. [Vídeo]. YouTube. https://www.youtube.com/watch?v=J4f3qeQ7ZQ0

INMUJERES. Programa Nacional para la Igualdad entre Mujeres y Hombres 2020 2024. gob.mx. https://www.gob.mx/inmujeres/acciones-y-programas/programa-nacional-para-la-igualdad-entre-mujeres-y-hombres

INEGI. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023. https://www.inegi.org.mx/programas/endutih/2023/

INEGI, Módulo sobre Ciberacoso 2023. (2024, 6 agosto). https://www.inegi.org.mx/rnm/index.php/catalog/999

Jumio. (2023, 19 diciembre). Validación de identidad, KYC y biometria | Tecnología con IA. Jumio: End-to-End ID, Identity Verification And AML Solutions. https://www.jumio.com/es/tecnologia/

Luchadoras México. (25 Mayo 2020). La violencia sexual digital: ¿más leyes, más justicia?. México. GenderIT.org Recuperado de https://www.apc.org/es/blog/la-violencia-sexual-digital-mas-leyes-mas-justicia

Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. New York University Press. https://nyupress.org/9781479837243/algorithms-of-oppression/

Tanaka, H. (2021). "AI and Gender-Based Violence: The Legal Challenges in Japan." *Japanese Journal of Law and Society*, 23(4), 120-136.

Tratados Multilaterales. *Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la mujer "Convención De Belem Do Para"* Recuperado de https://www.oas.org/juridico/spanish/tratados/a-61.html

Sensity, Report 2024: The State Of Deepfakes, 2024. Recuperado de: https://sensity.ai/reports/ y Team, S. (2024, 4 julio). Reports - Sensity AI. Sensity. https://sensity.ai/reports/

Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias (REVM-ONU) (14 de Junio de 2018). A/HRC/38/47. *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*. Recuperado de https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

Cámara de Diputados. (2022). *Ley General de Acceso de las Mujeres a una Vida Libre de Violencia*. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf

Cámara de Diputados. (2022). *Código Penal Federal*. México. Recuperado de https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Asamblea General de las Naciones Unidas, (Estados Unidos de Norteamerica) *Resolución 71/199, El derecho a la privacidad en la era digital, aprobada por la Asamblea General de las Naciones Unidas* el *25 de enero de 2017.* Recuperado de https://www.un.org/es/ga/71/resolutions.shtml

Tratados Multilaterales. *Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la mujer "Convención De Belem Do Para"* Recuperado de https://www.oas.org/juridico/spanish/tratados/a-61.html

Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias (REVM-ONU) (14 de Junio de 2018). A/HRC/38/47. *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*. Recuperado de https:// www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

ONU Mujeres, Comisión Interamericana de Mujeres, y el Mecanismo de Seguimiento de la Convención Belém do Pará. (2022). *Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención Belen Do Pará*. América Latina. ONU Mujeres e Iniciativa Spotlight Recuperado de https://lac.unwomen.org/sites/default/files/2022-04/Informe-Ciberviolencia-MESECVI_1Abr.pdf

OEA (2019). *Combatir la Violencia en Línea un Llamado a la Protección Contra las Mujeres.* Organización de los Estados Americanos OEA. Recuperado de https://www.oas.org/es/sms/cicte/docs/20191125-ESP-White-Paper-7-VIOLENCE-AGAINST-WOMEN.pdf

World Economic Forum. (2021). "Global Gender Gap Report 2021." https://www.weforum.org/reports/global-gender-gap-report-2021