

DEEPPAKES Y LIBERTAD DE EXPRESIÓN: DILEMAS ÉTICOS Y JURÍDICOS EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

DEEPPAKES AND FREEDOM OF EXPRESSION: ETHICAL AND LEGAL DILEMMAS IN THE AGE OF ARTIFICIAL INTELLIGENCE

Jorge Dragonetti y Valentina Araya¹

(Fecha de recepción: 26/09/25 - Fecha de aceptación: 05/11/25)

RESUMEN

La expansión de los *deepfakes* como producto de la inteligencia artificial plantea dilemas sin precedentes en el cruce entre tecnología, ética y derecho. Estas representaciones hiperrealistas, capaces de alterar rostros, voces y escenas, desafían los límites de la percepción humana y socavan la confianza en los medios, las instituciones y el debate público. Su utilización, tanto para fines legítimos —educación, entretenimiento o publicidad— como para prácticas maliciosas —fraude, violencia digital o manipulación política—, obliga a revisar la manera en que las sociedades equilibran innovación y protección de derechos fundamentales como la libertad de expresión y la privacidad.

El artículo examina los riesgos asociados a los *deepfakes*, destacando su impacto en la reputación, la integridad individual y la democracia. Asimismo, analiza el marco normativo emergente en distintas latitudes, contrastando el enfoque centralizado y preventivo de China con el modelo descentralizado y reactivo de Estados Unidos, así como las disposiciones regulatorias de la Unión Europea. Este abordaje comparado permite visibilizar cómo factores culturales, jurídicos y políticos moldean respuestas diversas frente a un mismo fenómeno tecnológico.

Finalmente, se discuten las estrategias de mitigación que combinan la cooperación internacional, la alfabetización digital, el desarrollo de herramientas de detección y la responsabilidad de las plataformas digitales. El estudio concluye que los *deepfakes* no solo ponen en riesgo la seguridad y la privacidad de los individuos, sino que también generan una “crisis de la verdad” con implicancias globales. En consecuencia, se sostiene la necesidad de un enfoque integral que articule legislación, educación y tecnología, garantizando la innovación sin menoscabar los derechos humanos ni la estabilidad democrática.

Palabras clave: deepfakes, libertad de expresión, regulación jurídica, desinformación digital, inteligencia artificial

¹ Universidad de Congreso.

ABSTRACT

The expansion of deepfakes as a product of artificial intelligence poses unprecedented dilemmas at the intersection of technology, ethics, and law. These hyperrealistic representations, capable of altering faces, voices, and scenes, challenge the limits of human perception and undermine trust in the media, institutions, and public debate. Their use, both for legitimate purposes—education, entertainment, or advertising—and for malicious practices—fraud, digital violence, or political manipulation—forces us to rethink how societies balance innovation and the protection of fundamental rights such as freedom of expression and privacy.

The article examines the risks associated with deepfakes, highlighting their impact on reputation, individual integrity, and democracy. It also analyzes the emerging regulatory framework in different parts of the world, contrasting China's centralized and preventive approach with the decentralized and reactive model of the United States, as well as the regulatory provisions of the European Union. This comparative approach highlights how cultural, legal, and political factors shape diverse responses to the same technological phenomenon.

Finally, mitigation strategies that combine international cooperation, digital literacy, the development of detection tools, and the responsibility of digital platforms are discussed. The study concludes that deepfakes not only jeopardize the security and privacy of individuals, but also generate a “truth crisis” with global implications. Consequently, it argues for the need for a comprehensive approach that articulates legislation, education, and technology, ensuring innovation without undermining human rights or democratic stability.

Keywords: deepfakes, freedom of expression, legal regulation, digital disinformation, artificial intelligence

INTRODUCCIÓN

La inteligencia artificial ha transformado el mundo y, entre sus diversas aplicaciones, destaca su capacidad para generar contenidos audiovisuales hiperrealistas. Estos materiales, conocidos como *deepfakes*, difuminan la línea entre lo ficticio y lo real, lo que representa una amenaza significativa para ámbitos como la política, el cumplimiento de la ley y los medios de comunicación.

