VERITAS, Nº 61, 32-67 ISSN 0718-9273

Análisis del abuso de aplicaciones deepfake y su impacto en la violencia digital de género en América Latina y el Caribe*

Ximena Cuzcano-Chavez**
ximena@situada.online
Investigadora de Situada (Lima, Perú)

Constanza González-Véliz***
constanza@situada.online
Directora General e Investigadora de Situada (Talca, Chile)

Resumen

Las tecnologías actuales no son neutrales. Reflejan las necesidades, perspectivas y experiencias de quienes las desarrollan. Estos sesgos han dado lugar a la creación de armas digitales como los deepfakes, una tecnología que, de manera desproporcionada, se utiliza en mujeres para crear contenido sexual. El presente estudio analiza el auge de aplicaciones deepfake en América Latina y el Caribe (ALAC), enfocándose en su disponibilidad, facilidad de uso y los riesgos que representan en contextos de desigualdad estructural y violencia digital de género. Para ello, se realizó una recolección automatizada de datos mediante una API, identificando 105 aplicaciones deepfake disponibles a diciembre de 2024 en Google Play Store. Posteriormente, se llevó a cabo una evaluación fundamentada en dimensiones como año, alcance, diseño, accesibilidad, modelos de negocio y funcionalidades. Finalmente, se realizó un análisis crítico para comprender cómo estas herramientas configuran dinámicas de poder, perpetúan narrativas de cosificación y amplifican la violencia digital contra las mujeres. Los hallazgos evidencian un diseño intencionado que facilita la adopción de estas aplicaciones, eliminando barreras técnicas y normalizando la cosificación de los cuerpos de las mujeres, siendo el 89.5% de estas herramientas un potencial peligro para ellas. La investigación enfatiza la urgencia de cuestionar la supuesta neutralidad de estas tecnologías y la necesidad de repensar su desarrollo desde una perspectiva que contribuya a construir entornos digitales más seguros y respetuosos para todas las personas.

---

* Esta investigación se enmarca en el proyecto VERITAS (Vulnerabilidades, Estrategias y Reflexiones sobre la Innovación Tecnológica y Asimetrías de Género en América Latina y el Caribe) desarrollado por Situada, una organización independiente dedicada a explorar la tecnología desde una perspectiva latinoamericana y feminista. https://situada.online/.

** Estudiante del Magíster en Éticas Aplicadas, Máster en Ciberseguridad e Ingeniera de Sistemas. Investiga las implicancias éticas de las tecnologías digitales, con énfasis en la seguridad digital y el desarrollo tecnológico situado en América Latina. En Situada Online, trabaja por una tecnología que sea ética, segura y orientada al bien común, considerando sus impactos sociales, territoriales y diferenciales.

*** Estudiante de Doctorado en Ciencias, Máster en Estudios Feministas, Magíster en Gestión Tecnológica (c) e Ingeniera Forestal. Investiga la intersección entre mujeres, ciencia y tecnología desde una perspectiva feminista latinoamericana. Directora General en Situada Online, espacio desde el cual impulsa investigaciones sobre sesgos de género, producción de conocimiento y justicia tecnológica en América Latina.

Recibido: 30/04/2025 - Aceptado: 21/07/2025

Palabras clave: tecnología patriarcal – aplicaciones deepfake – violencia digital de género – derechos de las mujeres – ética algorítmica

Analysis of the abuse of deepfake applications and their impact on digital gender violence in Latin America and the Caribbean

Abstract

Current technologies are not neutral; they reflect the needs, perspectives, and experiences of their developers. These biases have led to the creation of digital weapons like deepfakes, a technology that is disproportionately used against women to create sexual content. This study examines the rise of deepfake applications in Latin America and the Caribbean (LAC), focusing on their availability, ease of use, and the risks they pose in contexts of structural inequality and digital gender-based violence. To that end, an automated data collection was carried out using an API, identifying 105 deepfake applications available on the Google Play Store as of December 2024. Subsequently, an evaluation was conducted based on criteria such as year, scope, design, accessibility, business models, and functionalities. Finally, a critical analysis was performed to understand how these tools shape power dynamics, perpetuate objectification narratives, and amplify digital violence against women. The findings reveal an intentional design that facilitates the adoption of these applications, removing technical barriers and normalizing the objectification of women's bodies, with 89.5% of these tools posing a potential danger to them. The research emphasizes the urgency of questioning the supposed neutrality of these technologies and the need to rethink their development from a perspective that contributes to building safer and more respectful digital environments for everyone.

***Keywords**: patriarchal technology – deepfake applications – technology-facilitated gender based violence – women's rights – algorithmic ethics*

1. Introducción

La tecnología no es neutral; desde su diseño hasta su implementación, está moldeada por valores y decisiones humanas de quienes la crean, y a menudo refleja sesgos que refuerzan desigualdades y excluyen a comunidades vulnerables (Noble, 2018; Hare, 2022). Esta idea también ha sido desarrollada por pensadores como Neil Postman, quien sostiene que la amenaza no está en el uso de la tecnología, sino en los usos que esta posibilita (Rocha, 2022). Estos sesgos se manifiestan en dispositivos que no consideran la diversidad de personas usuarias o plataformas que no priorizan la seguridad de las mujeres o algoritmos que perpetúan violencia digital de género. Este es el caso de las aplicaciones deepfake, cuyo uso plantea serios peligros en la actualidad.

Según Sensity AI, para el año 2019, el 96% de los deepfakes eran material sexual no consensuado y, de ellos, el 99% presentaba a mujeres (Sensity AI, 2019). Este panorama persiste, ya que el informe "State of Deepfake 2023" de Security Heroes reveló que el 99% de la pornografía

deepfake sigue aplicada en mujeres (Security Heroes, 2023), con un aumento del 464% en su creación entre 2022 y 2023, pasando de 3,725 a 21,019 videos.

En contextos de desigualdad estructural como América Latina y el Caribe (ALAC), donde las mujeres enfrentan altos niveles de violencia de género, los riesgos digitales se amplifican. Las aplicaciones deepfake han facilitado la reproducción y difusión de abusos contra mujeres, como lo demuestran casos recientes ocurridos entre 2023 y 2024 en colegios e institutos de países como Perú, Ecuador, México y Chile (Rojas, 2023; Vistazo, 2023; Rodríguez, 2023; Molina, 2024) donde niñas y adolescentes fueron víctimas de deepfakes sexuales difundidos por sus propios compañeros. Este estudio tiene como objetivo evaluar la disponibilidad de las apps deepfake en Android y analizar críticamente su facilidad de uso y potencial uso indebido, con el fin de comprender cómo estas tecnologías pueden influir en las dinámicas de poder y violencia contra las mujeres.

Los resultados muestran que el 89.5% de estas aplicaciones representan un riesgo para las mujeres, al facilitar la creación de contenido sexual no consensuado. Además, se evidencia una normalización de la cosificación femenina, patrones de diseño sexistas y una alarmante falta de regulación en las plataformas que las alojan.

2. Marco conceptual y teórico

2.1. Conceptos Asociados al deepfake

2.1.1. Concepto y funcionamiento

El término *deepfake* surge de la combinación de *deep*, referido al aprendizaje profundo (deep learning), y *fake*, que significa falso en inglés (Altuncu et al., 2022). Los deepfakes son medios digitales falsos creados mediante algoritmos de deep learning, una rama de la inteligencia artificial (Heidari et al., 2023). Esta técnica se ha convertido en la forma de alteración digital más famosa y ampliamente utilizada, especialmente para superponer el rostro de una persona sobre el cuerpo de otra (Albahar y Almalki, 2019).

Su tecnología base son las Redes Generativas Antagónicas, o GAN por sus siglas en inglés. GAN se basa en la interacción de dos redes neuronales: la red generativa y la red discriminadora (Citron y Chesney, 2019). La red generativa se encarga de crear datos, como imágenes o videos falsos, mientras que la red discriminadora evalúa la autenticidad de las creaciones de la primera red (Yadav y Salmani, 2019). En otras palabras,

la red discriminadora informa a la red generativa si el contenido que ha creado es convincente o si necesita ser mejorado. A través de un proceso iterativo de entrenamiento, ambas redes mejoran: la generativa perfecciona las falsificaciones y la discriminadora afina su capacidad para detectarlas, generando contenido casi indistinguible del real (Yadav y Salmani, 2019; Zhu et al., 2017).

2.1.2. Origen del deepfake

Las redes GAN han transformado el campo de la inteligencia artificial, pero su impacto requiere explorar sus orígenes. Ian Goodfellow, creador de las GANs, relató en una entrevista con el portal de noticias *The Batch* (2020) que la idea surgió informalmente durante una conversación entre copas en un bar de Montreal. Esa misma noche comenzó a codificar la primera GAN, con la expectativa de que tendría aplicaciones significativas en ámbitos como ciencia y medicina.

Aunque Goodfellow reconoce los beneficios de las GANs, también reconoce sus riesgos. En entrevistas (MIT Technology Review, 2018; Lex Fridman, 2019), sostuvo que no existen soluciones exclusivamente tecnológicas para combatir la desinformación visual, y que es necesario fomentar el pensamiento crítico. Además, confía en que en las próximas décadas se desarrollen mecanismos para autenticar contenidos digitales y protegerlos de ataques adversarios. Sin embargo, esta posición traslada la responsabilidad casi por completo a las y los usuarios, minimizando el rol ético que deberían asumir quienes diseñan y comercializan estas herramientas. Aunque resalta el potencial de las GANs, Goodfellow no profundiza en cómo estas tecnologías pueden ser utilizadas para crear contenido perjudicial, como deepfakes que explotan imágenes de mujeres sin su consentimiento. Esta omisión refleja una visión tecnocrática que subestima los impactos sociales de la innovación y contribuye a un modelo de desarrollo tecnológico carente de responsabilidad ética.

