Universidad de San Andrés
Departamento de Derecho
Maestría en Propiedad Intelectual e Innovación

Tesis de Maestría

DEEPFAKED:
PROPUESTA DE REGULACIÓN DE RÉPLICAS DIGITALES

Malena Beatriz Mancini, D.N.I. 35.079.143
Directora de tesis: Verónica María Canese

Buenos Aires, marzo 2024

INDICE TEMÁTICO

Resumen **4**
1. Introducción **5**
2. Derecho a la imagen **8**
2.1. Regulación del derecho a la imagen en Argentina 12
2.2. Regulación del derecho a la imagen en Latinoamérica 14
Cuadro 1: protección del derecho a la imagen en América Latina. 14
2.3. Regulación del derecho a la imagen en Europa 16
Cuadro 2: protección del derecho a la imagen en Europa. 17
2.4. Regulación del derecho a la imagen en Estados Unidos 19
2.5. Regulación internacional del derecho a la imagen 21
2.6. Protección penal de la imagen personal 21
2.7. El particular caso de la Isla de Guernsey 23
3. *Deepfakes* y la creación de réplicas digitales **26**
3.1. ¿Qué son los *deepfakes*? 26
3.2. Taxonomía de los *deepfakes* 28
3.3. Consentimiento para el uso de la imagen personal en la creación de replicas digitales 31
4. Las réplicas digitales en la actualidad **39**
4.1. Distintos usos de las réplicas digitales 39
4.1.1. Desinformación 40
4.1.2. Suplantación de identidad 42
4.1.3. Entretenimiento 44
4.2. Acuerdo entre SAG-AFTRA y AMPTP para los contratos de televisión y salas de cine (*theatrical*) de 2023 47
4.3. Esfuerzos por combatir los usos perjudiciales de las réplicas digitales 52
4.4. Situación regulatoria actual 60
Cuadro 3: resumen de la 'DEEPFAKES Accountability Act' de 2023. 66
Cuadro 4: legislación en materia de réplicas digitales en los estados de EE.UU. 68
4.5. Breve análisis estructural de la legislación existente 77
Cuadro 5: breve análisis estructural de la legislación existente. 78
5. Parámetros y lineamientos para la regulación de réplicas digitales **80**
6. Conclusión **87**
Bibliografía **89**

Agradecimientos

A Federico, mi compañero de vida, por su apoyo incondicional y su motivación constante. Gracias por siempre escucharme y por los incontables debates que aportaron al desarrollo de este trabajo.

A Joaquín, que con menos de dos años fue muy paciente mientras mamá trabajaba.

A mi familia, por la inmensa ayuda que me dieron para que pudiera concluir este proyecto.

A Florencia Beati, por la confianza y el constante empuje.

A María de Lourdes Vázquez, por transmitirnos pasión por esta rama del derecho, contagiando siempre su entusiasmo por la propiedad intelectual.

A Verónica Canese, mi tutora, por sus aportes y el tiempo dedicado, a quien agradezco enormemente su generosidad.

A mis compañeros, cuyo acompañamiento fue esencial para transitar una maestría en medio de una pandemia.

A Tomillo, quien me acompaño incontables horas de trabajo y siempre estuvo a mi lado.

Resumen

Las réplicas digitales o *deepfakes* son reproducciones virtuales de la imagen de una persona que aparentan ser reales. Los softwares que permiten crearlas han avanzado significativamente en los últimos años, siendo hoy posible crear una réplica digital desde cualquier dispositivo móvil sin necesidad de conocimientos técnicos. Estos novedosos activos digitales presentan nuevas oportunidades comerciales para los titulares de derecho, pero su explotación no consensuada puede generar daños tanto al sujeto representado como al espectador. Tradicionalmente el abuso de la imagen ha sido un problema que ha inquietado principalmente a aquellos que se encuentran en la esfera pública, sin embargo la domesticación de estas tecnologías lo ha convertido en una preocupación para todos. Extorsiones, engaños, ciberacosos, robos, estafas y *phishing* son solo algunos de los riesgos asociados al mal uso de estas tecnologías. Los instrumentos legales existentes ya no son lo suficientemente adecuados para hacer frente a los abusos de las réplicas digitales en línea, por lo que es preciso contar con una regulación que contemple sus particularidades y establezca reglas claras para su creación, uso y difusión, otorgando a su vez seguridad jurídica a los titulares de derecho para aprovechar los beneficios que presentan estas tecnologías.

Abstract

Digital replicas or deepfakes are virtual reproductions of a person's image that appear to be real. Software that allows their creation has advanced significantly in recent years, and today it is possible to create a digital replica from any mobile device without the need for any technical knowledge. These novel digital assets present new commercial opportunities for right holders, but their non-consensual exploitation can cause harm to both the represented subject and the viewer. Traditionally, image abuse has been a problem that has primarily concerned those in the public sphere, however the domestication of these technologies has made it everyone’s concern. Extortion, deception, cyberbullying, theft, scams and phishing are just some of the risks associated with the misuse of these technologies. The existing legal instruments are no longer adequate to deal with the abuses of digital replicas online, making it is necessary to have regulation that takes into account their particularities and establishes clear rules for their creation, use and dissemination, granting legal security for right holders to take advantage of the benefits presented by these technologies.

1. Introducción

La imagen es parte esencial de la identidad de una persona, es por eso que el derecho a la imagen es considerado un derecho personalísimo. Sin embargo, esta tiene también una aplicación comercial, pudiendo representar una importante fuente de ingresos. Por lo tanto, su protección debe ser comprensiva tanto de la esfera personal como de la comercial, protegiendo no solamente la honra y la intimidad de las personas –como lo hacen las normas que la regulan en la actualidad– sino también su explotación comercial.

Una réplica digital es la reproducción virtual de una persona, hecha a su imagen y semejanza, procurando ser lo más fiel posible a la realidad. Tradicionalmente estas réplicas digitales han sido usadas en la industria del entretenimiento, en particular en grandes producciones audiovisuales que podían afrontar los costos que conllevaba su creación, pero en el último quinquenio su uso se ha popularizado.

Las réplicas digitales tienen muchas aplicaciones. Quienes suelen redituar de su imagen, han encontrado una nueva oportunidad comercial en la explotación de sus réplicas digitales y la aplicación de inteligencia artificial a su semejanza, las cuales amplían las opciones laborales de las celebridades, permitiéndoles hablar en idiomas que no conocen, participar de contenido sin siquiera estar presente e incluso presentan una posibilidad de ingreso económico para los derechohabientes luego del fallecimiento de quienes estuvieron en la órbita pública.

Los avances de la inteligencia artificial y el auge de los softwares de *deep learning* han facilitado la creación de estas réplicas digitales permitiendo que cada vez sea más sencillo acceder a ellas. Actualmente cualquier persona puede tener acceso a herramientas para generar un contenido que simule representar a una persona real o incluso que contenga una persona completamente ficticia. El problema es que no siempre este contenido es bien intencionado, desde 2017 cuando se publicó el primer *deepfake* –nombre con el que se conoce popularmente a estas representaciones digitales– han surgido numerosos casos en los que estas tecnologías fueron aplicadas para defraudar, desinformar e incluso afectar la integridad sexual de menores. El último año se ha observado un gran crecimiento en la aplicación de estas tecnologías, desde su popularización en redes sociales hasta denuncias públicas de celebridades que vieron su imagen reflejada en contenido que no autorizaron. El riesgo que conlleva su aplicación malintencionada y su

creciente abuso requiere prestar atención al fenómeno de las réplicas digitales que se está viviendo en Internet.

Estos riesgos podrían mitigarse mediante la sanción de una regulación que determine reglas claras en relación con la creación, uso y difusión de réplicas digitales. Si bien como se analizará a continuación, existen unas pocas jurisdicciones que ya cuentan con legislación en la materia, la regla en el entorno digital pareciera que continúa siendo la autorregulación de los proveedores de servicios de Internet, los cuales mediante cláusulas en sus términos y condiciones de uso establecen algunas reglas puntuales y buenas prácticas sobre como los usuarios deben comportarse ante este tipo de contenido sintético. Pero la autorregulación en materia de réplicas digitales no continuará siendo viable por mucho tiempo más[1], está siendo cada vez más evidente que las plataformas y redes sociales necesitan instaurar nuevas medidas para hacer frente a los abusos de estas tecnologías, medidas tanto proactivas como reactivas. Un ejemplo de esto es el reciente ataque a la imagen de la artista norteamericana Taylor Swift quien fue víctima de una serie de réplicas digitales con tenor sexual. Ante esta situación la respuesta de la plataforma X/Twitter donde estaban circulando estos *deepfakes* fue bloquear las búsquedas del nombre de la cantante[2] a fin de evitar que más usuarios accedieran al contenido. Esto fue claramente un intento desesperado de la red social por mitigar el daño que se estaba ocasionando a Swift pero resulta evidente que no es la respuesta más adecuada siendo que una de las publicaciones que contenían el material explícito alcanzó a tener más de cuarenta y cinco millones de vistas antes de ser dada de baja[3].

Por otro lado, el creciente uso de estas tecnologías está potenciando el desarrollo de softwares que pretenden combatir el mal uso de las réplicas digitales desde el plano técnico. Algunas de estas herramientas tienen un enfoque más bien preventivo, como por ejemplo aquellos softwares que permiten hacer alteraciones imperceptibles a las imágenes que se cargan a Internet a fin de dificultar el trabajo de los softwares de alteración de

[1] Guest, P. (26 de octubre de 2023). The UK's controversial Online Safety Act is now law. *Wired*. https://www.wired.co.uk/article/the-uks-controversial-online-safety-act-is-now-law

[2] Cohen, L. (2024, 29 enero). *Taylor Swift searches blocked on X after fake explicit images spread.* Reuters. https://www.reuters.com/technology/taylor-swift-searches-blocked-x-after-fake-explicit-images-spread-2024-01-28/

[3] Weatherbed, J. (25 de enero de 2024). Trolls have flooded X with graphic Taylor Swift AI fakes. *The Verge.* https://www.theverge.com/2024/1/25/24050334/x-twitter-taylor-swift-ai-fake-images-trending?ref=404media.co

imagen arrojando resultados que no parecen tan realistas[4]. Otras pretenden detectar el contenido sintético alertando a los usuarios de su falsedad. El problema con estas herramientas es que si bien hoy funcionan, no hay garantía de que los avances de la inteligencia artificial no logren superar las barreras que imponen y las tornen obsoletas[5]. *"Usar tecnología para detectar deepfakes siempre será una carrera armamentista"*[6].

Si bien las herramientas técnicas pueden ayudar a mitigar los riesgos, tienen sus limitaciones. Es preciso contar con una legislación que establezca normas claras y concretas que sean eficientes a la hora de confrontar este tipo de contenido, que sean pensadas considerando las características particulares tanto de las réplicas digitales como del entorno donde circulan, que no se limiten a plantear medidas reactivas o correctivas, sino que incluyan además medidas preventivas que mitiguen lo más posible el impacto de este tipo de contenido sintético, resguardando a su vez el ejercicio regular del derecho a la libertad de expresión.

El objetivo del presente trabajo es proponer parámetros y lineamientos para la regulación de réplicas digitales, exponiendo cuales son los puntos clave que debería considerar una legislación en la materia. Para ello, en primer lugar se analizarán las características del derecho a la imagen, derecho que se encuentra en la base de las réplicas digitales, procurando presentar un análisis comprensivo de la situación regulatoria de este derecho a nivel nacional e internacional. Luego, se procederá a estudiar qué son estas réplicas digitales o *deepfakes*¸ presentando una clasificación de los distintos tipos detectados, como así también un análisis de uno de los requisitos primordiales del uso de la imagen personal, el consentimiento. Se concluirá el análisis con un panorama completo de las réplicas digitales en la actualidad, abarcando sus usos más frecuentes, las novedades en la materia y la situación regulatoria actual a nivel global. Una vez asentado el estado del arte en el campo de réplicas digitales, se procederá a plantear una propuesta de parámetros y lineamientos para su regulación, con la esperanza de que al concluir sean evidentes los beneficios del cambio propuesto.

[4] Como por ejemplo PhotoGuard una aplicación desarrollada por el Laboratorio de Ciencias de la Computación e Inteligencia Artificial del Instituto de Tecnología de Massachusetts (MIT), o Fawkes desarrollada por el SAND Lab (Security, Algorithms, Networking and Data) de la Universidad de Chicago.
[5] Heikkilä, M. (31 de enero de 2024). *Tres lecciones a partir de los «deepfakes» porno de Taylor Swift.* MIT Technology Review. https://www.technologyreview.es/s/16137/tres-lecciones-partir-de-los-deepfakes-porno-de-taylor-swift
[6] Au, L. (3 de diciembre de 2019). *China targets 'deepfake' content with new regulation.* TechNode. https://technode.com/2019/12/03/china-targets-deepfake-content-with-new-regulation/. La traducción es propia.

2. Derecho a la imagen

Dentro del compendio de derechos personalísimos que poseemos los seres humanos, esos derechos innatos y vitalicios que están íntimamente unidos a nuestra persona, encontramos al derecho a la imagen.

El derecho a la imagen resguarda la expresión más externa de la personalidad, la cual se puede manifestar de diferentes formas[7]. El objeto de protección de este derecho se encuentra en la externalización de la esfera personal del individuo, la cual constituye la base de su identidad y un elemento central para el reconocimiento de su individualidad[8]. Habitualmente se encuentra relacionado a otros derechos personalísimos como lo son el derecho a la intimidad o a la honra, no obstante, se trata de derechos independientes. Así lo ha reconocido la Cámara Nacional de Apelaciones en lo Civil reiteradas veces: *"[…]sin perjuicio de estar el derecho a la imagen muy vinculado al derecho al honor y al derecho a la intimidad, se entiende que aquél reviste la condición de autónomo pues puede existir su vulneración sin que se configure a la par un ataque a la reputación o a la vida privada"*[9]*; "[l]a imagen o apariencia de una persona es protegida en forma autónoma, aun cuando también puede o no ella ser sustento de un ataque al honor o su intimidad"*[10].