El desarrollo de la tecnología *deepfake* evidencia su carácter interdisciplinario y su relevancia académica, al integrar campos como la informática, la psicología cognitiva y los estudios de medios de comunicación, sustentándose en principios de redes neuronales y aprendizaje automático. Si bien en áreas como la educación, la publicidad y el cine tiene aplicaciones legítimas, también puede ser utilizada para difundir información falsa, cometer fraudes y ejercer violencia digital. Este fenómeno plantea un desafío jurídico y ético: proteger a la sociedad de sus riesgos sin vulnerar la libertad de expresión, un derecho fundamental.

En la actualidad, el debate se enfoca en cómo prevenir abusos que puedan poner en riesgo la democracia, la privacidad tanto individual como colectiva y la integridad de las personas, logrando un equilibrio con la innovación tecnológica. Es así como, a partir de esta premisa, los estados llevan adelante diversas estrategias para abordar la problemática.

CARACTERÍSTICAS DE LOS DEEPFAKES

Los *deepfakes* son una mezcla de “aprendizaje profundo” y videos “falsos” que implica la alteración digital de contenido audiovisual para crear representaciones hiperrealistas de individuos diciendo y haciendo cosas que nunca ocurrieron genuinamente (Alanazi y Asif, 2024, p.1). Esto pone en jaque la confianza de la sociedad en los medios de comunicación, las instituciones e incluso en sus propias percepciones.

En el caso de los videos, el proceso implica alinear los rostros de dos personas diferentes, usar un autocodificador para capturar las características de un rostro —identificado como “rostro A”— y, posteriormente, fusionar estas características con otro rostro —identificado como “rostro B”— (Alanazi y Asif, 2023, p.1). Tras múltiples iteraciones, se obtiene un *deepfake* de alta calidad, casi indistinguible del material original.

Aunque este tipo de contenido digital puede ser usado con un propósito positivo, generalmente no es así. Las personas sin experiencia pueden generarlo gracias a aplicaciones como FaceSwap y Face2Face. Además, a medida que la tecnología avanza, se vuelven más convincentes y difíciles de detectar; por lo tanto, normalmente necesitan el uso de IA para hallar inconsistencias. En otras palabras, un oído o un ojo humano no puede notar la diferencia, sin importar cuán capacitado esté.

Existen principalmente tres tipos de *deepfakes* que en los últimos años han ganado gran popularidad debido a su capacidad para imitar la realidad. El primero de ellos es el *deepface*, que consiste en la generación de imágenes falsas mediante inteligencia artificial. Un caso representativo ocurrió en 2023, cuando el periodista británico Eliot Higgins difundió ampliamente imágenes manipuladas del expresidente Donald Trump, en las que se lo veía siendo arrestado por presuntamente ocultar documentos oficiales.

El segundo tipo corresponde a los *deepvoices*, que imitan la voz de una persona en un audio, haciéndola sonar como si hubiera pronunciado palabras que en realidad nunca dijo. Este tipo de *deepfake* se utiliza con frecuencia en fraudes y estafas, lo que lo convierte en una herramienta especialmente riesgosa.

Por último, se encuentran los *deepfakes* de vídeo, que consisten en alterar o reemplazar digitalmente el rostro de una persona

en un material audiovisual, por ejemplo, mediante la técnica de *face-swap*. De esta manera, se generan escenas falsas de situaciones que nunca ocurrieron. Este tipo de *deepfake* combina elementos de los dos anteriores y ha sido señalado como uno de los más complejos y difíciles de detectar (ISMS Forum, 2025).

RIESGO QUE PRESENTA ESTE TIPO DE CONTENIDO

La utilización de la tecnología *deepfake* plantea importantes dilemas éticos y jurídicos, a pesar de que pueda ofrecer ciertas ventajas (Diakopoulos & Johnson, 2021). Desde finales de 2022, los contenidos *deepfake* creados han sido descargados casi quince millones de veces, siendo las mujeres las principales víctimas de este fenómeno. En particular, las imágenes íntimas no consensuadas (NCII) generadas por inteligencia artificial muestran un crecimiento alarmante y se están expandiendo a un ritmo acelerado.

En el ámbito del entretenimiento y la política, las amenazas más recurrentes están vinculadas con la desinformación y el daño reputacional. Sin embargo, los reportes más recientes advierten sobre el incremento de ataques masivos dirigidos a fraudes financieros a través de redes sociales (ISMS Forum, 2025, p. 24).