2.1.3. Tipos de tecnología deepfake

Las tecnologías deepfake incluyen diversas técnicas diseñadas para manipular contenido, alterando la identidad o acciones de una persona. Entre los tipos más comunes está el intercambio de rostros (Face-Swap), que reemplaza el rostro de una persona con el de otra en imágenes o videos. (Pei et al., 2024; Mubarak et al., 2023; Farid y Schindler, 2020). La sincronización de labios (Lip-Syncing), que ajusta los movimientos labiales

para coincidir con un audio diferente, creando la ilusión de que alguien dice algo que no dijo (Masood et al., 2021; Rahman et al., 2022; Farid y Schindler, 2020).

La marionetización (Head Puppetry o Puppet Master) manipula movimientos de la cabeza, ojos y expresiones faciales para imitar gestos de otra persona, haciendo parecer que realiza acciones que nunca hizo (Sencar et al., 2022; Rahman et al., 2022; Farid y Schindler, 2020) y finalmente, la manipulación facial (Facial Manipulation), que modifica las expresiones o características faciales, cambiando emociones o gestos específicos.

2.1.4. Evolución del deepfake

Los deepfakes surgieron en 2017 con su popularización en Reddit, cuando un usuario creó videos falsos de celebridades mujeres en situaciones sexuales (González-Véliz y Cuzcano-Chavez, 2024). Desde entonces, estas tecnologías han expuesto a las mujeres a graves riesgos, convirtiéndose en herramientas de humillación y sexualización.

Aunque algunos estudios destacan posibles aplicaciones positivas, como resucitar artistas fallecidos, crear monumentos digitales o personalizar publicidad de manera económica (Seow et al., 2022; Petrova y Zonova, 2022), estos usos plantean dilemas éticos en torno al consentimiento y la explotación de imágenes de las personas representadas. La mayoría de estudios coinciden en que los impactos negativos asociados a esta tecnología superan sus beneficios (Seow et al., 2022; Masood et al., 2021; Khan y Dang-Nguyen, 2023). Desde su aparición, los deepfakes han sido utilizados para crear contenido sexual no consensuado y como medio para facilitar actos de extorsión y otras formas de violencia digital de género.

Un avance crucial ha sido el desarrollo de sistemas automatizados para detectar deepfakes. Sin embargo, como señalan Khan y Dang-Nguyen (2023), la detección y generación de deepfakes es como un *juego del gato y el ratón*, donde las mejoras en un área generan nuevos desafíos en la otra. (Masood et al., 2021). Un ejemplo es un estudio que usó el parpadeo como señal para detectar deepfakes, que quedó obsoleto cuando se perfeccionó la generación de videos con parpadeo realista (Masood et al., 2021).

Otro factor preocupante es la disponibilidad de datos. En la era de las redes sociales, resulta sencillo acceder a grandes cantidades de fotos y

videos de cualquier persona, materiales que pueden ser utilizados como base para capturar la estructura facial y expresiones, permitiendo así la creación de deepfakes altamente realistas (Stevens, 2020). Además, el software de creación de deepfakes como las aplicaciones gratuitas y tutoriales en línea, asegura que los deepfakes continúen propagándose, planteando desafíos en términos de seguridad digital.

2.2. Deepfake y violencia digital de género

El uso de tecnologías deepfake se ha convertido en una forma alarmante de violencia de género, al facilitar la creación de imágenes y videos sexualizados sin consentimiento, dirigidos en su mayoría contra mujeres y niñas (González-Véliz y Cuzcano-Chavez, 2024).

La mayoría de los deepfakes que circulan en Internet están destinados a la pornografía no consensuada, superponiendo rostros de mujeres en escenas sexuales falsas (Tripathi, 2019). Estas imágenes, que aparentan autenticidad, fueron utilizadas como mecanismos de venganza o entretenimiento misógino, con impactos graves sobre la integridad, salud mental y vida social de las víctimas (Chesney y Keats Citron, 2019).

Como señalan Cerdán y Padilla-Castillo (2019), estas tecnologías construyen un imaginario falsificado que perpetúa la degradación simbólica de las mujeres, reproduciendo roles tradicionales de subordinación y despersonalización. Mientras los hombres suelen aparecer en deepfakes de tono humorístico o político, las mujeres son representadas en contextos íntimos y sexualizados.

Esta forma de violencia digital se suma a otras ya documentadas como el ciberacoso, el hostigamiento sexual y la difusión no consentida de imágenes íntimas, con consecuencias graves sobre la privacidad y autonomía las mujeres (González-Véliz y de Andrés, 2023). A menudo, la agresión se trivializa, culpabilizando a las víctimas por su exposición en línea, mientras los agresores son eximidos de su responsabilidad. Como advierte la OEA (2021a), los medios, las plataformas y algunas instituciones tienden a minimizar el daño, infantilizar a los perpetradores y legitimar el retiro de las mujeres del espacio digital como única vía de protección.

Aplicaciones de deepfake, mayoritariamente desarrolladas por hombres, permiten desnudar digitalmente a mujeres con un solo clic, sin que sus desarrolladores enfrenten consecuencias, incluso cuando sus

productos han sido utilizados para acosar, chantajear o silenciar a mujeres (Cole, 2019a; 2019b).

Además de vulnerar derechos como la privacidad, el consentimiento y la libertad de expresión, el impacto de esta violencia trasciende el entorno digital: muchas mujeres optan por limitar su participación en redes sociales, en espacios de opinión o en entornos académicos por miedo a ser blanco de manipulación digital (CEPAL, 2023). Esta censura anticipada refuerza jerarquías de género, restringe su agencia y socava su autonomía. Tal como señala la CEPAL (2023), la violencia digital contra las mujeres impide el ejercicio de sus derechos y además obstaculiza su inclusión plena en los ecosistemas digitales, debilitando así la democracia y la igualdad.

3. Diseño metodológico para la evaluación de aplicaciones deepfake y su análisis crítico

La metodología adoptada en este estudio responde a la necesidad de analizar de forma integral y crítica las aplicaciones deepfake, atendiendo tanto a sus características técnicas como a sus implicaciones éticas. El objetivo fue construir un marco metodológico sólido para identificar, evaluar y analizar estas herramientas en el contexto de ALAC. Para ello, se implementaron cuatro fases interrelacionadas: (i) Revisión sistemática de la literatura, (ii) Revisión de metodologías de evaluación de aplicaciones móviles, (iii) Búsqueda y recolección de aplicaciones disponibles y (iv) Definición de dimensiones de evaluación de las aplicaciones y análisis crítico.

Dado que Android es el sistema operativo que lidera el mercado móvil en ALAC con una cuota del 88.24% (StatCounter, 2024), y que esta tendencia es corroborada por Melo (2024), que muestra una amplia adopción de Android en todos los países de la región, se seleccionó Google Play como fuente principal para la identificación de aplicaciones. Esta decisión permite contextualizar los hallazgos de acuerdo con la realidad tecnológica regional, asegurando la pertinencia del análisis.

3.1. Revisión sistemática de la literatura

En la primera fase, se realizó una revisión sistemática en bases de datos académicas como Scopus, Google Scholar, ACM, IEEExplore, Web of Science, y ScienceDirect. El objetivo fue identificar investigaciones previas que analizaran la disponibilidad y facilidad de uso de aplicaciones

deepfake. Utilizando operadores avanzados y palabras claves acompañadas del término 'deepfake' tales como *application usability*, *apps*, *ease of use*, *application analysis*, *tools*, *availability*, *accessibility*, *mobile applications*, *software*, y *technology*, se encontraron 2722 artículos hasta el 15 de octubre de 2024.

Tras descartar estudios centrados en la detección de deepfakes o en su uso en industrias como el marketing o cine, se seleccionaron 16 estudios relevantes centrados en herramientas y modelos deepfake, percepción de personas usuarias, capacidad de personas usuarias novatas para crear deepfakes y discusiones éticas o educativas vinculadas. Sin embargo, no se halló una evaluación integral ni análisis crítico sobre la disponibilidad y facilidad de uso de estas tecnologías en aplicaciones móviles, lo que evidenció una laguna significativa en la literatura y motivó las fases siguientes.

3.2. Revisión de metodologías de evaluación en aplicaciones móviles

En la segunda fase, se realizó una revisión de estudios centrados en la evaluación de aplicaciones móviles en sectores como salud, educación y ciberseguridad. Este análisis permitió identificar metodologías y dimensiones clave aplicados en estos contextos, así como reconocer sus limitaciones para proponer una perspectiva crítica y contextualizada.

Entre las dimensiones técnicas más relevantes, Aydin & Silahtaroglu (2021) y Dawson et al. (2019) combinaron técnicas manuales y automáticas para recopilar aplicaciones mediante APIs, evaluando elementos como privacidad, modelos de monetización y de negocio, descripciones, reseñas, categorización de contenido, versión y cantidad de instalaciones. Fasano et al. (2019) analizaron diferencias de calidad entre aplicaciones de tiendas oficiales y no oficiales, utilizando rastreadores web y herramientas automatizadas. En el ámbito multidisciplinario, Dawson et al. (2019) evaluaron contenido, usabilidad, estética y compromiso de aplicaciones nativas disponibles en mercados oficiales mediante una búsqueda bibliográfica en bases académicas.

En el sector salud, Hensher et al. (2021) revisaron marcos de evaluación para aplicaciones móviles, identificando dominios clave como experiencia, seguridad, privacidad, validez del contenido y accesibilidad. Frid et al. (2021), por su parte, evaluaron aplicaciones móviles de embarazo con un sistema de puntuación basado en integridad, privacidad,

precio, compras en la aplicación, conectividad y navegación. Patel y Dalal (2016) propusieron dimensiones relacionadas con usabilidad, como efectividad, eficiencia, utilidad, accesibilidad, facilidad de aprendizaje y satisfacción. Hussain et al. (2012) desarrollaron un modelo basado en *Goal Question Metric* (GQM), que fue adaptado por Hashim e Isse (2019) para aplicaciones de turismo.