En el ámbito internacional, el Tribunal Europeo de Derechos Humanos ha reconocido en más de una ocasión[11] la importancia de la protección de este derecho, diciendo que *"[l]a imagen de una persona constituye uno de los principales atributos de su personalidad, ya que revela sus características únicas y la distingue de sus pares. El derecho a la protección de la propia imagen es, pues, uno de los componentes esenciales del desarrollo personal y presupone el derecho a controlar el uso de esa imagen. Si bien en la mayoría de los casos el derecho a controlar dicho uso implica la posibilidad de que un individuo rechace la publicación de su imagen, también cubre el derecho del individuo a oponerse a la grabación, conservación y reproducción de la imagen por parte de otra*

[7] Ceballos Delgado, J. M. (2011). Aspectos generales del derecho a la propia imagen. Revista La propiedad inmaterial, (15), 61-83. https://dialnet.unirioja.es/servlet/articulo?codigo=3785211.
[8] Cámara Nacional de Apelaciones en lo Civil. Sala D. 20382/2015. Attardo, Raul Daniel c/ Editorial Los Alamos SA s/daños y perjuicios. 16 de diciembre de 2021.
[9] Cámara Nacional de Apelaciones en lo Civil. Sala B. 95667/2016. Ozu, Pablo c/ Olivan, Maria Julia y otro s/daños y perjuicios. 25 de abril de 2022.
[10] Cámara Nacional de Apelaciones en lo Civil. Sala J. 60235/2017. Vargas, Ricardo Andrés c/ THX Medios S.A. s/ daños y perjuicios. 10 de Junio de 2019.
[11] Véase Reklos and Davourlis v Greece, n° 1234/05, Tribunal Europeo de Derechos Humanos Sección Primera, § 38 (15 de enero de 2009); von Hannover v Germany (no 2), Tribunal Europeo de Derechos Humanos Gran Sala (7 de febrero 2012)

persona. Dado que la imagen de una persona es una de las características inherentes a su personalidad, su protección efectiva presupone, en principio […] obtener el consentimiento del interesado en el momento la fotografía se toma y no simplemente si se publica y cuándo. De lo contrario, un atributo esencial de la personalidad quedaría en manos de un tercero y el interesado no tendría control sobre cualquier uso posterior de la imagen"[12].

Es importante entender que el concepto de imagen excede la mera fisonomía de una persona y se extiende a todas aquellas características que permiten percibir la identidad de un sujeto. Puede suceder que una persona sea reconocida cuando su imagen no está completa, cuando su rostro no se muestra[13], o incluso cuando no se reproduzca rasgo físico alguno. Entendemos por 'imagen' *"cualquier aspecto exteriorizable de la persona que la haga reconocible ante terceros"*[14].

En este sentido, la Cámara Nacional de Apelaciones en lo Civil ha dicho que *"[l]a doctrina mayoritaria concibe al derecho a la imagen como aquel que protege de las agresiones a la integridad espiritual de la persona, con el objeto de impedir el avasallamiento de la manifestación externa o visible de la personalidad humana en cualquiera de sus formas (reproducción o captación de alguna parte del cuerpo, de la voz, de los gestos, utilizando para ello cualquier medio como fotografía, escultura, imitación, filmación, grabación, etc.)"*[15].

Si pensamos a la imagen como todo aquello que individualiza a la persona, que la diferencia del resto, entonces dentro de este concepto incluimos por supuesto su rostro y cuerpo, pero también sus rasgos característicos, su tono de voz, sus manerismos, su peinado, su vestimenta. A veces ocurre que un solo elemento es tan característico que incluso su presencia aislada, separada del todo que hace al sujeto, permite reconocerlo.

[12] Reklos and Davourlis v Greece (2009).
[13] En el caso *Braunstein Tamara Iliana c/ Palermo Films S.A. y otro s/diferencias de salarios*, la actora participó de una pieza publicitara cediendo debidamente los derechos de uso de su imagen a tal efecto. Vencido el plazo originalmente previsto en el contrato, al momento de su renovación las partes no lograron llegar a un acuerdo respecto de las pretensiones económicas de la actora, ante lo que el anunciante decidió editar la pieza y simplemente reemplazar el rostro de la Sra. Braunstein por el de una co-protagonista. El Tribunal falló a favor de la actora y dijo que el anunciante *"tenía derecho a no estar de acuerdo con las pretensiones de retribución reclamadas por la actora, pero en ese caso debía entonces inhibirse de utilizar en modo alguno la imagen de esta última, y* ***no proceder a seccionarla, como si su pretendido derecho de autor sobre el film publicitario le diera derecho a separar el cuerpo de una persona de su cabeza y rostro****"*. Véase Cámara Nacional de Apelaciones del Trabajo. 19988/2013. Braunstein Tamara Iliana c/ Palermo Films S.A. y otro s/diferencias de salarios. 21 de febrero de 2017. El resaltado me pertenece.
[14] Ceballos (2011).
[15] Vargas c/ THX Medios S.A. (2019).

Otras veces es un conjunto de estos elementos, que cuando se presentan combinados apelan a la semejanza de un individuo y permiten identificarlo[16].

El problema que presentan los reclamos basados en elementos distintivos de la persona, es que la notoriedad de las características que permiten individualizarla depende del propio criterio de la autoridad judicial que analiza el caso[17]. En España, en el caso *Emilio Aragón Álvarez c/ Proborín, S.L.* hubo disidencia entre las distintas instancias del proceso respecto al criterio a aplicar[18], en particular sobre si las características replicadas

[16] En este sentido se destaca el caso del bailarín español Joaquín Cortés quien demandó a la empresa Latona S.A. por un anuncio publicitario de la marca 'Cacaolat' que mostraba a *"un hombre de pelo lacio y negro hasta los hombros, con el torso desnudo, sudoroso, vestido con pantalón negro ajustado y botas negras, que realiza unos pasos de baile flamenco"*, alegando que estas eran todas características que lo identificaban y que en el anuncio la empresa hacía alusión a su persona. La Audiencia de Barcelona reconoció que la apariencia del Sr. Cortés *"trasciende de sus propios espectáculos para pasar a ser la que el mismo interesado ofrece además, como creación propia y plenamente identificatoria, distinta de la de los otros bailarines, cuando explota comercialmente su imagen, la cual de este modo llega a todo tipo de público, y no sólo al aficionado al baile que ejecuta profesionalmente, convirtiéndose en notoria"*. Véase *El bailarín Joaquín Cortés gana una batalla legal contra Cacaolat.* (28 de julio de 2002). Elmundo.es. https://www.elmundo.es/elmundo/2002/07/28/cultura/1027867605.html.

[17] La Corte de Apelaciones de Nueva York ha dicho en el caso *Cohen v. Herbal Concepts* que la suficiencia de las pruebas presentadas por el actor a fin de acreditar el uso indebido de su imagen o semejanza, dependerá necesariamente de la determinación que haga quien juzga el caso, quien deberá analizar la calidad y cantidad de las características identificables que presenta la imagen objetada, la claridad de la fotografía –en caso de corresponder–, la visibilidad de las mencionadas características identificables y su carácter distintivo (Emilio Aragón Álvarez c/ Proborín, S.L. [2001]); y agregó que incluso el contenido del texto publicitario que acompaña la imagen puede ayudar al reconocimiento de la persona. Véase Cohen v. Herbal Concepts, 63 N.Y.2d 379, 482 N.Y.S.2d 457, 472 N.E.2d 307 (N.Y. 1984).

[18] El Sr. Álvarez presentó una demanda contra la empresa Proborín, S.L. a raíz de una serie de publicaciones que incluían un dibujo de un personaje de piernas cruzadas, vistiendo pantalones negros y botas deportivas blancas, acompañado de la leyenda "*la persona más popular de España está dejando de decir te huelen los pies*". El actor alegaba que la publicación pretendía aprovecharse de su renombre siendo que esta incorporaba la combinación de dos elementos: (i) la particular forma en que se vestía en sus apariciones televisivas, y (ii) el hecho de que había compuesto e interpretado una canción llamada "Me huelen los pies". El juez de primera instancia desestimó la demanda basándose en que *"el dibujo en blanco y negro utilizado en la publicidad no responde al concepto legal y jurisprudencial de imagen, concebida como 'una figura humana plenamente identificable y reconocible, todo lo cual dimana de la personalidad misma'"*. Por su parte, el Tribunal de segunda instancia entendió que los hechos constituían una *"intromisión ilegítima consistente en el uso comercial, no autorizado, del nombre, voz e imagen de otra persona. Y ello por entender que del conjunto de los elementos incorporados a la publicidad emitida por la demandada resulta plenamente identificada la figura del demandante mediante el empleo de elementos que promueven e invitan a la confusión con el original"*. Sin perjuicio de ello, ante el recurso de casación presentado por la empresa demandada, el Tribunal Supremo resolvió que el dibujo incluido en la publicidad, por ser una reproducción gráfica realizada con computadora, no era suficiente para actuar por sí solo como elemento identificador de una persona. La actora una vez más recurrió el decisorio alegando que *"en el anuncio controvertido queda plenamente identificada la figura del recurrente sin necesidad de haber reproducido su cara o utilizar su nombre y que* ***al tratarse de la utilización comercial de la imagen, el objeto de protección no es la imagen en su sentido estricto, sino la identidad personal puesto que en casos de personajes famosos no es necesario utilizar sus rasgos físicos identificadores para que esa persona pueda ser reconocida****"*. No obstante, estos argumentos no fueron suficientes para convencer al Tribunal Constitucional quien desestimó el recurso presentado por el Sr. Álvarez. Véase Emilio Aragón Álvarez c/ Proborín, S.L., Sentencia Constitucional Nº 81/2001, Tribunal Constitucional de España Sala Segunda, Recurso de amparo 922/1998 (26 de marzo de 2001). El resaltado me pertenece.

poseían una intensidad identificatoria suficiente[19] para justificar la protección reclamada. Sin parámetros claros, la interpretación del concepto de imagen y su alcance se convierte en un análisis completamente subjetivo, que se encuentra muy lejos de otorgar seguridad jurídica al titular de derecho.

La cuestión de la recognoscibilidad aparece como elemento fundamental a la hora de determinar si existe una violación al derecho a la imagen de una persona[20]. En el caso *Cohen v. Herbal Concepts* la Corte de Apelaciones de Nueva York ha establecido que la legislación en materia de derecho a la imagen del Estado de Nueva York[21], la cual protege el uso no autorizado del nombre, retrato, imagen o voz de una persona con fines comerciales*, "está diseñada para proteger la identidad de una persona, no simplemente un derecho de propiedad sobre su "nombre", "retrato" o "imagen", y por lo tanto requiere implícitamente que el demandante sea capaz de ser identificado a partir del material objetado"*[22].

En nuestro país los magistrados también se han expedido sobre este requisito. En el caso *Hess Mariana Beatriz c/ Hagelstron Josefina y otros s/ daños y perjuicios* el Tribunal dejó en claro que para que exista vulneración del derecho a la imagen, la persona debe poder ser identificada. *"Debe ser fácilmente reconocible la persona de que se trata, aunque la semejanza no sea perfecta"*[23]. Por su parte, la Sala K de la Cámara Nacional de Apelaciones en lo Civil ha manifestado que *"[e]l reconocimiento de la imagen no depende*

[19] De La Cuadra, B. (5 de abril de 2001). Emilio Aragón, Desamparado. *El País.* https://elpais.com/diario/2001/04/06/agenda/986508006_850215.html

[20] La actriz Lindsay Lohan demandó a los desarrolladores de videojuegos Take-Two Interactive Software, Inc. y Rockstar Games por el uso indebido de su imagen y semejanza en el videojuego "Grand Theft Auto V" (GTAV). El reclamo se centraba en el personaje de 'Lacey Jonas' quien la actriz alegaba estaba basado en su persona debido a las similitudes de las características físicas del personaje, los detalles mencionados en el juego respecto al perfil del mismo, como así también la vestimenta y la pose con la que figuraba en la portada del juego –que según la actora replicaban una fotografía suya–. La Corte de Apelaciones de Nueva York finalmente decidió en contra de la Sra. Lohan. El *a quo* se centró en el análisis de la representación del mencionado personaje, procurando determinar si este era reconocible como la Sra. Lohan o no, y determinó que *"el personaje de Jonas simplemente no es reconocible como el demandante ya que es simplemente una representación artística genérica de una mujer de "veinte y tantos años" sin ninguna característica física particular que la identifique. […] son representaciones no distintivas y satíricas del estilo, la apariencia y la personalidad de una joven moderna que va a la playa. No se disputa que los demandados no se refirieron a la demandante en GTAV, no usaron su nombre en GTAV y no usaron una fotografía de ella en ese juego […] Además, las representaciones ambiguas en cuestión no son más que comentarios culturales que no son reconocibles como la demandante y, por lo tanto, no son procesables según el artículo 5 de la Ley de Derechos Civiles"*. Véase Lohan v. Take-Two Interactive Software, Inc., 73 N.Y.S.3d 780, 97 N.E.3d 389, 2018 N.Y. Slip Op. 2208, 31 N.Y.3d 111 (N.Y. 2018). La traducción es propia.

[21] New York Civil Rights Law §§ 50- 51

[22] Cohen v. Herbal Concepts (1984). La traducción es propia.

[23] Cámara Nacional de Apelaciones en lo Civil. Sala L. 47711/2013. Hess Mariana Beatriz c/ Hagelstron Josefina y otros s/ daños y perjuicios. 2 de diciembre de 2022.

de la expresa mención del nombre y apellido de la persona involucrada en la publicación periodística. Ello debe juzgarse de modo objetivo, atendiendo a la naturaleza de la fotografía, que al no tratarse de una persona pública, debe predicarse únicamente con relación a sus familiares, conocidos y allegados y a la razonable probabilidad de que esa información pueda llevar a que alguien vinculado a su entorno familiar o social lo reconozca"[24].

En el ámbito regulatorio, la protección del derecho a la imagen varía de país en país. Según los datos recabados, la mayoría de las legislaciones prevén directa o indirectamente la protección de la imagen de una persona, sin embargo, los pormenores de dicha protección varían en cada jurisdicción. Como se detalla a continuación, en algunos países la protección de este derecho fundamental se encuentra prevista en la Constitución Nacional, en otros en el Código Civil y en algunos otros en las normativas relacionadas a propiedad intelectual.

2.1. Regulación del derecho a la imagen en Argentina

En Argentina el derecho a la imagen se encuentra expresamente previsto en la ley. Originalmente, la protección de este derecho se encontraba exclusivamente en la Ley N° 11.723 Régimen Legal de la Propiedad Intelectual. Esta norma prevé en su artículo 31 la necesidad del consentimiento expreso para la comercialización del retrato fotográfico de una persona, previendo la libre disposición de este cuando se tratase de usos para "*fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público*"[25], y establece claramente que el consentimiento otorgado puede ser revocado.