Aunque el daño reputacional presenta una incidencia relativamente menor en comparación con otros riesgos, sigue constituyendo un factor de relevancia, en especial para figuras públicas y organizaciones. Este escenario pone en jaque principios jurídicos fundamentales como la protección del bienestar físico y espiritual, el derecho a la intimidad y el respeto de la vida personal y familiar (ISMS Forum, 2025, p. 25; Rizzica, 2021).

LIBERTAD DE EXPRESIÓN Y SUS LÍMITES

La libertad de expresión es un derecho reconocido internacionalmente por la Decla-

ración Universal de los Derechos Humanos (art. 19), que garantiza que toda persona pueda emitir ideas, opiniones e información sin censura previa. Sin embargo, la libertad de expresión no es absoluta. Tanto en el derecho internacional como en la jurisprudencia nacional, se establecen límites cuando el ejercicio de este derecho produce daños a terceros, como la difamación, la incitación a la violencia, la pornografía no consensuada o la vulneración de la privacidad.

Las operaciones de información no son nuevas y han sido empleadas por actores durante décadas. Sin embargo, la llegada de internet ha incrementado exponencialmente la escala, el alcance y la velocidad de las campañas de información, siendo las redes sociales el principal canal para dichas actividades (Kuźnicka y Kostyuk, 2025).

Esta situación obliga a la humanidad a enfrentarse a un dilema: ¿qué grado de protección corresponde otorgar a los *deepfakes* en una democracia, considerando que pueden entenderse como una forma de expresión? Algunas personas sostienen que deberían prohibirse por completo, mientras que otras defienden que las leyes de libertad de expresión también deberían ampararlos. Existe, además, una postura intermedia que propone permitir su uso con fines legítimos, como la educación o el entretenimiento, pero restringirlos cuando se empleen con intenciones maliciosas.

El debate resulta particularmente complejo, ya que los *deepfakes* desafían los límites de la libertad de expresión, un derecho fundamental que los Estados deben tener en cuenta al enfrentar fenómenos como el fraude electoral. La problemática se intensifica cuando estas creaciones dejan de estar vinculadas al humor o la parodia y pasan a emplearse con fines que afectan de manera directa a los ciudadanos.

CASOS Y REGULACIONES INTERNACIONALES

La creciente preocupación por el impacto de la tecnología *deepfake* ha puesto de relieve la necesidad de un análisis profundo en el ámbito del derecho penal y de las políticas públicas. Este examen resulta fundamental para comprender cómo los avances jurídicos actuales pueden servir como base para el desarrollo de futuras normativas que regulen de manera efectiva el uso de estas tecnologías.

En ese sentido, el eje central de este análisis se concentra en las legislaciones que continúan en proceso de evolución tanto en Estados Unidos como en China y la Unión Europea (Ramos-Zaga, 2024). A nivel global, distintos países han comenzado a elaborar normativas específicas para abordar el fenómeno de los *deepfakes*, aunque con enfoques diversos y particularidades propias de cada contexto.

En Estados Unidos, varios estados —entre ellos California— han implementado leyes que restringen la divulgación de *deepfakes* en escenarios electorales o con fines difamatorios. Si bien su aplicación aún es incompleta y varía según la jurisdicción, estas regulaciones buscan resguardar la integridad de los procesos democráticos, lo que ha generado un intenso debate respecto a su compatibilidad con la libertad de expresión.

Por su parte, China ha establecido la obligación de que todo contenido generado por inteligencia artificial, incluidas imágenes y videos, incorpore de manera visible una etiqueta que indique que se trata de un *deepfake*. Con ello, el país pretende asegurar la transparencia y proteger a la ciudadanía, sin prohibir el uso de la tecnología.

En el caso de la Unión Europea, el Digital Services Act (DSA) obliga a las plataformas digitales a detectar y retirar contenidos falsos que puedan ocasionar daños significativos, al mismo tiempo que impulsa la transparencia y la provisión de información a los

usuarios. De manera complementaria, el AI Act establece que los sistemas de inteligencia artificial destinados a generar o modificar contenidos deben garantizar estándares mínimos de transparencia, asegurando que los usuarios sean informados cuando interactúan con ellos, salvo en los casos en que la naturaleza del contenido haga evidente su origen artificial (Rouse, 2024).