En el área de ciberseguridad, Dini et al. (2012) clasificaron aplicaciones Android de tiendas no oficiales según confiabilidad, seguridad y funcionalidad. En educación, Dewi et al. (2018) evaluaron aplicaciones diseñadas para enseñar escritura en caracteres de Java considerando facilidad de uso, satisfacción, utilidad y facilidad de aprendizaje. Hussain et al. (2015) revisaron marcos que combinan diseño centrado en el usuario (HCI) y metodologías ágiles, mientras que Ahmad (2023) destacó dimensiones como uso de CPU, memoria, tamaño de la aplicación, acceso a hardware y soporte multiplataforma.

A pesar de estos avances, se observa una omisión recurrente de dimensiones éticas y sociales. Se tiende a asumir que las aplicaciones son inherentemente beneficiosas, sin cuestionar riesgos de uso indebido o sesgos en su diseño. Aunque la implementación de APIs para la recopilación automatizada de datos representa un avance metodológico importante, y fue incorporada en la siguiente fase, resulta imprescindible complementarla con un análisis basado en criterios éticos, que permita comprender los riesgos que estas tecnologías implican en contextos sociales específicos.

3.3. Búsqueda y recolección de aplicaciones disponibles

En la tercera fase, se implementó una estrategia experimental para identificar aplicaciones deepfake disponibles en Google Play. Basándose en las metodologías identificadas en la fase anterior, se seleccionaron los términos *deepfake*, *face swap*, *AI video*, *face morphing*, *deep learning video*, *fake video generator*, *lip-syncing*. Esta combinación de términos fue seleccionada por su capacidad para abarcar una amplia gama de aplicaciones que utilizan técnicas de deepfake más comunes, las cuales fueron previamente definidas en el marco conceptual.

Se desarrolló un script en Python haciendo uso de una API que se conectó a Google Play, el cual permitió extraer de manera automatizada información detallada sobre las aplicaciones asociadas a cada uno de los términos de búsqueda.

La búsqueda inicial identificó un total de 633 aplicaciones. Se llevó a cabo un proceso de filtrado manual que consistió en la eliminación de duplicados, es decir, aplicaciones repetidas en diferentes términos de búsqueda. Además, se realizó una revisión manual de las descripciones de cada aplicación para eliminar aquellas que, a pesar de estar asociadas a las palabras clave, no cumplían con la función de generar contenido deepfake. Tras este proceso, se obtuvo un conjunto de 112 aplicaciones candidatas. Posteriormente, se descartaron aquellas que no estaban disponibles en la región Latinoamericana, reduciendo el conjunto a 107 aplicaciones. Finalmente, se eliminaron las aplicaciones que presentaban errores al ejecutarlas, resultando en un conjunto final de 105 aplicaciones para un análisis posterior.

Cabe resaltar que, durante la fase de evaluación, se observó que algunas aplicaciones incluían anuncios que promocionaban otras aplicaciones deepfake con nombres propios específicos, lo que dificultó su detección mediante los términos de búsqueda empleados. Esto sugiere que el conjunto de aplicaciones analizado representa una muestra significativa, pero no total, de la oferta disponible de aplicaciones deepfake en Google Play. Por tanto, los hallazgos derivados deben ser interpretados como una estimación aproximada del alcance del fenómeno en la tienda de aplicaciones.

3.4. Definición de dimensiones de evaluación de las aplicaciones y análisis crítico

En la cuarta fase, se definieron las dimensiones de evaluación a partir de los hallazgos obtenidos en las fases anteriores. Inicialmente, se consideraron dimensiones técnicas obtenidas durante la recolección de datos como nombre, URL, año de creación, calificaciones, empresa o equipo de desarrollo, número de descargas y descripción.

Posteriormente, y con el fin de incorporar una mirada crítica y feminista, se ampliaron las dimensiones de análisis hacia aspectos sociotécnicos más complejos. Entre estas dimensiones se incluyeron su público objetivo, idioma, género representado en las imágenes de portada, modelo de negocio, precio (en caso de ser de pago), funcionalidades, facilidad de uso y si la aplicación representaba un peligro para las mujeres. La integración de estos criterios permitió desarrollar un enfoque metodológico mixto (cuantitativo y cualitativo), garantizando una

evaluación crítica y contextualizada, que aporte a la comprensión de los riesgos asociados al uso de tecnologías deepfake.

4. Resultados

4.1. Evaluación de aplicaciones

La evaluación de las 105 aplicaciones recolectadas se realizó entre noviembre y diciembre de 2024, aplicando las dimensiones previamente definidas. Cabe resaltar que, considerando los riesgos asociados a la divulgación de información que podría ser utilizada para reproducir violencia digital de género, se decidió anonimizar los datos que permiten identificar a las aplicaciones analizadas. En consecuencia, nombres, enlaces y detalles específicos de las aplicaciones fueron omitidos en los resultados públicos. El conjunto de datos completo permanece restringido para fines académicos, y su acceso está sujeto a supervisión con el objetivo de garantizar un uso responsable de la información y evitar cualquier contribución a la proliferación de herramientas que puedan ser utilizadas para causar daño.

Asimismo, con el propósito de evitar cualquier afectación a la privacidad, integridad o consentimiento de personas reales durante las pruebas, se prescindió completamente del uso de imágenes reales. En su lugar, se emplearon retratos generados artificialmente mediante la plataforma *This Person Does Not Exist*[1], la cual utiliza redes GAN para producir rostros fotorrealistas de personas inexistentes.

4.2. Resultados

Esta fase se centró en identificar y describir patrones técnicos, funcionales y sociales observados en las aplicaciones evaluadas. Se presentan a continuación los principales hallazgos empíricos por dimensión, con especial atención a elementos que podrían estar vinculados con dinámicas de riesgo o exposición digital, particularmente en el caso de mujeres.

4.2.1. Año de creación

Del total de 105 aplicaciones analizadas, se observa un crecimiento acelerado en su desarrollo durante los últimos años (2015–2024).

[1] Disponible en: https://thispersondoesnotexist.com/.

Tabla 1 Año de creación - Resultados

Año de creación	**Número de apps**	**%**
De 2015 a 2022	28	26.67
2023	33	31.43
2024	44	41.90

Este auge está vinculado al avance de tecnologías como las redes GAN, introducidas en 2014, que hicieron posible la creación de herramientas utilizadas como armas de violencia. Si bien las primeras aplicaciones deepfake surgieron en 2017 con el primer caso en Reddit, fue a partir de 2023 cuando los incidentes dirigidos a mujeres y niñas ganaron visibilidad, impulsando el desarrollo y la demanda de este tipo de aplicaciones.

Es relevante mencionar que algunas aplicaciones previas a 2017 inicialmente diseñadas para el retoque de fotos y videos, evolucionaron con el tiempo para incorporar funcionalidades deepfake, mostrando una evolución hacia usos más sofisticados y, en muchos casos, dañinos.

4.2.2. Autoría

La procedencia de las aplicaciones analizadas permite examinar la transparencia de los equipos de desarrollo, su relación con contextos tecnológicos y las posibles limitaciones para la rendición de cuentas. A continuación, se presenta una tabla con los países de autoría identificados o declarados en Google Play.

Tabla 2 Autoría - Resultados

País de autoría	**Número de apps**	**%**
No especificado	45	42.86
Turquía	16	15.24
Singapur	11	10.48
Estados Unidos	8	7.62
China	7	6.67
India	7	4.76
Japón	2	1.90
Otros	9	<1% cada uno

Del total de aplicaciones analizadas, la mayoría fue desarrollada por equipos cuya ubicación no se encuentra declarada en Google Play, así como otros detalles como la página web o descripción de la autoría.

Entre las aplicaciones con información disponible, Turquía, Singapur y Estados Unidos concentran la mayor proporción. Turquía destaca por su auge como centro de desarrollo en inteligencia artificial móvil (Rodríguez, 2024). Singapur es conocido por impulsar proyectos basados en IA generativa (Lacort, 2024), mientras que Estados Unidos continúa siendo uno de los principales exportadores de herramientas digitales a escala global. No se identificaron desarrollos originados en ALAC, limitada principalmente al consumo y no a la producción.

En una muestra reducida de empresas con presencia digital pública, se identificaron algunos patrones relevantes en sus comunicaciones institucionales, como la declaración de prácticas "éticas" en el uso de IA o el discurso de "democratización del acceso" a sus tecnologías. También se recolectaron datos visibles sobre la composición de equipos técnicos, observándose una notable brecha de género en varios casos. Por ejemplo, una empresa reporta en su página web una composición de 19 hombres frente a 4 mujeres. En otra empresa, más del 50% del equipo también está compuesto por hombres, en su staff visible.

4.2.3. Descripciones

Muchas aplicaciones deepfake se presentan ante el público mediante breves descripciones promocionales en la Google Play, que constituyen una primera aproximación a sus valores, usos esperados y públicos objetivo, por lo que su análisis permite detectar patrones discursivos.

Del total de aplicaciones analizadas, una gran mayoría utiliza descripciones centradas en el entretenimiento, la viralización de contenidos y la creatividad. Frases como "liberar tu creatividad", "dar vida a tus ideas", "crear contenido viral" o "hacer que tu cara baile" son utilizadas recurrentemente como parte de una narrativa positiva y comercial. En términos generales, este tipo de lenguaje promueve el uso de tecnologías generativas de imagen y video como herramientas sin riesgo aparente, enfocadas al consumo masivo y la producción de contenidos compartibles en redes sociales.