Sin perjuicio de lo anterior, si bien el derecho a la imagen no está expresamente receptado en nuestra Constitución Nacional, la Corte Suprema de Justicia de la Nación entendió en el fallo *Ponzetti de Balbín, Indalia y otro c. Editorial Atlántida S.A.*[26] que el derecho a la privacidad e intimidad previsto en el artículo 19 se extiende a la imagen[27].

[24] Cámara Nacional de Apelaciones en lo Civil. Sala K. 66872/2018. De La Fuente, Rodrigo Fernando c/ Artear S.A. s/ daños y perjuicios. 16 de marzo de 2021.
[25] Ley 11.723 Régimen Legal de la Propiedad Intelectual (1933). Artículo 31.
[26] Corte Suprema de Justicia de la Nación Argentina. Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A. s/ Daños y Perjuicios. 11 de diciembre de 1984.
[27] *"En rigor, el derecho a la privacidad comprende no sólo a la esfera doméstica, el círculo familiar y de amistad, sino a otros aspectos de la personalidad espiritual o física de las personas totales como la integridad corporal o la imagen y nadie puede inmiscuirse en la vida privada de una persona ni violar áreas*

Por otro lado, el ya no tan nuevo Código Civil y Comercial de la Nación (CCyC) amplía la protección prevista en la Ley 11.723, cuando en su artículo 53 establece la necesidad de contar con el consentimiento de una persona para "captar o reproducir" su imagen o voz. En la misma línea que la Ley 11.723, este artículo establece algunas excepciones al derecho a la imagen. En particular el consentimiento del titular no será necesario cuando se trate de una persona que participe en actos públicos, cuando exista un interés científico, cultural o educacional prioritario, y se procure no causar al titular un daño innecesario, y cuando se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.

La protección de este derecho trasciende la vida del titular de la imagen, ya que se prevé que una vez fallecida la persona el consentimiento para su uso recae sobre sus herederos[28] o la persona designada a tal efecto[29]. Sin embargo, este derecho no es infinito, tanto la Ley 11.723 como el CCyC establecen un límite temporal para la protección de la imagen. La primera de manera indirecta, mientras que el segundo incluye en el citado artículo un plazo expreso de vigencia de dicho derecho al establecer que la reproducción no ofensiva de la imagen de una persona es libre luego de trascurridos veinte años de su fallecimiento.

Considerando la naturaleza de este derecho y su conexión a otros derechos personalísimos como los mencionados anteriormente, se destacan algunas otras previsiones del CCyC argentino que vale la pena mencionar. Entre ellas podemos considerar por ejemplo el artículo 52 del CCyC que refiere a las afectaciones a la dignidad, estableciendo que quien de cualquier modo resulte menoscabado en su dignidad personal –mencionando expresamente las lesiones a la imagen– puede reclamar la prevención y reparación de los daños sufridos. En materia de reparación, los artículos 1.740 y 1.770 CCyC establecen que cuando se ve afectado el honor, la intimidad, o la identidad personal, en adición a la restitución o compensación del daño, el juez puede además, a pedido de parte, ordenar la publicación de la sentencia o de sus partes pertinentes.

de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ellos […]". Ponzetti de Balbín, Indalia y otro c/ Editorial Atlántida S.A. (1984).

[28] El artículo 31 de la Ley 11.723 prevé que muerto el titular de la imagen, el consentimiento para el uso de su imagen deberá ser concedido por su cónyuge e hijos o descendientes directos de estos, o en su defecto, del padre o de la madre. Faltando estos, o los descendientes directos de los hijos, la publicación sería libre.

[29] El artículo 53 del CCyC establece que "*[e]n caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el causante en una disposición de última voluntad. Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez*".

2.2. Regulación del derecho a la imagen en Latinoamérica

Como se mencionó anteriormente, la protección del derecho a la imagen en los países de la región varía según la jurisdicción. En el Cuadro 1 debajo se puede observar un detalle de las normativas locales de varios países de Latinoamérica en materia de derecho a la imagen, como así también una pequeña referencia a su contenido.

Cuadro 1: protección del derecho a la imagen en América Latina.

País	Normativa aplicable	Año	Disposiciones especificas	Excepciones
Argentina	Artículo 31 de la Ley 11.723 Régimen Legal de la Propiedad Intelectual	1933	El retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona. Este consentimiento es revocable.	Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público.
	Artículo 53 del Código Civil y Comercial de la Nación	2014	Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, salvo en los casos expresamente previstos por la ley. Pasados 20 años desde el fallecimiento de la persona, la reproducción no ofensiva de su imagen es libre.	No es necesario el consentimiento en los siguientes casos: a) que la persona participe en actos públicos; b) que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario; c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.
	Artículo 55 del Código Civil y Comercial de la Nación	2014	En relación con los derechos personalísimos, establece que el consentimiento no se presume, es de interpretación restrictiva y libremente revocable.	-
Brasil	Artículo 5 incisos V, X y XXVIII de la Constitución Política de la República Federativa del Brasil	1988	La imagen de las personas es inviolable, asegurándose el derecho de respuesta e indemnización ante su violación. La norma asegura la protección de las participaciones individuales en obras colectivas y de la reproducción de la imagen y voz humanas.	-
Chile	Artículo 19 N° 4 de la Constitución Política de la República de Chile	1980	La jurisprudencia ha interpretado que el artículo 19 de la Constitución Nacional, referido al derecho a la honra y a la vida privada, aplica al derecho a la imagen de manera tal que este debe interpretarse como un derecho personalísimo.	-
Colombia	Artículos 36 y 87 de la Ley 23 sobre Derechos de Autor	1982	Derecho de toda persona a oponerse a que su busto o retrato se exhiba o exponga en el comercio sin su consentimiento expreso. Este consentimiento es revocable.	La publicación del retrato es libre cuando se relaciona con fines científicos, didácticos o culturales en general o con hechos o acontecimientos de interés público o que se hubieren desarrollado en público.
México	Artículo 87 de la Ley Federal del Derecho de Autor	1996	El retrato de una persona sólo puede ser usado o publicado, con su consentimiento expreso. Este consentimiento es revocable.	No será necesario el consentimiento cuando se trate del retrato de una persona que forme parte menor de un conjunto o la fotografía sea tomada en

			Prevé que la protección de los derechos de la persona retratada se extiende por un plazo de 50 años luego de su fallecimiento.	un lugar público y con fines informativos o periodísticos.
Paraguay	Artículo 33 de la Constitución de la República de Paraguay	1992	Se garantiza el derecho a la imagen privada de las personas.	-
Perú	Artículo 2 inciso 7 de la Constitución Política del Perú	1993	Toda persona tiene derecho a la voz e imagen propias.	-
	Artículo 15 del Código Civil del Perú	1984	La imagen y la voz de una persona no pueden ser aprovechadas sin autorización expresa de ella.	No es necesario consentimiento cuando la utilización de la imagen y la voz se justifique por la notoriedad de la persona, por el cargo que desempeñe, por hechos de importancia o interés público o por motivos de índole científica, didáctica o cultural y siempre que se relacione con hechos o ceremonias de interés general que se celebren en público. No rigen estas excepciones cuando la utilización de la imagen o la voz atente contra el honor, el decoro o la reputación de la persona a quien corresponden.
Uruguay	Artículos 7, 72 y 332 de la Constitución de la República Oriental del Uruguay	1967	Su protección deriva implícitamente de los artículos citados, los cuales plantean la protección de los derechos inherentes a la personalidad humana sin limitación a los derechos expresamente reconocidos en la Constitución.	-
	Artículo 21 de la Ley 9.739 de Derechos de Autor	1937	El retrato de una persona no podrá ser puesto en el comercio sin el consentimiento expreso de la persona misma. Este consentimiento es revocable.	Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y, en general, culturales o con hechos o acontecimientos de interés público, o que se hubieren realizado en público.

Fuente: elaboración propia en base a la normativa de cada país.

Se puede observar que no todos los países analizados amparan expresamente el derecho a la imagen, en algunos la protección de la imagen deriva de una interpretación amplia de otros derechos de la personalidad, como es el caso de Chile. En aquellos donde sí se lo regula expresamente se destaca que no hay uniformidad en su tratamiento, en algunos casos la protección de la imagen de la persona se prevé en la Constitución Nacional (Brasil, Paraguay, Perú) o el Código Civil (Argentina, Perú); en otros casos está receptado en la norma local referida al derecho de autor (Argentina, Colombia, México, Uruguay); e incluso hay jurisdicciones que hacen referencia a este derecho en más de un cuerpo normativo (Argentina, Perú, Uruguay). En líneas generales, los países analizados establecen que la reproducción de la imagen de una persona requiere de su consentimiento.

La mayoría de las jurisdicciones estudiadas prevén expresamente ciertas excepciones al derecho a la imagen, es decir, escenarios en los cuales la imagen de una persona puede ser utilizada o reproducida sin requerir su consentimiento. Esto suele estar ligado al tipo de uso que se pretende hacer de la imagen, como por ejemplo en aquellos casos en los que el uso o reproducción se realiza con fines educativos, científicos o culturales (Argentina, Colombia, Perú, Uruguay) o cuando dicho uso está relacionado a la información de acontecimientos de interés público (Argentina, Colombia, México, Perú, Uruguay). Sin perjuicio de las excepciones establecidas en cada norma, en todos los casos se debe respetar la órbita privada del titular de la imagen.

Resulta interesante destacar el artículo 87 de la Ley Federal del Derecho de Autor de México, el cual hace mención expresa a la explotación económica de la imagen de una persona y establece que el pago de una remuneración permite presumir que el titular del derecho ha prestado su consentimiento para ser retratado. A diferencia de lo establecido en otras jurisdicciones, dicho consentimiento no puede ser revocado siempre que el uso realizado se encuentre dentro de los términos y fines pactados.

2.3. Regulación del derecho a la imagen en Europa

Aunque sin uniformidad, la mayor parte de los países europeos analizados (ver Cuadro 2) prevén expresamente, ya sea en sus normas de fondo o en leyes particulares, algún grado de protección del derecho a la imagen.

En algunos países, se replica la estructura observada en Latinoamérica respecto a la variedad de instrumentos legales en donde se encuentra receptado este derecho, y se detecta una diferencia en el hecho que las legislaciones europeas en general no suelen establecer excepciones al uso de la imagen personal.

España pareciera tener una protección más amplia, siendo el único país analizado que posee una ley específica de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen[30].

El Reino Unido amerita una mención especial ya que su situación es un tanto particular. Los tribunales de este país han dejado en claro que *"[e]n la legislación inglesa no existe ningún 'derecho a la imagen' ni 'derecho a la personalidad' que permite a una*

[30] Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

celebridad controlar el uso de su nombre o imagen"[31]. En este territorio, la protección de la imagen personal debe darse por alguna vía alternativa, como puede ser en relación con el derecho a la privacidad e intimidad, en materia de competencia desleal (*passing off*), incumplimiento contractual o mediante la aplicación de algún derecho de propiedad intelectual (como marca o derecho de autor). En el caso de los actores Michael Douglas y Katherine Zeta-Jones contra la revista inglesa 'Hello!' por el uso de fotografías de su boda[32], el tribunal dejó en claro que "*[a]unque la situación es diferente en otras jurisdicciones, según la ley inglesa no es posible que una celebridad reclame un monopolio sobre su imagen, como si se tratara de una marca registrada o de hecho. Nadie (ya sea una celebridad o no) tampoco puede quejarse simplemente de ser fotografiado. Debe haber algo más […]*"[33].

En el derecho inglés la concepción de la imagen es completamente distinta a lo observado en otros países del mundo. En más de una ocasión el tribunal de primera instancia ha dejado en claro que en Inglaterra no hay propiedad sobre la imagen de una persona y que su consideración se limita a efectos tributarios, siendo que esta debe concebirse como bien de capital y, como tal, pensarse como una especie de propiedad[34].

Cuadro 2: protección del derecho a la imagen en Europa.

País	Normativa aplicable	Año	Disposiciones especificas	Excepciones
Alemania	Artículos 1 y 2 de la Ley Fundamental para la República Federal de Alemania	1949	La protección del derecho a la imagen deriva de los artículos referidos a la protección de la dignidad humana y la libertad.	-
	Sección 60 de la Ley de Derechos de Autor y Derechos Conexos	1965	Se prevé expresamente el derecho de reproducción y distribución de un retrato sin pago y sin fines comerciales por parte del retratado o quien lo haya encargado, y sus derechohabientes. En caso de que se trate de una obra artística, dicha explotación está limitada a formato fotográfico.	Aplican las excepciones generales establecidas por la Ley para el uso de obras con fines educativos, científicos, informativos, entre otros.
España	Artículo 18 de la Constitución Española	1978	Se garantiza el derecho a la propia imagen.	-

[31] Fenty v Arcadia Group Brands Ltd. Tribunal de Apelación de Inglaterra y Gales, División Civil 3 (22 de enero de 2015), párrafo 29. La traducción es propia.
[32] Douglas & ors v Hello! Ltd & ors (No 3). Cámara de los Lores KHL 21 (2 de mayo de 2007).
[33] Douglas v Hello! Ltd (2007). La traducción es propia.
[34] Sports Club plc v Inspector of Taxes. Special Commissioners STC (SCD) 443 (8 de junio de 2000); Hull City (AFC) Tigers Limited v The Commissioners for HMRC. United Kingdom First Tier Tribunal (Tax Chamber) 227 (22 de marzo de 2019).

	Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen	1982	El derecho a la propia imagen es irrenunciable, inalienable e imprescriptible. La ley considera intromisiones ilegítimas: (i) la captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos (salvo excepciones expresamente previstas por la norma); y (ii) la utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.	El derecho a la propia imagen no impedirá: a) su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público. b) la utilización de la caricatura de dichas personas, de acuerdo con el uso social. c) la información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.
Francia	Artículo 9 del Código Civil francés	1803	La protección del derecho a la imagen deriva del artículo 9 del Código Civil que regula el derecho a la privacidad.	-
	Artículos 226-1 y 226-8 del Código Penal francés	1990	Castiga la fijación, grabación o transmisión de la imagen de una persona ubicada en un lugar privado, sin su consentimiento. Cuando dicha fijación, grabación o transmisión se hubiere realizado a la vista del titular de la imagen sin que se opusiera a ello, se presume su consentimiento. Asimismo, se castiga el hecho de publicar, por cualquier medio, el montaje realizado con las palabras o la imagen de una persona sin su consentimiento, si no es evidente que se trata de un montaje o si no se lo indica expresamente.	-
Italia	Artículo 10 del Código Civil italiano	1942	Si la imagen de una persona ha sido exhibida o publicada fuera de los casos en que la exhibición o publicación está permitida por la ley, o en perjuicio del decoro o reputación de la propia persona, la autoridad judicial, a petición del interesado, podrá ordenar el cese del abuso, previa indemnización de daños y perjuicios.	-
	Artículos 96 y 97 de la Ley N° 633 sobre la Protección del Derecho de Autor y los Derechos Conexos	1941	El retrato de una persona no puede exhibirse, reproducirse ni comercializarse sin su consentimiento.	No se requiere el consentimiento de la persona retratada cuando la reproducción de la imagen sea justificada por la notoriedad o por el cargo público desempeñado, por la necesidad de justicia o de policía, con fines científicos, educativos o culturales, cuando la reproducción esté vinculada a hechos, eventos, ceremonias de interés público o celebradas en público.
Reino Unido	Artículo 8 de la Convención Europea de Derechos Humanos (incorporada a		No existe una norma expresa que lo prevea. Supletoriamente puede aplicarse la Convención Europea en lo referido al derecho al respeto a la vida privada y familiar y las normas de	-

	la legislación del Reino Unido mediante la Ley de Derechos Humanos de 1998)		competencia desleal (*passing off*).	

Fuente: elaboración propia en base a la normativa de cada país.

2.4. Regulación del derecho a la imagen en Estados Unidos

En Estados Unidos los derechos de la personalidad suelen enfocarse en dos tipos de derechos: el derecho a la intimidad y el derecho de publicidad. A diferencia de lo que se observa en países con tradición civil, el derecho estadounidense se ha centrado en la protección económica del titular de la imagen.

El derecho de publicidad o *"right of publicity"* norteamericano (ROP) "*proporciona a las personas una causa de acción contra cualquiera que haga un uso comercial de su nombre, imagen, semejanza u otros indicios de identidad"*[35]. Esta concepción del ROP, de manera individual separado sobre todo del derecho a la intimidad, surge a raíz del caso *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*[36] de 1953.

Se trata de un derecho de propiedad de nivel estadual, por lo que su regulación queda sujeta a lo que establezca cada estado en particular. Algunos estados poseen legislaciones especificas en materia de derecho de publicidad, mientras que otros se apoyan en el derecho consuetudinario cuando emergen conflictos de esta índole. Actualmente cerca de treinta estados[37] cuentan con instrumentos legales específicos en materia de derecho de publicidad, siendo Nueva York y Luisiana los últimos en actualizar su normativa en esta materia.

En el año 2020 se aprobó el proyecto de ley[38] para incorporar a la Ley de Derechos Civiles del Estado de Nueva York la sección 50f dentro del artículo 5 referido al derecho a la privacidad. Antes de esta reforma, el derecho de publicidad estaba receptado de manera indirecta mediante la aplicación de las previsiones referidas al derecho a la privacidad, la cual establece la posibilidad de accionar ante el uso no autorizado del retrato

[35] Johnson, E. E. (2017). Disentangling the right of publicity. *Northwestern University Law Review*, 111(4), 891-944. Pág. 893. La traducción es propia.
[36] Haelan Labs., Inc. v. Topps Chewing Gum, Inc. 202 F.2d 866. Corte de Apelaciones de los Estados Unidos Segundo Circuito. (16 de febrero de 1953).
[37] Conforme informa el sitio web https://rightofpublicity.com/statutes
[38] Senate Bill S5959D. 2019-2020 Legislative Session (New York 2020) https://www.nysenate.gov/node/7125177

o de la imagen de una persona con fines publicitarios o comerciales. Uno de los grandes cambios que trae la sección incorporada por la reforma es la sobrevivencia de los derechos de publicidad una vez fallecido el titular de la imagen, aunque limitándolo solamente a la imagen de personalidades o intérpretes.

Más recientemente, en agosto de 2022 entró en vigencia en el estado de Luisiana una nueva normativa en materia de derecho de publicidad[39]. Hasta entonces, no existían en este territorio acciones específicas referidas a la protección del uso no autorizado de la imagen. Esta nueva ley establece expresamente que cada individuo tiene un derecho de propiedad con relación al uso con fines comerciales que haga de su identidad, la cual define como el nombre, la voz, la firma, la fotografía, la imagen, la semejanza o la réplica digital de un individuo.

California y Nueva York suelen ser los estados más actualizados en materia de derecho de publicidad[40], debido a que son el epicentro de la industria del entretenimiento del país y donde residen gran parte de las celebridades que suelen verse afectadas por el abuso de su imagen y semejanza. Las cortes norteamericanas, en particular en el estado de California, han aplicado una concepción amplia de la imagen con relación al derecho de publicidad, incluso más amplia que la observada en otras jurisdicciones. La profesora Jennifer Rothman, especialista en la materia, explica[41] que la protección del derecho de publicidad se ha expandido hasta cubrir también lo que caracteriza como la *"persona"* y dice que las acciones fundadas en este derecho estaban inicialmente limitadas a situaciones en las que se usara el nombre o semejanza de un individuo. Esta última abarca tanto una imagen real, por ejemplo una fotografía, como así también las recreaciones de la apariencia, por ejemplo mediante dibujos. Mientras que el concepto de *"persona"* hace referencia a un uso que no requiere ya de la presencia expresa del nombre o semejanza del sujeto, sino que basta con que el uso genere en el espectador un recuerdo del titular de derecho. Esto ha dado lugar a reclamos basados por ejemplo en personajes ficticios, donde el consumidor asocia la imagen de un actor con la del rol que ha interpretado[42].

[39] Allen Toussaint Legacy Act, SB 426, Louisiana State Legislature 2022 Regular Session. https://legiscan.com/LA/bill/SB426/2022

[40] Engler, J., & Love, M. (28 de junio de 2022). *New Allen Toussaint Legacy Act creates a right of publicity in Louisiana.* Louisiana Law Blog. https://www.louisianalawblog.com/intellectual-property/new-allen-toussaint-legacy-act-creates-a-right-of-publicity-in-louisiana/

[41] Rothman, Jennifer E., The Inalienable Right of Publicity (12 de noviembre de 2012). 101 Georgetown Law Journal 185 (2012), Loyola-LA Legal Studies Paper No. 2012-46. https://ssrn.com/abstract=2174646

[42] Rothman (2012).

Los doctrinarios norteamericanos han sido muy críticos de la forma en que este derecho ha sido aplicado por las cortes. Eric Johnson, profesor de derecho en *University of North Dakota School of Law*, plantea[43] que uno de los errores de las cortes ha sido definir al ROP de manera negativa, es decir, estableciendo repetidas veces lo que este derecho no es, en lugar de arriesgarse a definir los parámetros que lo delimitan. Según Johnson, quien ha estudiado los distintos casos que han aplicado este derecho a lo largo de los último sesenta años, el ROP tiene tres aristas: (i) un derecho de endoso (*"endorsement"* en inglés) o apoyo, (ii) un derecho a comercializar artículos de promoción (*"merchandizing"*), y (iii) un derecho contra la personificación virtual. Los tres tienen un claro enfoque comercial, distinto de lo que se presenta en los países de tradición civil, donde, como ya se ha comentado, el derecho a la imagen ha estado tradicionalmente vinculado a otros derechos personalísimos.

2.5. Regulación internacional del derecho a la imagen

En el plano internacional hay una gran deuda en este sentido. Los instrumentos internacionales más importantes no hacen mención alguna a este derecho, sino que se enfocan más bien en la protección de la intimidad de las personas. Así el artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 5 de la Declaración Americana de Derechos y Deberes del Hombre, los artículos 14.1 y 17 del Pacto Internacional de Derechos Civiles y Políticos, y el artículo 11 del Pacto de San José de Costa Rica, se refieren a la vida privada de la persona, de su familia, a su domicilio y/o su correspondencia, a la honra y a la reputación, pero no hacen mención específica al derecho a la imagen[44]. Si bien la Corte Interamericana de Derechos Humanos ha interpretado de manera amplia el artículo 11 del Pacto de San José de Costa Rica[45], el derecho a la imagen aún no ha sido mencionado.

2.6. Protección penal de la imagen personal

Adicionalmente, en el ámbito penal podemos observar previsiones en materia de protección de la imagen personal. Se destaca el caso de Francia, cuyo Código Penal incluye en el Capítulo que regula los "ataques a la personalidad" dos secciones que

[43] Johnson (2017).

[44] Gómez, F. L. (2013). El derecho a la imagen de niños, niñas y adolescentes en Chile. Una mirada crítica a la luz del derecho internacional de los derechos humanos y de los estatutos normativos iberoamericanos de protección integral de la infancia y de la adolescencia. *Revista Chilena de Derecho*, *40*(3), 929–952. http://www.jstor.org/stable/23729644

[45] Véase Tristán Donoso vs. Panamá. Corte Interamericana de Derechos Humanos (27 de enero de 2009); Escué Zapata vs. Colombia. Corte Interamericana de Derechos Humanos (4 de julio de 2007).

resguardan expresamente el derecho a la imagen de una persona. Una de ellas está relacionada a la protección de la órbita privada[46] y tipifica la violación de la intimidad mediante toda acción que capte, fije, grabe o transmita, sin consentimiento del titular de derecho, sus palabras o imagen cuando este se encontrare en un entorno privado[47]. La otra sección trata los delitos relacionados a la representación de la persona, en particular se castiga la publicación por cualquier medio de montajes o ediciones que utilizan la imagen o las palabras de una persona sin su consentimiento, siempre que no resulte evidente que se trata de un montaje o edición o no se lo mencione expresamente[48].

En la misma línea, el Código Penal alemán en su División 15 incluye un artículo que refiere expresamente a la violación de la intimidad y de los derechos de la personalidad mediante fotografías u otras imágenes[49]. Este pena la creación o transmisión no consentida de fotografías u otras imágenes de una persona en un espacio privado que afecten la intimidad u honra del retratado. Se pena asimismo la puesta a disposición no consentida de estas imágenes, incluso cuando ellas hubieran sido obtenidas con autorización del titular de derecho. Esta protección se extiende a las personas fallecidas y encuentra su límite cuando se trata de actividades realizadas en el ejercicio de intereses legítimos superiores, como el uso con fines culturales, educativos, informativos o de investigación.

En otras legislaciones, como España y varios países de América Latina, las previsiones en materia de protección de la imagen están atadas a aquellas que resguardan la órbita privada de la persona. Así, por ejemplo, en Chile se castiga a quien por cualquier medio y sin autorización del afectado capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público, como así también su difusión[50]. De manera similar, en Perú se pena a quien viole la intimidad de la vida personal o familiar mediante el registro de imágenes[51]. La legislación paraguaya en adición a un artículo referido a la protección de la intimidad[52], incluye en particular un artículo relacionado a la lesión de la imagen, penando a quien, sin consentimiento del afectado, produjera o

[46] Código Penal, parte legislativa. Capítulo VI, Sección 1: Invasión de la privacidad. 1° de enero de 2014 (Francia).
[47] Código Penal (Francia, 2014). Artículo 226-1.
[48] Código Penal (Francia, 2014). Artículo 226-8.
[49] Código Penal. Sección 201a. 13 de noviembre de 1998 (Alemania).
[50] Código Penal. Artículo 161 A. 12 de noviembre de 1874 (Chile).
[51] Código Penal. Artículo 154. 3 de abril de 1991 (Perú).
[52] Código Penal. Artículo 143. Ley N° 1.160/97. 26 de noviembre de 1997 (Paraguay).

transmitiera imágenes de otra persona dentro de su recinto privado, del recinto privado ajeno, o de otra persona fuera de su recinto violando su derecho al respeto del ámbito de su vida íntima[53]. Por su parte, el Código Penal español también destina un artículo a la regulación de actividades delictivas relacionadas al derecho a la propia imagen, castigando a quien *"sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona"*[54].

En nuestro caso, el Código Penal de la Nación Argentina carece completamente de normas destinadas a la protección de la imagen personal, es más, ni siquiera prevé como en los casos mencionados anteriormente, penas contra la violación de la órbita privada de las personas, a excepción de un capítulo destinado al resguardo de la información privada[55]. El proyecto de reforma del Código Penal, que ingresó al Congreso en 2019[56], propone la tipificación de la pornovenganza[57] que, al menos en determinadas situaciones, provee de mayores herramientas para defender la imagen personal.

2.7. El particular caso de la Isla de Guernsey

De todos los países estudiados, se destaca el particular caso de la Isla de Guernsey, una isla ubicada en el Canal de la Mancha dependiente de la Corona británica. En el año 2012 se inauguró en Guernsey el primer registro de derechos de imagen, sentando las bases para el desarrollo de un nuevo derecho de propiedad intelectual.

Similar al registro marcario, el registro de derecho de imagen de Guernsey pretende otorgar a los titulares de derechos una herramienta para gestionar de manera directa un nuevo activo con posibilidades de explotación comercial: su imagen personal.

[53] Código Penal (Paraguay, 1997). Artículo 144.
[54] Código Penal. Artículo 197, 7. Ley Orgánica 10/1995. 23 de noviembre de 1995 (España).
[55] Código Penal de la Nación Argentina. Capítulo III Violación de Secretos y de la Privacidad. Ley N° 11.179. 30 de septiembre de 1921 (Argentina).
[56] *El proyecto del Código Penal ya ingresó al Congreso.* (26 de marzo de 2019). Argentina.gob.ar. https://www.argentina.gob.ar/noticias/codigo-penal-congreso
[57] Según define el sitio argenitna.gob.ar, la pornovenganza es *"la difusión no consentida de imágenes o videos íntimos en redes sociales, servicios de mensajería instantánea o cualquier tipo de medio social donde se comparte información"*. Véase *¿Qué es la pornovenganza y cómo me protejo?* (Marzo 2024). Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-y-como-protegerse-de-la-pornovenganza

El sitio web de la Oficina de Propiedad Intelectual de Guernsey[58] explica: *"[l]os derechos de imagen son la expresión de una personalidad en el dominio público. La disposición legal de los derechos de imagen permite la definición, valor, explotación comercial y protección de los derechos de imagen asociados a una persona. La legislación sobre derechos de imagen de la Bailía de Guernsey permite a un personaje registrar su personalidad (y los derechos que subsisten dentro de esa personalidad). El derecho de imagen se convierte en un derecho de propiedad susceptible de ser protegido por la legislación mediante el registro. El registro permite proteger, licenciar y ceder el derecho de imagen"*.