LAS DIFERENCIAS ENTRE CHINA Y ESTADOS UNIDOS A LA HORA DE LEGISLAR LOS DEEPFAKES

Los métodos políticos y jurídicos de China y de Estados Unidos revelan enfoques claramente diferenciados en materia de regulación de los *deepfakes*. En el caso chino, se trata de un modelo centralizado y preventivo que controla el proceso desde la propia generación del contenido, mientras que Estados Unidos sigue un modelo descentralizado y de carácter reactivo, carente de una legislación federal específica. La regulación recae en leyes estatales, como las de Texas o California, que se concentran en problemáticas puntuales.

Desde enero de 2023, China regula los *deepfakes* con un enfoque centralizado y preventivo mediante las Provisions on the Administration of Deep Synthesis of Internet-Based Information Services. Estas normas obligan a las plataformas a identificar, marcar y bloquear contenido falso o dañino y exigen que cualquier edición de información facial, de voz u otra biométrica cuente con el consentimiento explícito de la persona afectada (Zhang, 2023).

Posteriormente, en marzo de 2025, la Administración del Ciberespacio de China (CAC) publicó las Measures for Labeling of Artificial Intelligence-Generated Synthetic Content, que entró en vigor el 1 de septiembre de 2025. Estas reglas establecen que todo contenido generado por inteligencia artificial debe estar claramente etiquetado, ya sea de forma explícita —como advertencias visibles— o implícita —mediante marcas de

agua digitales y metadatos—. Además, las plataformas deben mantener registros de la creación y difusión del contenido para fines de supervisión y posibles investigaciones.

Esta perspectiva evidencia el propósito del gobierno de China de tener control sobre todo el proceso de producción y difusión de contenidos, dando prioridad a la estabilidad social y a la seguridad nacional. No solo se sanciona la propagación de *deepfakes* maliciosos, sino también el hecho de que las plataformas tecnológicas no etiqueten ni supervisen.

En contraste, Estados Unidos no dispone de una ley federal unificada que regule los *deepfakes*. La normativa vigente se encuentra fragmentada en disposiciones estatales y en proyectos legislativos que atienden a situaciones particulares.

En septiembre de 2024, California promulgó la ley SB 926, que prohíbe la distribución de imágenes *deepfake* que representen partes íntimas del cuerpo sin consentimiento. Esta conducta se tipifica como un delito menor y contempla una pena máxima de un año de prisión junto con una multa de hasta 2.000 dólares.

En abril de 2025, el gobernador de New Jersey, Phil Murphy, firmó la legislación A3540/S2544, que establece sanciones tanto civiles como penales para quienes creen o distribuyan *deepfakes*. La norma considera esta práctica como un delito de tercer grado, punible con penas de hasta cinco años de prisión y multas que pueden alcanzar los 30.000 dólares.

Finalmente, el 19 de mayo de 2025, el presidente Donald Trump sancionó la ley Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act). Esta disposición prohíbe la publicación no consensuada de imágenes íntimas, ya sean reales o generadas mediante inteligencia artificial, y obliga a las plataformas en lí-

nea a eliminar dicho contenido en un plazo máximo de 48 horas tras recibir la notificación correspondiente.

En síntesis, ciertos estados han implementado regulaciones concretas. El empleo de *deepfakes* fraudulentos durante las campañas electorales está prohibido en Texas y California. Nueva York está progresando en la salvaguardia de la identidad digital y castiga la difusión de contenidos sexuales falsos (Latorre, 2025).

La ley federal “Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act” (también llamada “Take It Down Act”) ha suscitado inquietudes entre quienes defienden la privacidad y la libertad de expresión. La Electronic Frontier Foundation y la Cyber Civil Rights Initiative, entre otros críticos, alertan de que el lenguaje legal es excesivamente extenso y podría conducir a la censura y a infracciones de la Primera Enmienda.

ESTRATEGIAS DE MITIGACIÓN DE DEEPFAKES

A nivel global, se reconoce cada vez más la necesidad de regular los *deepfakes* de manera integral. Organismos como las Naciones Unidas y el Foro Económico Mundial han comenzado a debatir estrategias para proteger legalmente a las víctimas, buscando un equilibrio entre prevenir daños y mantener la libertad de expresión e innovación (Hilda, 2024).

La colaboración a nivel internacional es crucial para abordar este problema, dado que crear y difundir *deepfakes* generalmente implica traspasar fronteras. Esta cooperación incluye el intercambio de tecnologías, información y métodos. Asimismo, es fundamental colaborar con las empresas de tecnología porque su intervención en el monitoreo, gestión y desarrollo de herramientas de detección ayuda a disminuir la circulación de *deepfakes* y asegurar que se cumplan las normas del contenido.