Un hallazgo particularmente preocupante es el uso de términos que refuerzan estereotipos de género, como "crear selfies hermosos" o

"transformarte en una princesa Barbie", alineándose con ideales de belleza sexistas.

4.2.4. Público objetivo y clasificación de contenido

Cada aplicación disponible en Google Play Store incluye una sección sobre el público objetivo, asignada mediante el sistema de "Clasificación del contenido de apps y juegos" (Google, 2024). Este sistema fue diseñado para orientar a las personas usuarias sobre el nivel de madurez requerido para utilizar una aplicación. Las clasificaciones son asignadas mediante un cuestionario que deben completar los equipos o empresas que desarrollan las aplicaciones en Play Console, y son procesadas por la Coalición Internacional de Clasificación por Edad (IARC). En función de estas respuestas, se asigna una clasificación del contenido avalada por las autoridades. Según Google, el objetivo es informar a las personas usuarias sobre contenido censurable como violencia, lenguaje obsceno o referencias sexuales, y restringir el acceso a ciertas apps en función de normativas locales o características demográficas. Sin embargo, su efectividad depende de la honestidad en las respuestas. Si bien IARC puede revisar clasificaciones inconsistentes, este proceso es reactivo: las aplicaciones permanecen disponibles hasta que se denuncien.

Tabla 3 Clasificación de contenido - Resultados

Clasificación de contenido	**Número de apps**	**%**
Apto para todo público	69	65.71
Adolescentes	29	27.62
Para mayores de 17 años	7	6.67

Del total analizado, la mayoría fue categorizada como "Apto para todo público", lo cual resulta alarmante considerando que muchas de estas aplicaciones son utilizadas para crear contenido sexual de mujeres. Dentro de esta categoría, se identificaron descripciones como "violencia leve", "fantasía" o "uso poco frecuente de lenguaje moderado", sin advertencias específicas sobre riesgos asociados a la creación de deepfakes.

Entre las apps que están dirigidas a adolescentes (13-17 años) se encontraron etiquetas como "Contenido diverso: se aconseja discreción", "Contenido sexual", "Temas provocativos", "Violencia leve", "Sangre" y "Desnudo parcial". Por último, las pocas apps clasificadas para mayores

de 17 años contenían menciones directas a "Desnudos", "Temas sexuales" y "Consumo de drogas".

4.2.5. Idioma

El idioma en que se presenta una aplicación refleja su orientación comercial o geográfica, y además condiciona su alcance y posibles riesgos asociados a su uso. En esta dimensión se identificaron patrones relevantes sobre las lenguas utilizadas en las apps analizadas.

Tabla 4 Idioma - Resultados

Idioma	**Número de apps**	**%**
Inglés	49	46.67
Español	36	34.29
Multilingüe	11	10.48
Inglés y español	9	8.56

El idioma predominante en las aplicaciones analizadas es el inglés, el cual refleja su enfoque hacia un público global, al ser el idioma más utilizado en el ámbito tecnológico y comercial. Al tratarse del idioma hegemónico en el desarrollo de software y en las plataformas digitales, muchas de estas aplicaciones priorizan el inglés para facilitar su expansión internacional.

No obstante, estas aplicaciones no se limitan a personas angloparlantes, ya que su diseño tiene interfaces intuitivas con botones íconos claros que eliminan la necesidad de un conocimiento avanzado del idioma. Esta decisión responde a estrategias comerciales, dado que la mayoría de estas aplicaciones incluyen versiones de pago y buscan maximizar su alcance sin invertir en traducciones o soporte multilingüe auténtico.

En segundo lugar, las aplicaciones están disponibles en español, siendo una estrategia para captar a usuarias y usuarios en regiones donde el acceso a herramientas tecnológicas está en constante expansión, como lo es ALAC. Sin embargo, esta disponibilidad en múltiples lenguas no debe confundirse con una verdadera inclusión lingüística, sino como una táctica para ampliar el mercado, incluyendo fines malintencionados y casos de abuso.

4.2.6. Imágenes de portada

El análisis de las imágenes de portada utilizadas en Google Play revela una clara tendencia a la hiperrepresentación de cuerpos de las mujeres como recurso visual predominante.

Tabla 5 Imágenes de portada - Resultados

Tipo de representación	**Número de apps**	**%**
Mayoría mujeres	42	40
Exclusivamente mujeres	30	28.57
Representación equilibrada entre géneros	32	30.48
Sin imagen de portada	1	0.95

La mayoría de las portadas incluyen imágenes de mujeres con una presencia masculina nula o mínima. Muchas imágenes representan mujeres estilizadas, posando o actuando bajo cánones estéticos comunes en redes sociales.

Ilustración I. Imágenes de portada de una de las apps evaluadas

Incluso en las aplicaciones que presentan una mezcla visual de género, se observa que las funcionalidades o etiquetas siguen estando dirigidas principalmente a usos que implican transformar rostros de mujeres. La portada suele funcionar como un primer enganche visual, construyendo una narrativa sobre los posibles usos de la app y su atractivo. Solo una aplicación del total analizado no muestra imágenes de portada, tratándose de una herramienta técnica especializada.

4.2.7. Modelo de negocio

El análisis de los modelos de negocio revela que la mayoría de las aplicaciones deepfake disponibles en Google Play Store están diseñadas

para maximizar la monetización, priorizando el acceso restringido a funcionalidades mediante esquemas de pago.

Tabla 6 Modelos de negocio - Resultados

Modelo de negocio	**Número de apps**	**%**
Pago	71	67.62
Freemium	19	18.10
Gratuito	15	14.29

La mayoría de las aplicaciones requieren un pago directo para acceder a sus funciones principales. A pesar de esta barrera económica, muchas de estas aplicaciones no exigen un pago inicial para probar las funciones de deepfake. Ofrecen pruebas gratuitas que permiten experimentar con sus capacidades básicas, restringiendo la exportación de los resultados hasta que se realice un pago. Este modelo de negocio, conocido como modelo de suscripción, incentiva la compra al generar interés en las funcionalidades avanzadas.

Otras aplicaciones emplean un modelo *freemium*, en el que las funciones básicas son gratuitas, pero se cobra por eliminar restricciones como marcas de agua o por desbloquear funcionalidades avanzadas. Este modelo combina accesibilidad inicial con estrategias de monetización escalonada, permitiendo que un público más amplio acceda a estas tecnologías.

Cabe destacar que, en todos los modelos, las restricciones económicas pueden ser fácilmente eludidas mediante capturas de pantalla, grabaciones de pantalla o la creación de múltiples cuentas para extender el acceso gratuito. En un contexto como el latinoamericano, es probable que muchos jóvenes eviten pagar por las funciones avanzadas, sin embargo, las versiones básicas o de prueba ya son suficiente para crear contenido dañino.

4.2.8. Esquema de precios

Para evaluar el costo de acceso a las funcionalidades de las aplicaciones deepfake que operan bajo modelos de pago, se recopilaron los precios observados durante las pruebas realizadas. Para facilitar la comparación, todos los valores fueron convertidos a dólares estadounidenses, dado que los precios suelen visualizarse en la moneda local del país desde el cual se accede a la aplicación.

Tabla 7 Esquema de precios - Resultados

Esquema de precios	**Rango de precios**
Suscripción semanal	$0.13 – $15.63
Suscripción mensual	$2.96 – $29.65
Suscripción anual	$20.21 – $103.77
Pago único	$29.65 – $94.34

Las suscripciones semanales representan un esquema particularmente preocupante porque su rango más bajo permite generar deepfakes en poco tiempo, convirtiéndose en una puerta de entrada accesible incluso para jóvenes y adolescentes. Por su parte, las suscripciones mensuales o anuales también ofrecen acceso extendido a funcionalidades avanzadas, y están dirigidas a usuarios frecuentes.

Las apps que tienen acceso ilimitado mediante pago único están orientadas a quienes prefieren evitar pagos recurrentes y acceder indefinidamente a las herramientas de deepfake. Además, algunas aplicaciones operan bajo un sistema de créditos, donde los costos se asocian a funcionalidades específicas, como "desbloquear imágenes" o "usar créditos de procesamiento", facilitando el acceso ocasional a funcionalidades avanzadas sin necesidad de una suscripción.

En conjunto, estos esquemas de precios muestran una estrategia de segmentación de mercado, que adapta los costos al perfil económico de cada usuario, reduciendo así las barreras de entrada.

4.2.9. Cantidad de descargas

Se observó también el nivel de difusión que han alcanzado estas aplicaciones deepfake. Para ello, se clasificaron en rangos según la cantidad de descargas reportadas en Google Play Store.

Tabla 8 Cantidad de descargas - Resultados

Cantidad de descargas	**Número de apps**	**%**
100 – 1000+	6	5.71%
5,000 – 50,000+	15	14.29%
100,000 – 1,000,000+	38	36.19%
Más de 1,000,000	21	20%

Más de 10 millones	9	8.57%
Más de 50 millones	2	1.90%
Sin datos (estimación baja)	14	13.33%

Del total analizado, la mayoría de las aplicaciones se encuentra en los rangos intermedios y altos de descarga. Esta métrica permite dimensionar su nivel de adopción y posible normalización en el entorno digital. La combinación entre su disponibilidad en tiendas oficiales, su facilidad de uso, y estrategias promocionales que resaltan su "simplicidad" contribuye a eliminar barreras técnicas, lo que multiplica su impacto social sin mecanismos de contención eficaces.

Particularmente preocupantes son las aplicaciones con millones de descargas que, a pesar de estar clasificadas como "aptas para todo público" o dirigidas a adolescentes, incluyen funcionalidades que pueden ser utilizadas para la creación de contenido sexual, planteando preguntas sobre la responsabilidad de plataformas como Google. Permitir que aplicaciones de este tipo alcancen tal nivel de visibilidad y aceptación evidencia una supervisión deficiente del contenido que se pone a disposición del público.