Surge de esta definición un nuevo concepto acuñado por la legislación de Guernsey, el concepto de *"personnage"* o personaje, entendido por la novedosa legislación[59] como toda personalidad que sea objeto de una solicitud de registro o cuente con un registro otorgado y que represente:

(a) una persona física,

(b) una persona jurídica,

(c) dos o más personas físicas o jurídicas que estén o que públicamente se perciban como intrínsecamente vinculadas y que juntas tengan una personalidad conjunta ("personalidad conjunta"),

(d) dos o más personas físicas o jurídicas que estén o que públicamente se perciban que están vinculadas con un propósito común y que juntas formen un grupo o equipo colectivo ("grupo"), o

(e) un personaje ficticio humano o no humano ("personaje ficticio").

Lo interesante del registro establecido en Guernsey es que permite diferenciar la esfera personal del titular de la imagen, quizás mejor representado con el término "derecho a la imagen", de la esfera comercial de la imagen personal de un sujeto, lo que podría llamarse a fin de diferenciarlo del anterior, "derecho de imagen".

El *derecho a la imagen* protege la órbita personal del titular de derecho, está estrechamente vinculado con los derechos a la intimidad y la honra. Es un derecho

[58] Intellectual Property Office. (s. f.). *What are image rights.* Intellectual Property Office Serving the Bailiwick of Guernsey. https://ipo.guernseyregistry.com/article/103037/What-are-Image-Rights
[59] Ordenanza sobre derechos de imagen (2012). Bailía de Guernsey. Sección 1.

personalísimo y por lo tanto inherente a la persona misma. Por el contrario, esta nueva acepción de la imagen personal, orientada a su explotación comercial y quizás más cercana al ROP estadounidense, que podemos identificar como *derecho de imagen* tiene otra finalidad, diametralmente alejada de la intimidad y ajena a la honra, ya que mediante su comercialización el titular de derecho está consintiendo expresamente que su imagen personal sea usada con fines estrictamente comerciales, y si bien este uso se realizaría dentro de los parámetros establecidos por las partes y consentidos por su titular, su explotación sería ajena a este y saldría manifiestamente de su esfera de control.

La legislación de Guernsey ha sabido interpretar las necesidades del mercado moderno y ha creado una nueva herramienta para identificar un activo que emana de la personalidad, permitiendo mediante su registro individualizarlo a fin de poder diferenciarlo y comercializarlo. Como cuando en materia marcaria hablamos del carácter distintivo de los signos, el derecho de imagen viene a demostrar el carácter distintivo de un individuo[60] y su potencial comercial.

[60] Blackshaw, I. (2010). The island of Guernsey to introduce new IP image right. *The International Sports Law Journal*, (1-2), 135. https://www.asser.nl/media/2069/islj_2010-1-2.pdf

3. *Deepfakes* y la creación de réplicas digitales

En los últimos años hemos observado una rápida domesticación de la tecnología de alteración de imagen. Existen hoy numerosos softwares y aplicaciones móviles que permiten a los usuarios de manera fácil y rápida no sólo alterar las imágenes, videos y audios que deseen, sino también generar materiales completamente ficticios que repliquen la imagen o voz de personas reales. Si bien los usos de estas tecnologías pueden ser inocuos, como por ejemplo cuando son usados para imaginar cómo nos veríamos dentro de algunas décadas, también debemos ser conscientes que tienen potencial para causar daño, siendo usados por ejemplo para engañar, defraudar, suplantar identidades, difamar y desinformar.

3.1. ¿Qué son los *deepfakes*?

Uno de los máximos exponentes de este tipo de usos de las tecnologías es lo que se conoce como "*deepfakes*" o "ultras falsos". Este término se usa para identificar contenido (puede ser imágenes, videos, e incluso audios) creado mediante la aplicación de software de inteligencia artificial que altera o recrea de manera hiperrealista la imagen o la voz de una persona (real o no), el cual a simple vista aparenta ser auténtico cuando no lo es.

Estos contenidos son realizados aplicando softwares basados en mecanismos de *deep learning* (aprendizaje profundo) que utilizan algoritmos de redes neuronales artificiales, en particular redes generativas antagónicas (RGA o GAN por sus siglas en inglés), que en base a la información que se les provee analizan y reconocen patrones, y sin necesidad de ser programados, aprenden y se forman a sí mismos.

El término, compuesto por las palabras "*deep*" (derivado del concepto de *deep learning*¸ haciendo referencia a la tecnología usada) y "*fake*" (falso en inglés), comenzó a utilizarse en el año 2017 cuando un usuario de Reddit[61] publicó con este nombre una serie de videos pornográficos en los cuales había reemplazado con inteligencia artificial el rostro de las personas originalmente representadas con el de figuras reconocidas de la industria del entretenimiento como las actrices Gal Gadot, y Scarlett Johansson, y la cantante Taylor Swift.

[61] Reddit es una red social que funciona como un foro o agregador de contenido donde este es seleccionado y promovido por los usuarios.

Los *deepfakes* son sólo una arista de lo que se conoce como "*synthetic media*" o "medios sintéticos", término utilizado para describir videos, imágenes, textos o voces que han sido generados total o parcialmente mediante el uso de inteligencia artificial[62]. Este término se utiliza por oposición a "*non-synthetic media*" o "medios no sintéticos" que identifica aquel contenido generado con la intervención de un humano.

Los medios sintéticos nos permiten acceder a contenido a la carta, creado con instrucciones específicas y con un alto nivel de realismo que suele dificultar identificarlo como tal. Podemos distinguir distintos tipos de medios sintéticos:

- síntesis de imagen: permite generar cualquier tipo de imagen mediante el uso de algoritmos que crean contenido visual a partir de otras imágenes o incluso texto. Puede ser utilizado para hacer representaciones creíbles y realistas de personas reales o para crear imágenes de personas inexistentes, como así también para generar imágenes de animales, objetos o paisajes.
- síntesis de audio: permite generar cualquier sonido mediante la manipulación de ondas de audio, el cual podría imitar la voz humana, el sonido de instrumentos musicales, generar audio original o incluso alterar sonidos existentes. Tiene la capacidad de aprender patrones y estructuras en los sonidos, emular la voz de personas reales y reproducir acentos o entonaciones; y funciona en base a archivos de audio preexistentes o incluso texto. Recientemente la aplicación de estas tecnologías en la generación de música ha sido muy discutida[63].
- síntesis de texto: permite generar contenido escrito, aplicando herramientas de procesamiento del lenguaje natural (PLN o NLP por sus siglas en inglés) para

[62] Conforme define el sitio de la empresa Synthesia. *Ver* https://www.synthesia.io/glossary/synthetic-media#:~:text=is%20synthetic%20media%3F-,Synthetic%20media%20is%20a%20catch%2Dall%20term%20to%20describe%20video,generated%20using%20artificial%20intelligence%20algorithms.

[63] En abril de 2023 el usuario de TikTok 'ghostwriter' se viralizó por un video en dónde afirmaba haber utilizado inteligencia artificial para hacer una canción de los artistas Drake y The Weeknd, llamada "Heart on My Sleeve". El tema tuvo millones de reproducciones en varias plataformas, incluidas TikTok, YouTube y Spotify. Poco después de que la noticia comenzó a circular, la canción fue dada de baja tras que la empresa Universal Music Group, de los cuales ambos artistas son parte, presentara un reclamo. El evento despertó el interés no sólo del público, sino también de la industria musical y los versados en derecho de autor, disparando conversaciones sobre la legalidad de esta obra, la ética detrás de su creación y los riesgos de estas tecnologías. Véase Coscarelli, J. (19 de abril de 2023). An A.I. Hit of Fake 'Drake' and 'The Weeknd' Rattles the Music World. *The New York Times.* https://www.nytimes.com/2023/04/19/arts/music/ai-drake-the-weeknd-fake.html

generar texto y respuestas coherentes y fluidas símil a cómo lo haría un humano.

- síntesis de video: permite generar videos sin la intervención de sujetos u objetos físicos, como actores y cámaras u otros equipos de filmación. Pueden crearse videos que representen personas reales o no, escenarios del mundo real o completamente ficticios.

El mercado de software de creación y manipulación de medios sintéticos está en alza. En los próximos años se predice un crecimiento exponencial de estas tecnologías con una tasa de crecimiento compuesto anual (CAGR) esperado de más del 35% para el período 2023-2032[64]. Algunos de los programas más reconocidos hoy son Midjourney[65] para imágenes, Synthesia[66] para video y Jasper[67] para generación de texto. Otro de los más populares –y controvertidos– en el momento es ChatGPT[68] de la empresa OpenAI. La popularización de estas tecnologías y su proliferación en el mercado ha resultado en softwares más accesibles y sencillos, que permiten generar contenido de mayor calidad sin requerir conocimientos técnicos específicos.

3.2. Taxonomía de los *deepfakes*[69]

Es importante entender que no todos los *deepfakes* son iguales o requieren el mismo tratamiento, incluso cuando se trata de réplicas digitales realizadas sin consentimiento. A la hora de plantear una potencial regulación para este tipo de contenido, no se puede pretender aplicar las mismas consecuencias legales a la réplica digital de una celebridad haciendo un baile de TikTok[70] que a un caso de pornovenganza. Si bien en el presente trabajo se aboga por la necesidad de consentimiento para la utilización, reproducción y difusión de la imagen y semejanza de una persona, no todos los usos tienen los mismos efectos y existen derechos contrapuestos que deben ser tenidos en cuenta, como por ejemplo el derecho a la libertad de expresión. Las réplicas digitales pueden resultar ser una herramienta interesante y tener aplicaciones prácticas y útiles. El objeto

[64] *Global deepfake software industry trends analysis report 2024, forecast to 2032 (broken down by type, end user, regional analysis, and competitive landscape)*. (23 de noviembre 2023). Absolute Reports. https://www.absolutereports.com/global-deepfake-software-industry-25803343
[65] https://www.midjourney.com/home?callbackUrl=%2Fexplore
[66] https://www.synthesia.io/
[67] https://www.jasper.ai/
[68] https://chat.openai.com/
[69] Ullrich, Q. J. (2021). Is This Video Real? The Principal Mischief of Deepfakes and How the Lanham Act Can Address It. *Columbia Journal of Law & Social Problems*, *55*, 1.
[70] TikTok es una red social que permite grabar, editar y compartir videos cortos.

de una potencial regulación no debe ser su prohibición, sino más bien establecer parámetros claros para un uso adecuado y, sobre todo, consentido.

Es difícil establecer un estándar para determinar cuándo un contenido es inocuo y cuándo tiene potencial de generar daño, ya que su apreciación debe ser completamente subjetiva y ha de tener en cuenta las circunstancias que lo rodean. Una de las características principales de las réplicas digitales es su capacidad para parecer auténticas, generando en el espectador la convicción de que se trata realmente del sujeto retratado y no de una imagen sintética. Si bien ello dependerá en gran parte de la calidad del resultado final –al igual que una imagen mal editada, una réplica mal realizada advertiría inmediatamente al espectador respecto a su falsedad–, no podemos obviar que esa confusión tendrá un importante elemento subjetivo. Por ejemplo, cualquier fanático de la saga Star Wars probablemente haya identificado fácilmente que la participación póstuma de la actriz Carrie Fisher en el film 'Star Wars: Episodio IX - El ascenso de Skywalker' (2019)[71] se trataba de una recreación digital ya que conocía de su fallecimiento, sin embargo, la réplica digital resultante de la adaptación de escenas previamente grabadas y ajustadas mediante efectos especiales es tan convincente que un espectador promedio nunca cuestionaría su autenticidad.

No hay dudas que determinados usos de la imagen de una persona pueden tener efectos devastadores en su vida, como por ejemplo cuando una réplica digital es utilizada en material con tenor sexual o pornográfico. Pero no es necesario que el contenido sintético tenga estas características para generar daño, pensemos en un *deepfake* de un empresario consumiendo el producto de la competencia, su publicación podría costarle el trabajo independientemente de su veracidad o calidad.

Considerando lo anterior, es interesante realizar una taxonomía[72] de los distintos tipos de *deepfakes* que podemos encontrar, clasificándolos según los efectos que estos contenidos puedan tener sobre el titular de derecho. En este sentido podemos distinguir:

(a) Contenido que genera daño porque tiene la capacidad de confundir al espectador: se trata de réplicas digitales que por su calidad y realismo podrían confundir a un espectador promedio respecto a su veracidad, pensando este que

[71] Breznican, A. (30 de diciembre de 2019). An oral history of Carrie fisher's return in the rise of skywalker. *Vanity Fair*. https://www.vanityfair.com/hollywood/2019/12/carrie-fisher-oral-history-rise-of-skywalker-star-wars
[72] Ullrich (2021).

realmente se trata del sujeto representado realizando determinadas acciones o expresando determinadas opiniones.

(b) Contenido que genera daño a pesar de no generar confusión sobre su veracidad: el ejemplo típico viene dado por los orígenes de los *deepfakes*, la sustitución del rostro de figuras públicas en videos con contenido explícito. En estos casos no hay riesgo de confusión, ya que el espectador sospecha de su veracidad o incluso reconoce su falsedad. A pesar de ello, estas réplicas generan un enorme perjuicio para el titular de la imagen, incluso cuando lo único que se haya replicado sea su rostro e incluso cuando la ilusión generada no sea efectiva.

(c) Contenido que asocia la imagen de una persona con un producto (endoso o "*endorsement*"): esto es realmente un riesgo para las figuras públicas. El endoso de productos –o "*endorsement*" en inglés– puede representar una importante fuente de ingresos para las celebridades, y suele ser algo que estas manejan con cuidado, ya que su capacidad de venta está ligada a su perfil y credibilidad. Cuando las marcas asocian la imagen de una figura pública a sus productos sin su consentimiento, esto no sólo genera un aprovechamiento ilícito por parte del anunciante, sino que además podría generarle un perjuicio económico al titular de derecho al afectar su relación con aquellas marcas con las que tiene vínculo comercial y repercutir negativamente en su imagen pública.

(d) Contenido que genera un perjuicio económico para el titular de derecho: el perjuicio económico puede suceder también cuando la imagen o semejanza de una persona es usada, reproducida o difundida sin su consentimiento con fines comerciales (distintos al endoso). Por ejemplo la reproducción digital de un actor para su incorporación en un film, es evidentemente un uso de su imagen que debería ser remunerado y cuando no lo es genera un perjuicio económico para el titular de derecho. Aquí yace uno de los motivos en los que se centró el conflicto que sufrió Hollywood durante 2023, cuando el Sindicato de Actores de Cine - Federación Estadounidense de Artistas de Radio y Televisión (*Screen Actors Guild - American Federation of Television and Radio Artists* – SAG-AFTRA) se declaró en huelga. Uno de los puntos más

discutidos se enfocó en la preocupación de los intérpretes por la falta de control de sus réplicas digitales[73].