La alfabetización digital es esencial para que los usuarios puedan identificar contenidos falsos. Es crucial que los usuarios sean conscientes de la existencia de los *deepfakes* y comprendan su impacto ético y social. Además, la investigación destaca la importancia de integrar la educación sobre *deepfakes* en los programas escolares para fomentar una ciudadanía digital crítica (Walsh, 2024).

El desarrollo de tecnologías para identificar *deepfakes* es una prioridad. Un estudio de Science Direct analiza diversos métodos técnicos para detectarlos, incluyendo el uso de redes neuronales y algoritmos avanzados. Sin embargo, la evolución constante de las técnicas de generación de este tipo de contenidos representa un enorme desafío para mantener la eficacia de estas herramientas (Soundarya, 2025).

Las plataformas digitales desempeñan un papel fundamental en la administración de contenidos creados por inteligencia artificial. Naciones como la Unión Europea y Canadá han establecido normativas que requieren que las plataformas marquen los contenidos producidos por IA y penalicen su uso malintencionado. El propósito de estas acciones es mejorar la transparencia y la responsabilidad en el entorno digital.

¿CÓMO DETECTAR UN DEEPPFAKE?

Las 8 recomendaciones más importantes a la hora de detectar un *deepfake* (Lisa Institute):

- Señales visuales evidentes: muchos *deepfakes* muestran fallos que delatan su manipulación, como expresiones faciales que no coinciden del todo, ángulos de cabeza extraños o iluminación poco natural. Las ediciones digitales también pueden dejar rastros visibles, como bordes difuminados, piel demasiado uniforme o movimientos antinaturales.
- Frecuencia de parpadeo: un método sencillo para detectar *deepfakes* es obser-

var cómo parpadea la persona en el video. Normalmente, los *deepfakes* presentan un parpadeo irregular o menos frecuente, ya que los algoritmos todavía tienen dificultades para replicarlo de manera convincente. No obstante, esta técnica se vuelve menos confiable a medida que mejora la tecnología.

- Desajuste entre rostro y cuerpo: la mayoría de los *deepfakes* modifican solo la cara, dado que alterar el cuerpo completo es más complicado. Por lo tanto, si hay incoherencias entre la cabeza y el cuerpo, como proporciones extrañas o características físicas incongruentes, puede ser un indicio de manipulación.

- Duración del video: generalmente, los *deepfakes* son cortos, con pocos segundos de duración, porque generar contenido extenso requiere mucho tiempo y procesamiento. Un clip breve con elementos poco creíbles puede alertar sobre su falsedad.

- Revisar la fuente: identificar quién compartió el video, dónde apareció por primera vez y en qué contexto es esencial para evaluar su autenticidad. Esta investigación es fundamental en la verificación digital y el análisis en línea.

- Desincronización del audio: en ciertos *deepfakes*, la voz no coincide perfectamente con el movimiento de los labios, lo que puede indicar una edición deficiente o falta de ajuste entre imagen y sonido.

- Observación de detalles y fondo: reproducir el video a cámara lenta puede ayudar a notar transiciones abruptas, cambios repentinos o alteraciones en el fondo que revelen manipulación.

- Interior de la boca: reproducir con precisión la lengua, dientes y otras estructuras internas sigue siendo complicado para la IA. Cualquier error mínimo en estas áreas puede servir como señal de que el contenido es falso.

Además, existen herramientas y plataformas en línea diseñadas para detectar *deepfakes*. Estas aplicaciones analizan imágenes y videos en busca de señales de edición, como desajustes en expresiones, parpadeo irregular o problemas de sincronización de audio. Algunas utilizan inteligencia artificial para identificar patrones que resultan difíciles de notar a simple vista, facilitando así la verificación de la autenticidad digital.

CONCLUSIONES

Los *deepfakes* no solo afectan a las víctimas individuales, sino que también representan una amenaza para la democracia. Un video falso puede alterar el curso de una elección, fomentar la polarización social o deslegitimar instituciones.

Este tipo de situaciones erosionan la confianza en la información y pueden llevar a lo que se conoce como “crisis de la verdad”, en la que las personas ya no saben qué es real y qué no. Esto debilita el debate público y puede ser utilizado por gobiernos o grupos de poder para manipular a la ciudadanía.