Por otro lado, las aplicaciones con menos de 10,000 descargas, como las de las categorías 500+ o 1,000+ no deben ser subestimadas, ya que son recientes (año 2024). Por lo que, al estar en etapas iniciales de adopción, pueden representar un nicho peligroso que crece rápidamente conforme más personas las descubren.

4.2.10. Puntuación

Las puntuaciones asignadas por personas usuarias reflejan una variedad de percepciones, centradas principalmente en la experiencia de uso.

Tabla 9 Puntuación - Resultados

Puntuación	**Número de apps**	**%**
Alto (4.0 – 5.0)	47	44.77%
Bajo (2.3 – 3.9)	10	9.52%
Sin puntuación visible	48	45.71%

Las aplicaciones con puntajes bajos podrían ser indicativas de una experiencia negativa, sin embargo, al analizar los comentarios, se observa

que no critican el contenido peligroso que generas los deepfakes, sino aspectos técnicos o económicos como la exportación de contenido, interfaces poco intuitivas y costos adicionales para acceder a funciones clave que inicialmente parecían incluidas. Las bajas calificaciones están más relacionadas con frustraciones de uso que con cuestionamientos críticos sobre la naturaleza de estas aplicaciones.

En contraste, las aplicaciones con puntajes altos indican una alta aceptación. Los comentarios positivos destacan su facilidad de uso, calidad de los resultados y funciones avanzadas, especialmente en las aplicaciones de pago. Por otro lado, las aplicaciones que no presentan calificaciones suelen contar con descargas recientes, lo que indica que están en fases iniciales de adopción y aún no han alcanzado suficiente visibilidad para acumular puntuaciones, pero es cuestión de tiempo para que obtengan mayor notoriedad y retroalimentación.

En conjunto, estos datos muestran un panorama mixto: mientras que una parte de usuarios señala fallas técnicas y costos como limitantes, una gran proporción valida y normaliza su uso sin cuestionar los riesgos, dejando en evidencia la falta de conciencia sobre su impacto.

4.2.11. Funcionalidades

El análisis de las funcionalidades de las 105 aplicaciones deepfake evaluadas, basado en sus descripciones en Google Play y pruebas técnicas, evidenció cómo estas herramientas suelen ocultar su potencial para usos cuestionables bajo un discurso de creatividad y entretenimiento.

La mayoría ofrece funciones como intercambio de rostros (face-swap), mapeo de expresiones faciales y sincronización de labios, logrando resultados realistas. Por ejemplo, permiten reemplazar rostros con imágenes de celebridades, figuras públicas o personas desconocidas, sin requerir su autorización. También se identificaron funcionalidades como la creación de videos animados a partir de fotos estáticas, generación de clips con "personas digitales" que cantan o bailan, y conversión de texto a video. Una tendencia preocupante identificada en varias aplicaciones es la simulación de interacciones humanas, como abrazos, besos, bailes e interacciones íntimas entre dos personas.

Adicionalmente, muchas aplicaciones permiten modificar características faciales, como intercambio de género, envejecimiento o rejuvenecimiento de rostros. También incluyen plantillas para videos y

fotos que abarcan desde temas culturales hasta escenarios de moda, entretenimiento y celebridades, diseñadas para simplificar el uso de las herramientas, haciéndolas accesibles para usuarios con poca experiencia técnica.

4.2.12. Facilidad de uso

Como se abordó en el apartado sobre metodologías de evaluación en aplicaciones móviles, la facilidad de uso es un factor determinante para la accesibilidad e impacto de cualquier tecnología. En el caso de las aplicaciones deepfake, esta dimensión resulta clave para entender su rápida adopción y masificación.

Para evaluar esta dimensión en las 105 aplicaciones analizadas, se diseñó un instrumento, que consiste en una rúbrica con tres categorías, que evalúa la simplicidad del proceso para crear deepfakes.

Tabla 10 Dimensión "Facilidad de uso": Categorías para evaluar la facilidad de uso de aplicaciones deepfake

Categoría	**Criterio de evaluación**
Navegación sencilla	¿La interfaz es intuitiva? (Sí/No)
Ingesta de datos	¿Es fácil cargar imágenes o videos en la aplicación? (Sí/No)
Generación de contenido	¿Es simple el proceso de generación de deepfake? (Sí/No)

Los resultados revelaron que más de la mitad de las aplicaciones fueron calificadas como "fáciles de usar", al cumplir satisfactoriamente con las tres categorías. Estas aplicaciones eliminan barreras técnicas, haciéndolas accesibles incluso para personas sin experiencia avanzada. Por ejemplo, algunas aplicaciones que están en inglés cuentan tutoriales integrados, señalizaciones como "ingrese aquí" o botones destacados para iniciar procesos, evidenciando un diseño orientado a monetizar.

Tabla 11 Facilidad de uso - Resultados

Facilidad de uso	**Número de apps**	**%**
Fácil	57	54.29%
Parcialmente fácil	44	41.90%
No evaluable	3	2.86%
Difícil	1	0.95%

Las aplicaciones clasificadas como parcialmente fáciles obtuvieron resultados positivos en las categorías de navegación e ingesta de datos, pero presentaron una limitación en la generación de contenido, ya que esta etapa requiere un pago para desbloquear la funcionalidad. Esta accesibilidad puede incentivar al pago, especialmente en usuarios interesados en experimentar con las herramientas, aunque sea temporalmente.

En muy pocos casos, las aplicaciones no pudieron ser completamente evaluadas ya que, si bien su navegación era sencilla, tanto la ingesta de datos como la generación de contenido estaban bloqueadas tras un muro de pago. A pesar de ello, estas aplicaciones siguen atrayendo a usuarios por las expectativas creadas en su promoción. Finalmente, solo una aplicación fue calificada como difícil de usar debido a su interfaz técnica y poco intuitiva, que complicó el acceso a las funciones.

4.2.13. Representa un peligro para las mujeres

La evaluación de las aplicaciones deepfake reveló una alarmante realidad sobre sus riesgos, especialmente para la seguridad de las mujeres en el ciberespacio. Los resultados obtenidos se clasificaron en tres categorías.

Tabla 12 Dimensión "Representa un peligro para las mujeres": Categorías para evaluar si las aplicaciones deepfake representan un peligro para las mujeres

Categoría	**Criterio de evaluación**
Sí es peligroso	¿La aplicación normaliza la cosificación, perpetúa estereotipos de género y/o es potencialmente explotada para generar contenido sexual de los cuerpos de las mujeres? (Sí/No)
No es peligroso	¿La aplicación no presenta contenido abusivo o sexualizado, limitándose a plantillas o animaciones profesionales? (Sí/No)
No se sabe	¿Las funcionalidades están bloqueadas tras un pago, impidiendo verificar si contienen características peligrosas? (Sí/No)

Los resultados fueron contundentes: la mayoría de las aplicaciones analizadas fueron clasificadas como peligrosas para las mujeres.

Tabla 13 Representa un peligro para las mujeres - Resultados

Nivel de riesgo	**Número de apps**	**%**
Representa un peligro	94	89.52%
No representa un peligro	5	4.76%
No evaluable	6	5.71%

Esta categoría incluye herramientas cuyas funcionalidades permiten o promueven la cosificación de los cuerpos femeninos, la reproducción de estereotipos sexistas, o la generación de contenidos sexualizados no consensuados. Este proceso comienza con la carga de una imagen de un rostro, seguido de la selección de una plantilla proporcionada por la aplicación o la carga de un segundo archivo que contiene el cuerpo deseado. Las aplicaciones procesan ambas imágenes utilizando algoritmos GAN para mapear el rostro cargado y adaptarlo al cuerpo o escena seleccionada, ajustando detalles como expresiones faciales, movimientos, proporciones y condiciones de iluminación. El resultado se genera en segundos o minutos, produciendo imágenes o videos realistas listos para descargar o compartir.

Besos y abrazos

Entre las funciones más peligrosas se encuentran aquellas que simulan besos, abrazos o situaciones íntimas, permitiendo cargar fotografías de dos personas. Estas funciones, ampliamente promocionadas en los anuncios de las aplicaciones, suelen mostrar representaciones forzadas, casi siempre protagonizadas por un hombre que utiliza una foto propia junto con la imagen de una mujer.

Plantillas

Muchas aplicaciones incluyen plantillas explícitamente diseñadas para sexualizar a las mujeres, mostrando cuerpos en bikini o atributos corporales exagerados.

Categorías como *Caliente*, *Hot Bikini*, *Latex*, *Sexy Girl*, *Pink for fox underwear*, *Exquisite Girl*, *Dominant*, *Cherry*, *Devil*, *Flirty*, *Bunny Girl*, *Chicas Moto*, *Cuerpo de Playa*, *Angels of Victoria* (en alusión a modelos de lencería), *Fatal Attraction*, *Beautiful Women* evidencian un diseño orientado a la erotización de la mujer. Otras categorías como *Luxury*, *Cosplayers*, *Streamers*, *Christmas* y *Halloween* camuflan su contenido sexualizado bajo temáticas generales. Las categorías muestran una marcada disparidad de género, ya que mientras los hombres aparecen vestidos completamente, las mujeres lo hacen con escotes, lencería o disfraces sexualizados. Por ejemplo, en *Christmas*, las mujeres aparecen con escotes, mientras que los hombres son mostrados con ropa de invierno, cubiertos completamente.

Un ejemplo particularmente preocupante es la categoría *Body Latino*, que refuerza estereotipos fetichistas sobre las mujeres latinas,

presentándolas en trajes ajustados y sexualizados. Otras plantillas, como *Anime Girl*, *Pink for Fox Underwear*, y *Devil* también se apropian de estéticas culturales para sexualizar aún más las representaciones femeninas.