(e) Contenido inocuo realizado sin consentimiento del titular de derecho: este último caso refiere a aquellas réplicas digitales que pueden ser consideradas inofensivas, a pesar de haber sido realizadas sin autorización del titular de derecho. Estos suelen ser casos en lo que la falsedad del contenido es evidente, ya sea porque fue directamente divulgada –por ejemplo mediante la inclusión de marcas de agua o leyendas que indican que se trata de una réplica digital o *deepfake*– o resulte del contexto en el que se usan –por ejemplo cuando tienen un fin cómico o de parodia–. Por lo general se trata de usos que debido al tenor del contenido no generan daño alguno. Aquí podemos incluir por ejemplo a aquellas cuentas en redes sociales que a modo de parodia replican la imagen de celebridades y publican videos con fines de entretenimiento, como por ejemplo un video del actor Tom Cruise en bata realizando el baile de la serie Merlina Adams[74]. Por supuesto que dicha inocuidad quedará sujeta a interpretación de la persona retratada y puede ser que los parámetros no sean iguales en todos los casos.

3.3. Consentimiento para el uso de la imagen personal en la creación de replicas digitales

"Este peligro surge en forma de medios sintéticos, que extrae audio o imágenes existentes para fabricar de forma realista vídeo, audio o una combinación de los dos para mostrar a un individuo diciendo o haciendo algo que nunca ha dicho o hecho. Cuando estos medios se crean de forma consensuada, no hay nada más que un temor general para justificar su regulación. Sin embargo, la apropiación no consensuada de la voz o la imagen de otra persona conlleva un amplio motivo para justificar la regulación porque un individuo obligado a hablar o actuar a instancias de alguien más no se ha expresado voluntariamente. La pregunta es, ¿qué protección le ofrecerá la ley a esa persona?"[75]

[73] Collier, K. (14 de julio de 2023). Actors vs. AI: Strike brings focus to emerging use of advanced tech. *NBC News*. https://www.nbcnews.com/tech/tech-news/hollywood-actor-sag-aftra-ai-artificial-intelligence-strike-rcna94191

[74] https://www.tiktok.com/@deeptomcruise/video/7181490100314885382

[75] Greenlee, M. (2021). Gun to Your Head: How Deepfakes and Other Non-Consensual Synthetic Media Hold Individual Autonomy Hostage. *UMKC L. Rev.*, *90*, 431, página 432. La traducción es propia.

Uno de los problemas que surgen con este tipo de usos de las tecnologías viene de la mano del consentimiento. En este sentido, debemos analizar no solamente la existencia del consentimiento, sino cuales deberían ser las características de su expresión, como así también la extensión de la autorización otorgada y el uso realizado por la parte autorizada.

Si bien el uso –o mal uso– de estas tecnologías debería preocuparnos a todos, debido a su exposición, son las figuras públicas quienes suelen ser más susceptibles a los abusos de los *deepfakes*. Sin perjuicio de ello, este último año se ha observado un crecimiento del uso de estas tecnologías para realizar estafas de las cuales ha sido objeto el público en general, siendo Argentina el segundo país más afectado en Latinoamérica por incidentes que involucran contenido sintético[76].

Como se analizó anteriormente, existen en la mayoría de las legislaciones instrumentos legales que protegen la imagen personal, pero estas herramientas no están preparadas para hacer frente a los riesgos que conllevan estas nuevas tecnologías que cada día son más comunes y accesibles.

En los últimos meses las denuncias públicas por mal uso de *deepfakes* parecen haber aumentado:

- El 1° de octubre de 2023 el actor Tom Hanks publicó en su cuenta de Instagram una captura de una imagen que pareciera ser él, con una leyenda que decía *"Cuidado!! Hay un vídeo que promociona un plan dental con una versión de inteligencia artificial mía. No tengo nada que ver con eso"*[77].
- Apenas unos días después, el 3 de octubre de 2023, el youtuber conocido como MrBeast (Jimmy Donaldson) denunció en su cuenta de X/Twitter que había personas que estaban recibiendo un video estafa que presentaba una réplica digital suya. En su descargo, el creador de contenido plantea *"¿Están preparadas las plataformas de redes sociales para hacer frente al aumento de los deepfakes de IA? Este es un problema grave"*[78].

[76] Sum and Substance Ltd (2023). *Sumsub Identity Fraud Report 2023*. https://sumsub.com/guides-reports/identity-fraud-report-2023/

[77] Hanks, T. [@tomhanks]. (1° de octubre de 2023). [Fotografía]. Instagram. https://www.instagram.com/p/Cx2MsH9rt7q/?utm_source=ig_web_copy_link. La traducción es propia.

[78] MrBeast [@MrBeast]. (3 de octubre de 2023). *Lots of people are getting this deepfake scam ad of me… are social media platforms ready to handle the rise of AI deepfakes? This is a serious problem* [Posteo]. X. https://x.com/MrBeast/status/1709046466629554577?s=20. La traducción es propia.

- El 1° de noviembre de 2023 varios portales online publicaron[79] la noticia de que la actriz Scarlett Johansson había tomado acciones legales contra una aplicación popularizada en la red social TikTok que permite generar imágenes con inteligencia artificial llamada "*Lisa AI: 90s Yearbook & Avatar*". La actriz reclama que su imagen y voz fueron utilizadas en una publicidad publicada en X/Twitter promocionando la aplicación[80].
- En los últimos meses han surgido también numerosas cuentas en redes sociales[81] que replican la imagen de celebridades mediante softwares de *deepfake* y publican videos parodiando su vida cotidiana.

Evidentemente en los casos mencionados no existió consentimiento alguno de parte de los titulares de derecho para que su imagen sea replicada y asociada con productos o marcas que no patrocinaban.

En Argentina, la Ley 11.723 plantea la necesidad de un consentimiento expreso, mientras que el CCyC nada dice al respecto en su artículo relacionado al derecho a la imagen. Sin perjuicio de ello, el artículo 55 CCyC establece en materia de disposición de derechos personalísimos que el consentimiento no se presume, es libremente revocable y es de interpretación restrictiva, debiendo este no ser contrario a la ley, la moral o las buenas costumbres.

En cuanto a qué es lo que se debe consentir, la Ley 11.723 establece que este será necesario para que la imagen del titular sea "puesta en el comercio", mientras que el CCyC establece, más precisamente, que será necesario consentimiento "para captar o reproducir" la imagen de una persona. Respecto de esto último, la Sala A de la Cámara Nacional de Apelaciones en lo civil ha dejado claro que esto significa que "*toda captación de imagen sea puesta o no en el comercio, requiere del consentimiento de su titular*"[82] y que "*la autorización para captar imágenes de una determinada persona no implica*

[79] Véase Shanfeld, E. (1° de noviembre de 2023). Scarlett Johansson Takes Legal Action Against AI App That Ripped Off Her Likeness in Advertisement. *Variety.* https://variety.com/2023/digital/news/scarlett-johansson-legal-action-ai-app-ad-likeness-1235773489/

[80] El video contaba con una leyenda que decía *"Imágenes producidas por Lisa AI. No tiene nada que ver con esta persona".*

[81] Véase *https://www.tiktok.com/@deeptomcruise, https://www.tiktok.com/@synthetic.luis, https://www.instagram.com/unreal_tousledhair/, https://www.instagram.com/unreal_chalamet/, https://www.instagram.com/unreal.stark/ , https://www.instagram.com/unmusking_by_elon/*

[82] Cámara Nacional de Apelaciones en lo Civil. Sala A. 22520/2019. Alzugaray, Mirna Fernanda c/ Taraborelli Automobile SA s/ daños y perjuicios. 16 de julio de 2021.

necesariamente la autorización para reproducirlas. Se trata de dos acciones diferentes que suponen consentimientos independientes"[83].

En lo que respecta a su exteriorización, el Tribunal[84] ha dicho que puede ser manifestado de manera verbal, escrita o por signos inequívocos, siendo que predomina la libertad de formas. En el caso *Alzugaray, Mirna Fernanda c/ Taraborelli Automobile SA s/ daños y perjuicios*[85], al analizar la suma de los elementos probatorios, el Tribunal consideró una sonrisa de la actora como uno de los indicios inequívocos de autorización para el uso de la imagen, conformado una especie de consentimiento tácito, es decir, que se infiere de las acciones de la persona.

Sin perjuicio de lo anterior, siempre se debe hacer una interpretación restrictiva de este consentimiento. En este sentido la Cámara Nacional de Apelaciones en lo Civil dijo muy claramente que *"la circunstancia que el accionante se hubiese prestado a fotografiarse, no implicaba autorización para su divulgación"*[86]. Zavala de González explica que "*el consentimiento no es verdaderamente una excepción a la libre utilización de la imagen sino, antes bien, una exigencia como principio*"[87].

En el mismo sentido se han expresado los tribunales de otros países, por ejemplo, en Italia la Corte Suprema de Casación determinó que la manifestación del consentimiento implica un acto jurídico unilateral y explicó que si bien dicho consentimiento puede estar incluido en un contrato, sigue siendo siempre distinto e independiente del acuerdo que lo contiene[88].

Considerando el tenor de los derechos en juego y el daño que puede generar el mal uso de la imagen de una persona, es preciso elevar aún más el nivel de exigencia a fin de garantizar la protección de los titulares de derecho, en particular de aquellos que cuentan con mayor exposición pública.

En materia de protección de datos, el Proyecto de Ley de Protección de Datos Personales recientemente enviado a la Cámara de Diputados exige para el tratamiento de los datos personales de una persona que esta haya otorgado su consentimiento de manera

[83] Alzugaray c/ Taraborelli Automobile (2021).
[84] Alzugaray c/ Taraborelli Automobile (2021).
[85] Alzugaray c/ Taraborelli Automobile (2021).
[86] De La Fuente c/ Artear S.A. (2021).
[87] Zavala de González "Resarcimiento de daños", Tº 2 d, p. 179, citado en De La Fuente c/ Artear S.A. (2021).
[88] Corte Suprema de Casación de Italia. Sección Civil I. Sentencia N° 1748. 29 de enero de 2016.

previa, expresa, libre, inequívoca, informada y específica, mediante una declaración o una clara acción afirmativa[89]. Pareciera que un consentimiento como el que plantea este Proyecto sería más apropiado para autorizar el uso de un aspecto tan característico del individuo como es su imagen personal.

Si bien ni la actual Ley de Protección de los Datos Personales N° 25.326 (LPDP), ni el citado Proyecto, hacen mención expresa a la imagen como dato personal, definen[90] a estos como toda información referida a personas[91] determinadas o determinables. La imagen de una persona recae definitivamente dentro de esta conceptualización. El propio sitio web del Ministerio de Justicia y Derechos Humanos[92] al explicar la LPDP dice claramente que la imagen es un dato personal[93].

Entonces, si entendemos a la imagen como dato personal, es razonable que su captación, reproducción, difusión o cualquier otro uso requiera de una expresión de consentimiento como la que propone el mencionado Proyecto, a saber:

- previo: requiere que el consentimiento sea solicitado anticipadamente;
- expreso: requiere una exteriorización de la voluntad del titular de la imagen que cumpla[94] con los requisitos establecidos por el artículo 262 del CCyC para la manifestación de la voluntad;
- libre: requiere que el consentimiento esté exento de vicios. Peyrano expresa correctamente que esta exigencia podría ser considerada sobreabundante, siendo que el consentimiento prestado bajo coacción no sería válido[95];
- inequívoco: requiere que sea posible interpretar claramente cuál es el alcance del consentimiento otorgado;

[89] Fernández, A. y Rossi, A. O. (30 de junio de 2023). Proyecto de Ley 0012-PE-2023. *Mensaje Nro: 0087/23 y Proyecto de Ley. Régimen de protección de datos personales. Derogación de las Leyes 25326 y 26343.* https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/0012-PE-2023.pdf. Artículo 2.

[90] Tanto la Ley de Protección de los Datos Personales N° 25.326, como el Proyecto de Ley de Protección de Datos Personales definen este término en su artículo 2.

[91] La Ley N° 25.326 incluye en su definición a las personas físicas o de existencia ideal, mientras que el Proyecto sólo hace mención a personas humanas.

[92] *Datos personales.* (s. f.). Argentina.gob.ar. https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales

[93] En respuesta a la pregunta "¿Mi imagen en videos de sistema vigilancia también es un dato personal?", el citado sitio responde "Si".

[94] Peyrano, G. F. (7 de julio de 2003). *El principio del consentimiento en el «sistema de protección de los datos personales». Condiciones de validez y posibilidad de revocación del consentimiento prestado. El derecho de oposición.* SAIJ. http://www.saij.gob.ar/doctrina/dacf070007-peyrano-principio_consentimiento_en_sistema.htm;jsessionid=fawxfxf0rrudeh4vfxwp85wy?0&bsrc=ci

[95] Peyrano (2003).

- informado: requiere que el titular cuente con información completa respecto al uso que se pretende realizar de su imagen, como mínimo debería entender con qué fin será captada, cómo será usada, en qué territorios, durante qué plazo y para qué medios;
- específico: requiere que el titular consienta expresamente las acciones que el autorizado pretenda realizar, ya sea que se autoriza la captación o su reproducción, como ya estableció nuestro Tribunal, la autorización para una no implica la otra;
- mediante una declaración o una clara acción afirmativa: requiere de una acción positiva que externalice indudablemente la existencia del consentimiento.

Otro aspecto esencial del consentimiento es el hecho de que es revocable. Esto surge claramente de los dos instrumentos legales que regulan el derecho a la imagen en nuestro país[96]. En particular la Ley 11.723 prevé el resarcimiento de los daños y perjuicios que la revocación del consentimiento puede generar a terceros. Nada dice esta norma respecto a la necesidad de formalidades ni de justa causa, simplemente basta con que se manifieste.