Los países adoptan enfoques diferentes para legislar sobre los *deepfakes* debido a sus marcos legales, culturales y políticos particulares. Factores como la tradición jurídica, la importancia que se le da a la libertad de expresión, la protección de la privacidad y la capacidad tecnológica influyen en cómo se regula esta tecnología. Estas diferencias hacen que la legislación pueda variar desde medidas estrictas hasta enfoques más flexibles, según las prioridades y valores de cada sociedad.

Asimismo, la rapidez con la que las tecnologías de inteligencia artificial y los *deepfakes* avanzan exige que cada nación logre un balance entre la necesidad de resguardar a sus ciudadanos y la protección de derechos esenciales. Esta tensión produce variedad en las tácticas legales, porque lo que es efectivo en un contexto puede no serlo o no ser aceptable en otro, resultando así en un

mosaico de prácticas de supervisión y regulaciones.

La lucha contra los *deepfakes* requiere un enfoque integral que combine educación, tecnología, legislación y responsabilidad de las plataformas. Es fundamental que los usuarios estén informados, las herramientas de detección sean eficaces, las leyes sean justas y las plataformas asuman su responsabilidad en la gestión de contenidos.

REFERENCIAS BIBLIOGRÁFICAS

- Alanazi, S., & Asif, S. (2023). *Understanding deepfakes: A comprehensive analysis of creation, generation, and detection*. <https://doi.org/10.54941/ahfe1003290>
- Alanazi, S., & Asif, S. (2024). Explorando la tecnología deepfake: creación, consecuencias y contramedidas. *Human-Intelligent Systems Integration*, 6, 49–60. <https://doi.org/10.1007/s42454-024-00054-8>
- Consejo de Administración del Ciberespacio de China. (2025, marzo 14). *Disposiciones sobre síntesis profunda*. https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm
- Diakopoulos, N., & Johnson, D. (2021). Anticipating and addressing the ethical implications of deepfakes in the context of elections. *New Media & Society*, 23(7), 2072–2098. <https://doi.org/10.1177/1461444820925811>
- Kuźnicka-Błaszowska, D., & Kostyuk, N. (2025). Necesidad emergente de regular los deepfakes en el derecho internacional: la guerra ruso-ucraniana como ejemplo. *Journal of Cybersecurity*, 11(1), tyaf008. <https://doi.org/10.1093/cybsec/tyaf008>
- Hilda, H. (2024, septiembre 30). 16 types of identity theft and how to prevent them. *HyperVerge*. <https://hyperverge.co/blog/types-of-identity-theft/>
- Instituto ISMS. (s. f.). *Deepfake: riesgos, tipos y consejos de seguridad*. <https://www.ismsforum.es/ficheros/descargas/deepfake-final1742458135.pdf>
- Lisa Institute. (s. f.). *Deepfakes: tipos, consejos, riesgos y amenazas*. https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas?srsId=AfmBOooQh_fvHhdZyTiNMUKOPB7jsy_uZ4bSliQvwIPF_S86IOyxevw
- Oxford Internet Institute. (s. f.). *Dramatic rise in publicly downloadable deepfake image generators*. <https://www.oii.ox.ac.uk/news-events/dramatic-rise-in-publicly-downloadable-deepfake-image-generators/>
- Rizzica, A. (2021). *Sexually explicit deepfakes: To what extent do legal responses protect the depicted persons?* (Tesis de maestría, Tilburg University). <http://arno.uvt.nl/show.cgi?fid=154764>
- Rouse. (2024). *AI-generated deepfakes: What does the law say?* <https://rouse.com/insights/news/2024/ai-generated-deepfakes-what-does-the-law-say>
- Soundarya, B. C. (2025). A framework for deepfake detection using convolutional neural networks. *ScienceDirect*. <https://www.sciencedirect.com/science/article/pii/S1877050925017235>
- Universidad de la Ciudad de Concordia. (s. f.). *Ficción peligrosa: deepfakes, política y violencia digital*. <https://www.ucc.edu.ar/notas/ficcion-peligrosa-deepfakes-politica-violencia-digital>

Walsh, M. (2024, octubre 28). *A framework for detection in an era of rising deepfakes*.
<https://doi.org/10.58012/e5sh-hp94>

Zhang, L. (2023). China: Entran en vigor las disposiciones sobre la tecnología de síntesis profunda. *Biblioteca del Congreso*. <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/>