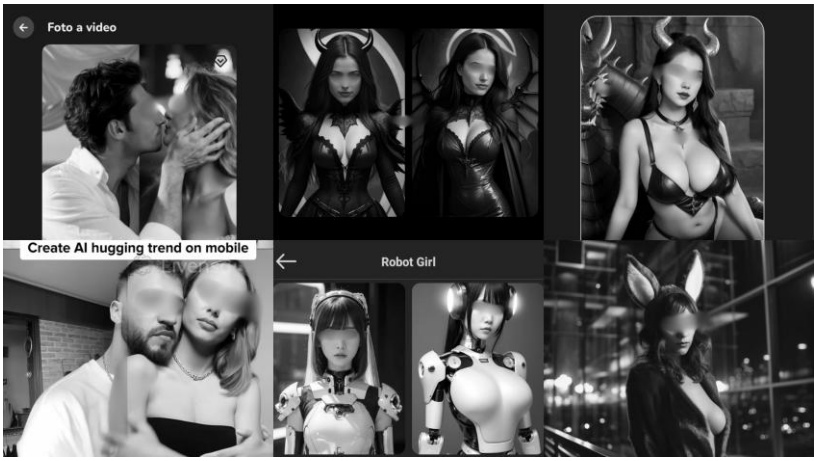

Ilustración II. Capturas de las apps analizadas

Generación por texto

Algunas aplicaciones permiten cambiar la vestimenta mediante texto. En un caso concreto, al escribir *blue bikini*, una aplicación transformó la ropa original de la imagen en un bikini azul, alterando también las proporciones corporales para aumentar los senos. Otras aplicaciones, por su parte, generan imágenes a partir de palabras ingresadas, por ejemplo, al escribir términos como *sexy*, producen representaciones de mujeres a menudo con poca ropa, poses y atributos corporales exagerados. En esa misma línea, otra funcionalidad preocupante es la animación de fotos estáticas para "hablar" en sincronía con el texto ingresado. Esto permite crear videos donde la imagen de una mujer puede ser forzada a decir frases humillantes, violentas o sexualmente explícitas.

Casos preocupantes

Entre los casos alarmantes identificados, están funciones como *Crea Videos Calientes*, que genera videos donde las mujeres aparecen con poca ropa o en situaciones que refuerzan su cosificación. Otra aplicación crea un *Compañero IA* personalizado, permitiendo al usuario cargar una imagen y elegir características altamente sexualizadas para interactuar con el deepfake generado. Bajo el pretexto de ofrecer experiencias personalizadas, la aplicación solicita información al usuario mediante una

serie de preguntas, entre ellas temas de carácter sexual. Uno de los pasos iniciales consiste en elegir la apariencia/cuerpo del *Compañero IA*, donde las opciones incluyen plantillas de mujeres sexualizadas. En la última etapa del proceso, la aplicación plantea preguntas como: *"¿Está bien si me convierto en algo más que un amigo y envío mensajes personales?"*. La *Compañía IA* menciona su edad predeterminada de 18 años y aparece un chat.

Al conversar con el deepfake generado, este envía mensajes y audios con contenido sexual. De manera preocupante, la aplicación intenta persuadir al usuario a adquirir la versión paga enviando imágenes explícitas de mujeres desnudas, en donde se muestran sus genitales. Además, la personalización permite elegir características como *tímida*, *coqueta*, *amistosa* o *misteriosa*.

Evasión de responsabilidad

Muchas aplicaciones deslindan su responsabilidad mediante cláusulas legales que las personas deben aceptar si quieren empezar a usarlas. Estos avisos prohíben el uso de material no autorizado, pero transfieren toda la responsabilidad a la persona usuaria, mientras siguen promoviendo este tipo de armas digitales. Por ejemplo, aseguran que las fotos y videos cargados serán eliminados de sus servidores tras su procesamiento, pero permiten su exportación, facilitando su explotación a lo largo del tiempo.

Estas cláusulas incluyen declaraciones como *"no ofrecemos garantías respecto a la precisión, integridad o funcionalidad del contenido generado"*, y que *"los servicios se basan en fuentes de información permitidas por leyes y regulaciones"*. Aunque afirman que aplican filtros manuales y automáticos, admiten que estos no son infalibles y, en caso de fallas, delegan la responsabilidad a las personas afectadas de reportarlas mediante un correo electrónico.

Muchas aplicaciones incluyen cláusulas legales en las que se indica que el contenido generado es responsabilidad exclusiva de las personas usuarias. Un caso preocupante es el aviso que menciona explícitamente: *"Asegúrate de que las fotos que uses estén autorizadas por las personas en la imagen. Usar fotos no autorizadas que infrinjan los derechos de imagen de alguien está estrictamente prohibido y los usuarios asumirán la responsabilidad legal"*.

Funcionalidades menos peligrosas

En la categoría "No representa un peligro" se encuentran aplicaciones que no presentan contenido abusivo, limitándose a plantillas profesionales o

animaciones no sexualizadas. Aunque implementan sistemas para bloquear contenido inapropiado, estas herramientas son minoría en el análisis, y sus restricciones, muchas de las cuales están bloqueadas tras un modelo de pago, no garantizan la eliminación total de riesgos. Finalmente, seis aplicaciones no fueron evaluables debido a que funcionalidades centrales, como la ingesta de datos o la generación de contenido, estaban bloqueadas tras un pago. Esto genera incertidumbre, ya que no se puede descartar que contengan características peligrosas similares a otras herramientas evaluadas.

5. Discusiones

5.1. Violencia estructural en el diseño tecnológico

Los hallazgos revelan que el ecosistema de aplicaciones deepfake profundiza estructuras de desigualdad ya existentes. La ausencia de desarrollos originados en ALAC, así como la hegemonía de empresas estadounidenses y turcas, esta última con alarmantes índices de violencia de género (TIKFD, 2023), pone en evidencia una geopolítica del diseño tecnológico donde las decisiones que afectan a millones de personas usuarias se toman desde contextos socioculturales ajenos. Esta distancia no es neutra, como advierte Sandra Harding (1991), la ciencia y la tecnología que excluye a grupos sociales produce sesgos que refuerzan su marginación. Para Harding, iniciar el pensamiento desde las vidas de las personas más marginadas dentro de la comunidad científica permite una comprensión más completa y menos distorsionada de la realidad natural y social.

En este caso, la ausencia de equipos de desarrollo diversos y sensibles al contexto refuerza un modelo extractivista de datos y cuerpos. Como ha mostrado Judy Wajcman (2004), los hombres, particularmente del norte global, han dominado históricamente los procesos de innovación tecnológica, lo que ha excluido experiencias, saberes y necesidades de las mujeres. Por lo tanto, esta exclusión no se debe únicamente a la falta de acceso o habilidades, sino a una cultura técnica profundamente masculinizada, que impone barreras a la participación femenina en el diseño tecnológico. Por ello, las decisiones sobre qué se diseña, para quién y con qué fines, se ven condicionadas por estructuras de género que rara vez se cuestionan.

Por otro lado, la interfaz amigable, el acceso gratuito o freemium, y la abundancia de funciones visuales no deben leerse como sinónimos de

"democratización tecnológica", como argumentan algunas de estas empresas, sino como parte de una infraestructura técnica cuyo foco es la expansión comercial sobre cualquier principio ético. La instrumentalización de conceptos como "creatividad", "empoderamiento" o "contenido viral" en sus descripciones revela una narrativa que oculta los riesgos mediante un lenguaje optimista, mientras se desatiende cualquier advertencia.

5.2. Cosificación algorítmica y violencia contra las mujeres

La reiterada presencia de imágenes de mujeres, mayormente sexualizadas o estilizadas bajo cánones de belleza normativos, tanto en las portadas como en las plantillas prediseñadas, constituye una prolongación digital de la lógica patriarcal que trata los cuerpos de las mujeres como bienes disponibles para el deseo ajeno. Esto representa una forma estructural de violencia, en la que la cosificación reduce a la mujer a objeto sexual y elimina su agencia al servicio del placer masculino (MacKinnon 1987).

Para Rita Segato (2016) la violencia sexual no es una anomalía de un sujeto solitario, es un mensaje de poder y apropiación pronunciado en sociedad. Desde su enfoque, los cuerpos de las mujeres se convierten en soportes simbólicos de ese mensaje. Aplicado al caso de las deepfakes sexuales, estas tecnologías no solo afectan a una víctima concreta, sino que perpetúan un orden patriarcal donde los cuerpos de las mujeres pueden ser manipulados, distribuidos y expuestos sin consentimiento. La estética digital se convierte en lo que Segato llama una "pedagogía de la crueldad", es decir, una cultura visual que enseña a normalizar la violencia y la cosificación como parte de lo aceptable.

Judith Butler (1993) aporta aquí un giro fundamental al plantear que los cuerpos no existen como entidades previas a su inscripción social, sino que son "performados" en y por el discurso. Las funciones de las apps deepfake como "hacer que tu cara baile" o "crear videos irresistibles", operan como tecnologías de la performatividad que fabrican cuerpos disponibles y sexuales.

En este marco, la "aparición" del cuerpo de las mujeres en estas plataformas no es algo inesperado, sino una consecuencia previsible de lógicas que promueven la disponibilidad visual y afectiva de ciertos cuerpos para el deseo ajeno. En términos de la propia Butler (2009), muchas de estas representaciones configuran "vidas no lloradas" (ungrievable lives), es decir, vidas cuyo daño o humillación no activa duelo

ni reparación social, porque ya fueron deshumanizadas simbólicamente incluso antes de ser violentadas tecnológicamente.

5.3. Injusticia epistémica y consentimiento opaco

Los resultados muestran que la mayoría de las aplicaciones evita ofrecer información clara sobre los riesgos de uso, limitándose a deslindes legales enterrados en cláusulas complejas, muchas veces redactadas exclusivamente en inglés. Esta barrera lingüística no es menor, pero además configura una forma de *injusticia hermenéutica*, en los términos de Miranda Fricker (2007), que ocurre cuando las estructuras sociales no han producido aún los conceptos adecuados para nombrar ciertas experiencias. Las víctimas, entonces no pueden comprender plenamente lo que les sucede ni hacerse entender ante otros, lo cual profundiza su desprotección y aislamiento.