Los tribunales españoles se han expedido reiteradas veces sobre este asunto[97]. Con relación a la revocación del consentimiento de artistas profesionales del espectáculo o aquellos que autorizan el uso de su imagen con fines comerciales, la Sala Segunda del Tribunal Constitucional de España ha dicho que incluso en estos casos la revocación del consentimiento es posible siendo que el derecho a la imagen, como derecho personalísimo, prevalece sobre cualquier otro derecho u obligación que la cesión contractual haya creado[98]. En el mismo caso, este Tribunal se expresó respecto al alcance de dicha revocación y dijo que "*tratándose del ejercicio de una facultad derivada de un derecho constitucional de la personalidad, la posibilidad de revocación no se agota con su ejercicio frente a quien originariamente resultó beneficiario de la licencia, sino que se extiende a todos los que sucesivamente hayan podido ir adquiriendo la titularidad sobre lo transmitido, puesto que se trata de recobrar el derecho a la imagen, irrenunciable e*

[96] El artículo 31 de la Ley 11.723 establece que *"[l]a persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios*" y el artículo 55 del CCyC dice que el consentimiento para la disposición de los derechos personalísimos es libremente revocable.
[97] Véase Tribunal Supremo. Sala de lo Civil. Sentencia 1779/2016. 21 de abril de 2016; Tribunal Constitucional de España. Sala Segunda. Sentencia 117/1994. 25 de abril de 1994.
[98] TC de España. Sentencia 117/1994 (1994).

inalienable en su esencia, dejando sin efecto la autorización que es una facultad excepcional otorgada"[99].

Un punto interesante destacado por el mencionado Tribunal es que la revocación del consentimiento no puede proyectarse hacia el pasado[100], por ello, si bien es cierto que esta puede manifestarse en cualquier momento, puede suceder que su revocación llegue tarde. Por ejemplo, en el caso analizado por este Tribunal la actriz Ana Obregón había manifestado la revocación de su consentimiento respecto al uso de unas fotografías suyas en la revista "Play Boy España". Uno de los codemandados manifestó que la revocación expresada por la actora había sido recibida "*veinte días antes de la tirada del ejemplar […] cuando estaba ya compuesta la revista, en fase avanzada de impresión y posterior distribución*". Tanto el Juzgado de Primera Instancia como la Sala Primera del Tribunal Supremo entendieron que "*la publicación de las fotografías era un evento que, a los efectos de la revocación del consentimiento, debía tenerse por acaecido porque, según su fundamentación, la editora demandada sólo tuvo conocimiento de aquélla cuando era ya materialmente imposible detener, sin grave perjuicio y quebranto, la publicación de la revista*". Al recurrir la actora contestó que "*en tanto no se hubiera hecho pública la edición, la revocación obligaba en toda su extensión a los demandados, sin que pudiera argumentarse en términos de menoscabo económico para negarle su eficacia, pues, caso de producirse algún perjuicio, la editora habría tenido derecho a la indemnización*". Finalmente, la Sala Segunda del Tribunal Constitucional coincidió con la consideración de que "*la publicación no era un acontecimiento singular e instantáneo, sino un proceso integrado por una pluralidad de fases sucesivas, de las cuales algunas de las más importantes ya se habían producido con anterioridad a la revocación y a su conocimiento por la editora*" por lo que "*se trataba de un acontecimiento que -por su contenido plural y sucesivo- había que tenerse por prácticamente concluido cuando la revocación se produjo*".

Entonces, ¿cómo debería ser el consentimiento para el uso de la imagen personal en la creación de replicas digitales? Si bien encontramos algunos casos en la jurisprudencia cuyo objeto disputado es un dibujo o caricatura y quizás unos pocos que se sustancian alrededor de la evocación de la personalidad, la mayoría de los conflictos que involucran la imagen personal se centran en el uso de una fotografía. Las fotografías se capturan en

[99] TC de España. Sentencia 117/1994 (1994).
[100] TC de España. Sentencia 117/1994 (1994).

un instante y pueden ser obtenidas sin mayor preparación, en un momento fugaz, por lo tanto, el fotógrafo podría alegar que interpretó una seña o sonrisa como consentimiento. La creación de una réplica digital, en cambio, requiere de un comportamiento proactivo y consciente que implica trabajos preparativos, como por ejemplo seleccionar imágenes del sujeto a replicar, como así también un proceso de producción. Por más sencillos que sean de usar los softwares de alteración de imagen que permiten generar *deepfakes*, el usuario debe cargar las imágenes a replicar y proveer al sistema de alguna comanda o *prompt* respecto al resultado que se pretende obtener. Se entiende entonces que suele haber una intención clara y premeditada antes de la creación de una réplica digital, pudiendo el creador de dicho contenido sintético procurar obtener previamente el consentimiento del sujeto a replicar. A diferencia de lo que ocurre con las fotografías, en donde el consentimiento puede ser espontáneo y derivar en la creación del retrato, las réplicas digitales no tienen –al menos aún– esta misma inmediatez en su creación, es decir que el creador de dicho contenido tiene la oportunidad para asentar el consentimiento necesario en algún medio fehaciente o, al menos, asegurar la inequivocidad de su expresión.

Considerando lo anterior, es lógico exigir que el consentimiento necesario para autorizar la creación y uso de réplicas digitales sea, siguiendo la línea del Proyecto de Ley de Protección de Datos Personales, previo, expreso, libre, inequívoco, informado, específico y externalizado mediante una declaración o una clara acción afirmativa.

4. Las réplicas digitales en la actualidad

4.1. Distintos usos de las réplicas digitales

Las tecnologías que permiten generar réplicas digitales de una persona no son nuevas, pero hasta hace poco, debido a los altos niveles de conocimiento técnico que requerían y los elevados costos relacionados a su implementación, podíamos encontrarlas aplicadas casi exclusivamente en el ámbito del entretenimiento. Sin embargo, en los últimos años, en gran parte gracias a redes sociales como Snapchat[101], Instagram[102] y TikTok, hemos observado una domesticación de estas tecnologías y hoy podemos acceder a ellas desde cualquier teléfono celular.

Si bien no siempre se usan con fines ilícitos o mal intencionados, no podemos ignorar la capacidad de generar daño que poseen. El riesgo de las réplicas digitales o *deepfakes* emana de su capacidad de engañar, por eso cuando la calidad del resultado es tal que puede pasar por real, es importante que este se acompañe de alguna leyenda o descripción que permita identificarlo como sintético, sobre todo cuando ello no pueda deducirse del propio contenido ni del contexto.

Un estudio de la Universidad de Sungkyunkwan en Corea del Sur publicado en septiembre de 2023[103] centrado en *deepfakes*, recopiló dos mil videos de las plataformas Reddit, YouTube[104], TikTok y Bilibili[105], con origen en más de veinte países y en cuatro idiomas distintos. Como parte de la información analizada, se propuso identificar las intenciones detrás de los usos de estos contenidos sintéticos, logrando reducirlas a tres: fraude, político, entretenimiento. Con esto en mente, se plantea a continuación una clasificación similar que pretende identificar los distintos usos de los *deepfake*.

[101] Snapchat en una aplicación de mensajería que permite a los usuarios enviar y recibir fotos y vídeos que desaparecen poco después de haber sido enviados.
[102] Instagram es una red social que permite compartir fotos y videos con otros usuarios.
[103] Cho, B., Le, B. M., Kim, J., Woo, S., Tariq, S., Abuadbba, A., & Moore, K. (Octubre 2023). Towards understanding of deepfake videos in the wild. In *Proceedings of the 32nd ACM International Conference on Information and Knowledge Management* (pp. 4530-4537). https://www.researchgate.net/publication/373686936_Towards_Understanding_of_Deepfake_Videos_in_the_Wild
[104] YouTube es una red social que permite subir, alojar, compartir y reproducir videos que han sido creados por los usuarios.
[105] Billibilli es una res social disponible solamente en el territorio de China, destinada a alojar y compartir videos.

4.1.1. Desinformación

"La creciente prevalencia de vídeos falsos (deepfakes) podría socavar lo que sabemos que es verdad."[106]

Uno de los principales riesgos asociados al uso mal intencionado de tecnologías como las que nos ocupan tiene que ver con la desinformación. Internet ha facilitado enormemente el acceso a todo tipo de información y se ha convertido en la principal fuente de noticias para la mayor parte de la población. Si bien aún subsisten los medios tradicionales de información (radio, televisión y medios impresos), todos ellos cuentan hoy además con una presencia en línea. En particular, las redes sociales han jugado un rol central en el enorme cambio que ha ocurrido en los últimos años en el modelo de consumo de noticias[107]. La encuesta anual del Instituto Reuters sobre hábitos de información de 2023[108] informa que en los últimos años se ha observado que el acceso directo a aplicaciones y sitios web de medios de comunicación ha disminuido, habiendo ocupado este lugar las redes sociales debido a su ubicuidad y conveniencia. Según este reporte, entre 2018 y 2023 el porcentaje de personas que accedieron a las noticias mediante los sitios webs de los medios de comunicación ha caído diez puntos en todo el mundo, mientras que el acceso a través de redes sociales ha aumentado casi en la misma medida.

Este cambio en el modo en que consumimos información viene acompañado de una mayor exposición a la desinformación. Los efectos y la eficacia de campañas de *fake news*[109] ha quedado evidenciada en el documental de Netflix de 2019 "Nada es privado" en donde se devela como la consultora Cambridge Analytica utilizando la información de perfiles de redes sociales realizó una campaña de *microtarget* enviando información específica a los usuarios, mucha de la cual era falsa[110], en el marco de la campaña electoral de Donald Trump en 2016.

[106] Fallis, D. (2020). The epistemic threat of deepfakes. *Philosophy & Technology, 34*(4), 623-643. https://doi.org/10.1007/s13347-020-00419-2. La traducción es propia.
[107] Baroja, A. G. (14 de junio de 2023). Las redes sociales ganan terreno en el consumo de noticias y TikTok sigue su ascenso entre los jóvenes. *El País.* https://elpais.com/comunicacion/2023-06-14/las-redes-sociales-ganan-terreno-en-el-consumo-de-noticias-y-tiktok-sigue-su-ascenso-entre-los-jovenes.html
[108] Reuters Institute for the Study of Journalism (2023). Digital News Report 2023 https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023
[109] Término popularizado para describir noticias falsas.
[110] Sobornos, mujeres y noticias falsas: el CEO de Cambridge Analytica confesó en una cámara oculta los métodos que salpican a Facebook. (20 de marzo de 2018). *Infobae.* https://www.infobae.com/america/eeuu/2018/03/19/sobornos-mujeres-y-noticias-falsas-el-ceo-de-cambridge-analytica-confeso-en-una-camara-oculta-los-metodos-que-salpican-a-facebook/

Los *deepfakes* presentan un enorme riesgo cuando se utilizan para desinformar, en especial cuando la información falsa perpetrada tiene que ver con temas de salud –como lo fue durante la pandemia de Covid-19[111]– o seguridad pública. El conflicto Rusia-Ucrania ha resultado ser un claro ejemplo de los riesgos de los *deepfakes*. En marzo de 2022 un sitio de noticias, como resultado de un supuesto hackeo, publicó un video del presidente de Ucrania Volodymyr Zelensky pidiendo a las tropas que abandonaran el conflicto armado. Este es uno de los primeros casos en los cuales se ha publicado una réplica digital de un funcionario público con intenciones expresas de engañar al público y difundir información falsa[112]. A pesar de que la calidad del video era mala, el propio Zelensky recurrió a las redes sociales para desmentirlo. *"Estamos en casa y defendiendo a Ucrania. No vamos a deponer las armas. Por nuestra victoria"* publicó en la red social X/Twitter el Ministerio de Defensa de Ucrania junto a un video del Presidente[113]. Si este *deepfake* hubiera pasado por cierto, podría haber tenido implicancias significativas para la guerra[114].

Las réplicas digitales parecieran ser la nueva herramienta estrella de la propaganda política. Poco después de lo acontecido con el presidente Zelensky, la cuenta oficial de Ucrania en la red social X/Twitter publicó un video que mostraba al presidente de Rusia, Vladímir Putin, recorriendo las zonas afectadas por la guerra[115]. La publicación leía "*Putin dice la verdad, ¿eh? Bueno, intentamos imaginar qué diría si lo hiciera*"[116]. El video no pretendía pasar por cierto, siendo que no sólo contenía una marca de agua fija que manifestaba que se trataba de contenido sintético, sino que además comenzaba con la siguiente leyenda que indicaba que el video era falso: *"Descargo de responsabilidad. El personaje de esta película, aunque está basado en una persona real, es ficcional y su voz es personificada. Pero la historia que cuenta es tristemente muy real. Esta película está*

[111] Incluso años luego de la pandemia, la información falsa continúa circulando. Según el reporte de Reuters, en febrero de 2023 más del 40% de los encuestados reportaron haber visto o leído información falsa sobre el Covid-19 en la última semana. Véase Reuters Institute for the Study of Journalism (2023).
[112] Twomey, J. G., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G. (2023). Do deepfake videos undermine our epistemic Trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. *PLOS ONE, 18*(10), e0291668. https://doi.org/10.1371/journal.pone.0291668
[113] Defense of Ukraine [@DefenceU]. (16 de marzo de 2022). 🔊 *«Ми вдома і захищаємо Україну. Ніякої зброї ми складати не збираємось. До нашої перемоги», - Президент України @ZelenskyyUa* [Video]. X. https://x.com/DefenceU/status/1504054999793512449?s=20. La traducción es propia.
[114] Twomey, *et al*. (2023).
[115] Ukraine / Україна [@Ukraine]. (21 de abril de 2022). *Putin telling truth, huh? Well, we tried to imagine what he'd say if he did. Created by ADC*UA, Gvardiya Production House and AI startup Reface. @reface_app @Gvardiya_ph👏 #ArmUkraineNow* [Video]. X. https://x.com/Ukraine/status/1517119052904374272?s=20
[116] Ukraine / Україна. X. (2022). La traducción es propia.

realizada con el uso de medios sintéticos como metáfora para contar al mundo sobre los verdaderos motivos y consecuencias de la guerra de Rusia contra Ucrania. Estamos seguros de que todos los hechos expresados en esta película serán probados en la Corte Penal Internacional, directamente en La Haya […]"[117].

Si bien la intención de este video no es engañar al espectador, sí busca generar un impacto en él, situando al presidente ruso en escenarios en los cuales no ha estado, generando intencionalmente un contraste entre los estragos causados por la guerra a la ciudad de Mariupol, Ucrania, y la imagen pulcra y sosegada de Putin. Incluso cuando la intención no sea engañar, ciertos usos de estas tecnologías pueden generar daños al titular de la imagen. En este caso, como sucede también en aquellos en los cuales la falsedad del contenido es evidente por la calidad o el contexto[118], los materiales están enfocados más en afectar o atacar la imagen del sujeto representado que en engañar al observador.