Este escenario se agrava en contextos como ALAC, donde la alfabetización digital es desigual, y donde el acceso a mecanismos de reparación o denuncia por violencia digital es limitado. Esta injusticia no solo es lingüística, sino también histórica y geopolítica. Desde la perspectiva de María Lugones (2008), la colonialidad del saber implica una jerarquización epistémica que invisibiliza y subordina las formas de conocimiento de los pueblos colonizados, en particular aquellas vinculadas a cuerpos de mujeres racializadas y empobrecidas. En ese sentido, la elección excluyente de idiomas, la ausencia de advertencias y la falsa apariencia de neutralidad son mecanismos de control epistémico que perpetúan violencias estructurales.

5.4. Ética del diseño y evasión de responsabilidad

En el centro del problema ético de estas aplicaciones se encuentra la responsabilidad de quienes las diseñan, no solo de quienes las usan. Aunque muchas apps prohíben el uso no consensuado de imágenes, sus propias funcionalidades como "interacción íntima simulada" o "rostros en videos provocativos" están diseñadas precisamente para ese fin. Al colocar la carga moral exclusivamente sobre la persona usuaria, las empresas evaden su responsabilidad ética como diseñadoras de tecnología con impactos previsibles. Esta evasión es una elección política, ya que constituye una forma de negligencia moral que permite que el lucro se construya sobre la exposición al daño.

La inteligencia artificial no puede razonar moralmente, solo imita decisiones que tienen consecuencias éticas (Arriagada, 2024). Por eso, el diseño importa. Cuando los equipos de desarrollo no se preguntan qué concepción de justicia están operando, o cómo sus decisiones técnicas afectan diferencialmente a mujeres, adolescentes y minorías, están perpetuando modelos algorítmicos de violencia.

Desde la ética dialógica, Adela Cortina (2006) sostiene que una tecnología que afecta negativamente a un grupo sin su participación ni posibilidad real de rechazar su funcionamiento es éticamente ilegítima. Si las mujeres representadas no pueden decir "sí" racionalmente al uso de su imagen, esa práctica no se sostiene. Incluso si existiera un consentimiento formal, no puede considerarse éticamente válido si transgrede mínimos morales universales como el respeto a la dignidad. Aplicaciones que humillan, objetualizan o exponen a las personas sin advertencias reales, aunque haya "términos de uso", infringen con ese principio.

5.5. Normalización algorítmica del daño

El modelo de negocio freemium, los esquemas de precios accesibles, y la masividad de descargas revelan una aceptación social progresiva de herramientas que permiten la producción de contenidos no consensuados, muchas veces sexuales o violentos. Esta masificación no puede desvincularse de una economía de la conectividad que premia lo viral, lo visualmente impactante, lo replicable. Así, el número de descargas legitima estas prácticas como aceptables, invisibilizando sus impactos dañinos.

La existencia de apps que permiten simular rostros de mujeres en escenas sexuales no puede analizarse solo desde la crítica a la privacidad o al uso indebido de la imagen, sino además como parte de una infraestructura patriarcal digital donde la tecnología reproduce y refuerza la cosificación.

Desde una ética del cuidado y la responsabilidad colectiva, esta lógica es insostenible. La facilidad de uso, aunque en principio parece inclusiva, se convierte en un vector de riesgo cuando no se acompaña de mecanismos de advertencia o control. Al permitir que adolescentes sin conciencia crítica accedan fácilmente a estas apps, se está promoviendo la trivialización del consentimiento, el control sobre los cuerpos ajenos y la desensibilización ante la violencia digital.

6. Conclusiones

Esta investigación demuestra que las aplicaciones deepfake no son meras herramientas técnicas, sino expresiones concretas de estructuras de poder que, lejos de ser neutras, refuerzan la violencia digital de género. Su diseño, modelo de negocio y difusión están orientados a maximizar la circulación de imágenes manipuladas, muchas de ellas sexualizadas, sin garantizar mecanismos de consentimiento ni protección real para quienes pueden ser afectadas.

En contextos como ALAC, donde las mujeres ya enfrentan niveles alarmantes de violencia estructural, estas tecnologías reproducen el daño bajo el discurso del entretenimiento o la innovación. El acceso fácil, la ausencia de advertencias y la evasión sistemática de responsabilidad por parte de quienes diseñan y distribuyen estas apps constituyen formas de negligencia que deben ser denunciadas.

Plataformas como Google Play legitiman este ecosistema, permitiendo la circulación masiva de tecnologías que posibilitan agresiones simbólicas y sexuales sin consentimiento, bajo esquemas comerciales lucrativos. Esta permisividad revela cómo el beneficio económico se antepone a principios como la dignidad, autonomía, privacidad y protección de datos. Responsabilizar únicamente a las personas usuarias es insuficiente. Se requiere cuestionar el sistema técnico, económico y normativo que habilita estas violencias. Esto implica avanzar hacia políticas públicas con enfoque feminista y prácticas de diseño que reconozcan que toda tecnología tiene implicancias morales y políticas.

Esta investigación busca abrir un espacio para la reflexión crítica sobre la relación entre tecnología y violencia de género. Al hacerlo, invita a seguir investigando y construyendo alternativas para un desarrollo ético de la inteligencia artificial, que proteja los derechos de todas las personas.

Referencias

Albahar, M, y Almalki, J. (2019). Deepfakes: Threats and Countermeasures Systematic Review. *Journal of Theoretical and Applied Information Technology, 97*(22), 3242-3250. http://www.jatit.org/volumes/Vol97No22/7Vol97No22.pdf.

Ahmad, M. (2023). *Analysis of cross-platform mobile application development frameworks*. Tesis de Bachiller. Riga Technical University.

Altuncu, E., Franqueira, V., & Li, S. (2022). Deepfake: Definitions, Performance Metrics and Standards, Datasets and Benchmarks,

and a Meta-Review. *Frontiers in Big Data,* 1-31. https://doi.org/10.48550/arXiv.2208.10913.

Arriagada, G. (2024). Los sesgos del algoritmo. *Editorial Pollera.*

Aydin, G., y Silahtaroglu, G. (2021). Insights into mobile health application market via a content analysis of marketplace data with machine learning. *PLoS One*, 16(1), 1-22. https://doi.org/10.1371/journal.pone.0244302.

Butler, J. (1993). *Bodies That Matter: On the Discursive Limits of "Sex"*. Routledge.

_____ (2009). *Frames of War: When Is Life Grievable?*. Verso.

Cerdán Martínez V., y Padilla Castillo G. (2019). Historia del "fake" audiovisual: "deepfake" y la mujer en un imaginario falsificado y perverso. *Historia y Comunicación Social, 24*(2), 505-520. https://doi.org/10.5209/hics.66293.

Chen, Y., Xia, S., Zhao, J., Jian, M., Zhou, Y., Niu, Q., Yao, R., y Zhu, D. (2020). Person image synthesis through siamese generative adversarial network. *Neurocomputing,* 490-500. https://doi.org/10.1016/j.neucom.2020.09.004.

Chesney, R., y Keats Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *107 California Law Review 1753*, 1753-1773.

Citron, D., y Chesney, B. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review,* 1753-1820. https://doi.org/10.15779/Z38RV0D15J.

Cole, S. (2019a). This Horrifying App Undresses a Photo of Any Woman With a Single Click. *Vice*. https://www.vice.com/en/article/kzm59x/deepnude-app-creates-fake-nudes-of-any-woman.

_____ (2019b). Creator of DeepNude, App That Undresses Photos of Women, Takes It Offline. *Vice*. https://www.vice.com/en/article/qv7agw/deepnude-app-that-undresses-photos-of-women-takes-it-offline.

Comisión Económica para América Latina y el Caribe (CEPAL). (2023). *La igualdad de género y la autonomía de las mujeres y las niñas en la era digital: aportes de la educación y la trans-formación digital en América Latina y el Caribe*. Santiago, Chile.

Cortina, A. (2006). *Ética pública: Los derechos fundamentales como ética mínima*. Editorial Tecnos.

Dawson, R., Felder, T., Donevant, S., McDonnell, K., Card, E., King, C., y Heiney, S. (2019). What makes a good health "app"? Identifying the strengths and limitations of existing mobile application

evaluation tools. *Nursing Inquiry*. https://doi.org/10.1111/nin.12333.

Dewi, R., Priandani, N., Brata, K., y Fanani, L. (2018). Usability Evaluation of Mobile-Based Application for Javanese Script Learning Media. *Journal of Information Technology and Computer Science, 3*(1), 88–93. https://doi.org/10.25126/jitecs.20183146.

Dini, G., Martinelli, F., Matteucci, I., Petrocchi, M., Saracino, A., y Sgandurra, D. (2012). A Multi-criteria-Based Evaluation of Android Applications. *Lecture Notes in Computer Science,* 67–82. https://doi.org/10.1007/978-3-642-35371-0_7.

Farid, H., y Schindler, H. (2020). *Deep Fakes. On the Threat of Deep Fakes*. https://tohear.info/pdf/CEP-KAS_Deep%20Fakes_062920.pdf.

Fasano, F., Martinelli, F., Mercaldo, F., y Santone, A. (2019). Investigating mobile applications quality in official and third-party marketplaces. *Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2019),* 169–178. https://doi.org/10.5220/0007757601690178.

Frid, G., Bogaert, K., y Chen, K. (2021). Mobile health apps for pregnant women: Systematic search, evaluation, and analysis of features. *Journal of Medical Internet Research, 23*(10). https://doi.org/10.2196/25667.

Fridman, L. [Lex Friedman] (2019). *Ian Goodfellow: GANs and Deep Learning | AI Podcast #23* [Video]. YouTube. https://www.youtube.com/watch?v=Z6rxFNMGdn0.

Giles, M. (2018). *The GANfather: The man who's given machines the gift of imagination*. MIT Technology Review. https://www.technologyreview.com/2018/02/21/145289/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/.

González-Véliz, C., y de Andrés, S. (2023). Corrientes del ciberfeminismo y transición digital feminista en América Latina y el Caribe: hacia un futuro digital más equitativo. *Revista Punto Género,* (20), 31-61. https://doi.org/10.5354/2735-7473.2023.73459.

González-Véliz, C., y Cuzcano-Chavez, X. (2024). Desafíos y dimensiones de la desinformación en ALAC: deepfakes y la urgencia de proteger los derechos de las mujeres. *Espacio I+D, Innovación más Desarrollo, 13*(36), 162-175. https://doi.org/10.31644/IMASD.36.2024.a19.

Google (2024). *Política de contenido para desarrolladores*. https://support.google.com/googleplay/answer/6209544.

Harding, S. (1991). *Whose Science? Whose Knowledge? Thinking From Women's Lives*. Cornell University Press.

Hare, S. (2022). *Technology is not neutral: A short guide to technology ethics*. London Publishing Partnership.

Hashim, N., y Isse, A. (2019). Usability evaluation metrics of tourism mobile applications. *Journal of Software Engineering and Applications, 12*(7), 267–277. https://doi.org/10.4236/jsea.2019.127016.

Heidari, A., Jafari Navimipour, N., Dag, H., y Unal, M. (2023). Deepfake detection using deep learning methods: A systematic and comprehensive review. *WIREs Data Mining and Knowledge Discovery, 14*(2), 1-45. https://doi.org/10.1002/widm.1520.

Hensher, M., Cooper, P., Dona, Sithara Wanni Arachchige, Angeles, M., Nguyen, D., Heynsbergh, N., Chatterton, M., y Peeters, A. (2021). Scoping review: Development and assessment of evaluation frameworks of mobile health apps for recommendations to consumers. *Journal of the American Medical Informatics Association, 28*(6), 1318–1329. https://doi.org/10.1093/jamia/ocab041.

Hussain, A., Kutar, M., Abdul M., Arifin, y Md Kamal, F. (2012). Modeling subjective metrics for mobile evaluation. *Journal of Information Systems Research and Innovation, 10*(1), 11–20. http://repo.uum.edu.my/id/eprint/9706/.

Hussain, A., Saleh, A., Taher, A., Ahmed, I., y Lammasha, M. (2015). Usability evaluation method for mobile learning application using Agile: A systematic review. *Jurnal Teknologi (Sciences & Engineering), 77*(5), 51–56. https://doi.org/10.11113/jt.v77.6116.

Khan, S., y Dang-Nguyen, D. (2023). Deepfake Detection: A Comparative Analysis. 1-28. https://dx.doi.org/10.48550/arXiv.2308.03471.

Lacort, J. (3 de marzo de 2024). El modelo de Singapur: así está preparando a su ciudadanía para la inteligencia artificial. *Xataka*. https://www.xataka.com/robotica-e-ia/modelo-singapur-asi-esta-preparando-a-su-ciudadania-para-inteligencia-artificial.

Lugones, M. (2008). Colonialidad y Género. *Tabula Rasa,* 73–101. https://www.revistatabularasa.org/numero-9/05lugones.pdf.

MacKinnon, C. (1987). *Feminism Unmodified: Discourses on Life and Law*. Harvard University Press.

Masood, M., Nawaz, M., Mahmood M., Khalid, J., Ali, e Irtaza, A. (2021). Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. https://arxiv.org/pdf/2103.00484.

Molina Sanhueza, J. (2024). *Escándalo en el Saint George: alumnos de colegio élite crearon imágenes de compañeras desnudas usando IA y las viralizaron*.

Interferencia. https://interferencia.cl/articulos/escandalo-en-el-saint-george-alumnos-de-colegio-elite-crearon-imagenes-de-companeras.

Mubarak, R., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., y Parkinson, S. (2023). A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats. *IEEE Access,* 144497-144529. https://doi.org/10.1109/ACCESS.2023.3344653.

Noble, S. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

Organización de los Estados Americanos (OEA). (2021a). Ciberviolencia y ciberacoso contra las mujeres y las niñas en el marco de la convención Belém do Pará.

Organización de los Estados Americanos (OEA). (2021b). La violencia de género en línea contra las mujeres en línea.

Patel, N., y Dalal, P. (2016). Analysis of usability metrics for mobile applications. *VNSGU Journal of Science and Technology, 5*(1), 28-52.

Pei, G., Zhang, J., Hu, M., Zhang, Z., Wang, C., Wu, Y., Zhai, G., Yang, J., Shen, C., y Tao, D. (2024). Deepfake Generation and Detection: A Benchmark and Survey. *ArXiv,* 1-28. https://doi.org/10.48550/arXiv.2403.17881.

Petrova, N. D., y Zonova, M. V. (2022). Deepfake Technology in Marketing. *Escuela de Minera de los Ural – para las Regiones,* 593-594. https://www.elibrary.ru/item.asp?id=49378663.

Rahman, A., Islam, M., Moon, M., Tasnim, T., Siddique, N., Shahiduzzaman, Md., y Ahmed, S. (2022). A Qualitative Survey on Deep Learning Based Deep fake Video Creation and Detection Method. *Australian Journal of Engineering and Innovative Technology,* *4*(1), 13-26. https://doi.org/10.34104/ajeit.022.013026.

Rocha Álvarez, D. (2022). Filosofía, tecnología y educación. La lectura platónica de Neil Postman. *Revista Española de Pedagogía, 35*, 237-258. https://doi.org/10.51743/cpe.339.

Rodríguez, A. (13 de octubre de 2023). Acusado un universitario de alterar con inteligencia artificial miles de imágenes de alumnas para venderlas como pornografía. *El País*. https://elpais.com/mexico/2023-10-14/acusado-un-universitario-de-alterar-con-inteligencia-artificial-miles-de-imagenes-de-alumnas-para-venderlas-como-pornografia.html.

Rodríguez, H. (2 de noviembre 2024). Turquía se convierte en el epicentro de la era de la IA móvil en el MBBF 2024. *La ecuación*

digital. https://www.laecuaciondigital.com/empresas/eventos/turquia-se-convierte-en-el-epicentro-de-la-era-de-la-ia-movil-en-el-mbbf-2024/.

Rojas Berríos, M. (19 de agosto de 2023). Chorrillos: Escolares que alteraron fotos de compañeras con IA y las comercializaron no fueron expulsados. *Infobae*. https://www.infobae.com/peru/2023/08/29/chorrillos-escolares-que-alteraron-fotos-de-sus-companeras-con-ia-para-venderlas-no-fueron-expulsados/.

Sencar, H., Verdoliva, L., y Memon, N. (2022). Multimedia Forensics. *Advances in Computer Vision and Pattern Recognition*. https://doi.org/10.1007/978-981-16-7621-5.

Security Heroes (2023). *State of Deepfakes*. https://www.securityhero.io/state-of-deepfakes/.

Segato, R. (2016). *La guerra contra las mujeres*. Traficantes de Sueños.

Sensity AI (2019). *Reports*. https://sensity.ai/reports/.

Seow, J., Lim, M., Phan, R., y Liu, J. (2022). A comprehensive overview of Deepfake: Generation, detection, datasets, and opportunities. *Neurocomputing,* 351-371. https://doi.org/10.1016/j.neucom.2022.09.135.

Shyika, A., y Kyiv, U. (2022). DEEPFAKE TECHNOLOGY AS AN ENGINE FOR THE DEVELOPMENT OF THE MARKETING INDUSTRY. *V All-Ukrainian Scientific and Practical Student Conference*, 336-338.

Sontakke, N., Utekar, S., Rastogi, S., y Sonawane, S. (2023). Comparative Analysis of Deep-Fake Algorithms. *ArXiv*. https://doi.org/10.48550/arXiv.2309.03295.

StatCounter (2024). *Mobile operating system market share in South America*. https://gs.statcounter.com/os-market-share/mobile/south-america.

Melo, M. (3 de julio de 2024). Sistema operativo móvil con la mayor cuota de mercado por país. *Statista*. https://es.statista.com/grafico/29620/sistema-operativo-movil-con-la-mayor-cuota-de-mercado-por-pais/.

Stevens, D. (2020). *Regulating Deepfake Technology: Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography*. Tesis de Máster. Tilburg Law School.

The Batch (30 de septiembre de 2020). *How Ian Goodfellow invented GANs*. https://www.deeplearning.ai/the-batch/ian-goodfellow-a-man-a-plan-a-gan/.

Tripathi, S. (2019). Women and online harassment. *Feminist Dissent,* (6), 133-158. https://doi.org/10.31273/fd.n6.2022.1265.

Turkish Federation of Women's Associations (TKDF) y United Nations Population Fund (UNFPA). (2023). *Domestic violence report 2023*. https://turkiye.unfpa.org/en/tkdf-domestic-violence-report-2023.

Wajcman, J. (2004). *TechnoFeminism*. Polity Press.

Yadav, D., y Salmani, S. (2019). Deepfake: A Survey on Facial Forgery Technique Using Generative Adversarial Network. *2019 International Conference on Intelligent Computing and Control Systems (ICCS),* 852-857. https://doi.org/10.1109/iccs45141.2019.9065881.

Zhu, J., Park, T., Isola, P., y Efros, A. (2017). Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks. *2017 IEEE International Conference on Computer Vision (ICCV),* 2242-2251. https://doi.org/10.1109/iccv.2017.244.