Un estudio realizado por la University College Cork de Irlanda identificó que el uso de contenido sintético como el que realizó el gobierno de Ucrania con el mencionado video puede resultar desfavorable e incitar la desconfianza en la entidad, siendo que de esta forma el público toma conocimiento de las capacidades técnicas de dicha institución para realizar réplicas digitales convincentes. El mencionado estudio recomienda que los gobiernos y organizaciones que dependen de la confianza del público eviten el uso de *deepfakes* en sus campañas y mensajes[119].

4.1.2. Suplantación de identidad

Otra de las crecientes amenazas relacionadas con esta tecnología es la suplantación de identidad, la cual aumenta a medida que las herramientas disponibles se popularizan y el nivel de eficacia de los softwares para generar réplicas digitales mejora.

Quizás la posibilidad de hacerse pasar por otra persona con una imagen estática o un video es limitada, pero los avances de la inteligencia artificial generativa están permitiendo alterar imágenes y audio en directo. Esto presenta un reto incluso para los sistemas de verificación de identidad en los que se basan gran parte de los mecanismos de seguridad digital, como por ejemplo aquellos de reconocimiento facial o de voz. Otro estudio de la ya citada Universidad de Sungkyunkwan en Corea del Sur publicado en

[117] Ukraine / Україна. X. (2022). La traducción es propia.
[118] Por ejemplo videos pornográficos de los líderes militares, según reporta Twomey, *et al*. (2023).
[119] Twomey, *et al*. (2023).

marzo de 2021 dejó en evidencia la facilidad con la que las réplicas digitales pueden evadir las medidas de seguridad basadas en reconocimiento facial[120]. Esto abre el abanico a nuevas oportunidades para cometer ilícitos: extorsiones, engaños, ciberacosos, robos, estafas, *phishing*[121], entre otros.

En particular en Argentina no se encuentra tipificado el delito de suplantación de identidad digital. Para nuestra legislación, este tipo de conductas conforman la antesala o el primer eslabón[122] de otras actividades ilícitas que nuestro ordenamiento jurídico sí castiga penalmente. En el ámbito de la Ciudad Autónoma de Buenos Aires, en el año 2020 mediante la última actualización del digesto jurídico de la Ciudad a través de la Ley N° 6.347, se incorporó al Código Contravencional de la Ciudad un artículo referido a la suplantación digital de la identidad, el cual prevé una multa para quienes, sin consentimiento y sin constituir un delito, utilicen la imagen o datos filiatorios de una persona, o con ellos creen una identidad falsa, mediante la utilización de cualquier tipo de comunicación electrónica, transmisión de datos, página web o cualquier otro medio[123].

Entre los usos ilegales de las réplicas digitales, podemos identificar desde casos en los que la imagen de celebridades ha sido utilizada para promover productos o servicios sin autorización –como los mencionados casos de Tom Hanks y Scarlett Johansson– hasta situaciones en las que altos directivos de empresas han sido víctimas de engaños y realizado transferencias de dinero bajo la ilusión de estar realizando transacciones legítimas de la empresa[124].

[120] Tariq, S., Jeon, S., & Woo, S. S. (Abril 2022). Am I a Real or Fake Celebrity? Evaluating Face Recognition and Verification APIs under Deepfake Impersonation Attack. In *Proceedings of the ACM Web Conference 2022* (pp. 512-523). https://arxiv.org/pdf/2103.00847.pdf

[121] El *phishing* es una técnica de ingeniería social usada para obtener información confidencial de una persona de forma fraudulenta a fin de apropiarse de su identidad.

[122] Pilnik, F. (16 de diciembre de 2021). *Comentarios sobre la suplantación de identidad digital.* SAIJ. http://www.saij.gob.ar/franco-pilnik-comentarios-sobre-suplantacion-identidad-digital-dacf210223-2021-12-16/123456789-0abc-defg3220-12fcanirtcod?&o=171&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema/Derecho%20civil%5B3%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Doctrina&t=3985#

[123] Código Contravencional de la Ciudad de Buenos Aires (28 de Octubre de 2004). Artículo 77.

[124] Véase Ciber 4 All Team. (19 de diciembre de 2023). *IA, deepfake y la evolución del fraude del CEO.* Tarlogic Cybersecurity Experts. https://www.tarlogic.com/es/blog/ia-deepfake-fraude-del-ceo/; Damiani, J. (3 de septiembre de 2019). A voice deepfake was used to scam a CEO out of $243,000. *Forbes.* https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=33417c842241

Asimismo, la suplantación de identidad mediante el uso de réplicas digitales puede generar perjuicios al titular de la imagen resultado de ciberacosos o difamación. Hoy en día esta tecnología se encuentra accesible para el público en general. Si bien existen softwares más sofisticados y complejos, a los cuales tienen acceso los profesionales, que permiten obtener resultados de mejor calidad y credibilidad, con ellos coexisten aquellas aplicaciones móviles que proveen opciones más amigables con el usuario y que pueden ser utilizadas sin necesidad de poseer conocimiento técnico alguno[125]. Estas últimas permiten generar contenido sintético de manera fácil y rápida, y a pesar de que probablemente los resultados obtenidos sean de menor calidad, podrían engañar a un espectador desprevenido.

Actualmente no es necesario contar con mayores herramientas que un teléfono celular para poder acceder a crear réplicas digitales. Incluso la 'materia prima' para alimentar estas aplicaciones basadas en inteligencia artificial generativa pueden encontrarse sin mayor problema en Internet o redes sociales, o si se hiciese con fines maliciosos, a través de técnicas de ingeniería social[126].

4.1.3. Entretenimiento

Las técnicas de alteración de imagen son usadas desde hace décadas en la industria del entretenimiento. En particular, en el ámbito audiovisual estas han avanzado notablemente en los últimos tiempos. Desde la aplicación de maquillaje y prótesis, hasta la utilización de softwares de inteligencia artificial, las producciones audiovisuales han recorrido un largo camino. A principios de los 2000 se comenzó a popularizar el uso de imágenes generadas por computadora (CGI por sus siglas en inglés) para alterar la apariencia de los intérpretes. Uno de los primeros usos de estas técnicas lo encontramos en el film 'X-Men 3: La batalla final' de Brett Ratner (2006), en donde se observan los rostros rejuvenecidos de dos personajes icónicos de la saga. Otro gran ejemplo es la película 'El curioso caso de Benjamin Button' de David Fincher (2008), en donde observamos como el actor Brad Pitt rejuvenece a medida que avanza la historia. En este

[125] Algunos ejemplos disponibles en la tienda online de aplicaciones móviles de Google son FaceApp (https://play.google.com/store/apps/details?id=io.faceapp&hl=es&gl=US), Deepfake Studio (https://play.google.com/store/apps/details?id=com.deepworkings.dfstudio&hl=es_AR&gl=US), Revive (https://play.google.com/store/apps/details?id=revive.app&hl=es&gl=US&pli=1). FaceSwap (https://play.google.com/store/apps/details?id=com.ai.faceswap&hl=es_VE&gl=US=), Deepswap (https://play.google.com/store/apps/details?id=ai.deepswap.android&hl=es_AR&gl=US), entre otros.

[126] La ingeniería social hace referencia a aquellas prácticas ilegítimas utilizadas para obtener información confidencial, datos personales o contraseñas mediante la manipulación de usuarios, muchas veces haciéndose pasar por personas de confianza como familiares, amigos o compañeros de trabajo.

caso el director utilizó diversas técnicas para caracterizar al personaje en sus distintas edades, en algunas escenas se utilizaron hasta dobles de cuerpo sobre los cuales luego se incorporó digitalmente el rostro de Pitt.

El cambio que se observa en las últimas producciones audiovisuales es que los avances de la tecnología han permitido, mediante la utilización de softwares de inteligencia artificial, prescindir de los intérpretes. Es decir que ya no es necesario que estos se encuentren presentes en los sets de filmación, y ni siquiera que realicen grabaciones preliminares a fin de que los técnicos puedan luego trabajar sobre ese material. Hoy en día estos softwares se pueden 'alimentar' de grabaciones anteriores, e incluso de material disponible en línea, y permiten generar escenas nuevas a gusto del director.

Varios intérpretes han expresado su preocupación ante la aplicación de esta tecnología, como así también sobre la falta de control de sus réplicas digitales. En una entrevista con la revista WIRED[127], el actor Keanu Reeves, protagonista de las sagas 'Matrix' y 'John Wick', comentó que tiene la costumbre de incluir en sus contratos una cláusula que prevé que todo retoque digital sobre su persona debe ser previamente aprobado por él. *"No me importa si alguien quita un parpadeo durante una edición. Pero a principios de los 2000, o puede que haya sido en los 90, me modificaron una actuación. Agregaron una lágrima en mi cara y yo me quedé como '¿eh?'. Fue como si ni siquiera hiciera falta que estuviera ahí"*[128]. Por su parte, el actor y experto en artes marciales Jet Li, comentó en una entrevista en el año 2002 que rechazó un rol en la saga 'Matrix' por no estar dispuesto a que sus movimientos sean digitalizados y cedidos a la productora[129].

En cambio, existen aquellos que han encontrado en esta tecnología una nueva oportunidad comercial y han sabido sacar provecho de estas herramientas, como por ejemplo el actor Bruce Willis, quien a pesar de que su salud no le permite continuar

[127] Watercutter, A. (14 de febrero de 2023). Keanu Reeves will never surrender to the machines. *WIRED*. https://www.wired.com/story/keanu-reeves-chad-stahelski-interview/. La traducción es propia,
[128] Watercutter (2023). La traducción es propia.
[129] Tabany, S. (30 de julio de 2023). Huelga en Hollywood: pese al reclamo, los estudios redoblan la apuesta a la IA. *El Economista.* https://eleconomista.com.ar/internacional/huelga-hollywood-pese-reclamo-estudios-redoblan-apuesta-ia-n64674

actuando, ha participado de una publicidad realizada por la empresa Deepcake[130] para una compañía rusa[131].

Desde 2018 el uso de estas tecnologías ha crecido más del 100% anual[132], lo cual explica uno de los grandes debates que se dio en Hollywood durante el año 2023, en donde el Sindicato de Guionistas de Estados Unidos (*Writers Guild of America* – WGA) y el ya mencionado SAG-AFTRA pararon a la industria durante varios meses protestando, entre otras cosas, por la aplicación de inteligencia artificial a las producciones audiovisuales. En particular, uno de los puntos que preocupaba a SAG-AFTRA tenía que ver con el derecho a la imagen de los intérpretes ante la falta de regulación de la inteligencia artificial y su uso en la industria. Finalmente, las negociaciones con la Alianza de Productores de Cine y Televisión (*Alliance Of Motion Picture And Television Producers* – AMPTP) avanzaron y la huelga que duró 118 días llegó a su fin con un acuerdo tentativo[133] que incluía las primeras protecciones del sindicato en torno a las tecnologías de inteligencia artificial[134].

Otro ejemplo del uso de la tecnología de *deepfake* en el ámbito del entretenimiento lo encontramos en el Museo Salvador Dalí ubicado en la ciudad de San Petersburgo, Florida, Estados Unidos. En el año 2019 el museo estrenó '*Dali Lives'*, una interesante muestra interactiva en la cual los visitantes podían interactuar con una versión en tamaño real del artista mediante una pantalla, treinta años luego de su fallecimiento, e incluso sacarse una foto con él, permitiendo tener un acercamiento al arte según el artista[135]. Nathan Shipley, director técnico del proyecto, comenta en un video publicado por el museo en YouTube[136] que utilizaron inteligencia artificial para traer a Dalí de regreso entrenando al software con entrevistas, citas y material de archivo existente del artista, dividiéndolo en más de 6.000 fotogramas y seleccionando cuidadosamente aquellos donde este mira en la dirección correcta. El sistema utilizado, continúa diciendo Shipley, aprende

[130] https://deepcake.io/
[131] Gajewski, R. (1° de octubre de 2022). Bruce Willis' Rep Refutes Report That He Sold His Digital Likeness to Deepfake Company. *The Hollywood Reporter*. https://www.hollywoodreporter.com/business/digital/bruce-willis-refutes-report-digital-likeness-deepfake-1235231331/
[132] Conforme Cho, *et. al.* (2023).
[133] Según informó el sindicato en su sitio web https://www.sagaftrastrike.org/
[134] *SAG-AFTRA members approve 2023 TV/Theatrical Contracts Tentative agreement.* (5 de diciembre de 2023). SAG-AFTRA. https://www.sagaftra.org/sag-aftra-members-approve-2023-tvtheatrical-contracts-tentative-agreement
[135] The Dalí Museum. (8 de mayo de 2019). *Behind the Scenes: Dalí Lives* [Archivo de Vídeo] YouTube. https://www.youtube.com/watch?v=BIDaxl4xqJ4
[136] The Dalí Museum. YouTube. (2019).

exactamente cómo se ve y cómo se mueve la boca de Dalí, cómo se mueven sus ojos y sus cejas, replicando cada pequeño detalle sobre lo que hace a Dalí, Dalí. El material generado con más de 1.000 horas de entrenamiento de modelos de *machine learning* fue luego incorporado al cuerpo de un actor real con características físicas generales parecidas a las de Dalí[137] y se combinó con las grabaciones de un actor de voz que interpretó los guiones[138]. El resultado del trabajo de la agencia de publicidad Goodby Silverstein & Partners[139] fueron casi 45 minutos de nuevo material de Dalí[140], original y nunca antes visto, 125 videos interactivos y 190.512 combinaciones posibles para sorprender a los visitantes del museo.

Si bien el término *deepfake* pareciera tener una connotación negativa debido a sus orígenes, '*Dali Lives*' es un claro ejemplo de las posibilidades enriquecedoras que nos provee esta tecnología. Hank Hine, director del museo, opina que esta experiencia *"añade una sensación de emoción, si [los visitantes] pueden empatizar con este hombre como ser humano, entonces podrán relacionarse con su trabajo de manera mucho más directa y apasionada"*[141].

Como se mencionó anteriormente, el objetivo del presente no es condenar el uso de réplicas digitales, sino más bien proponer una estructura legal que permita su existencia y dé lugar a los beneficios y oportunidades que presenta esta tecnología, siempre y cuando exista el consentimiento adecuado.

4.2. Acuerdo entre SAG-AFTRA y AMPTP para los contratos de televisión y salas de cine (*theatrical*) de 2023

El acuerdo para los contratos de televisión y salas de cine (*theatrical*) de 2023 (el "Acuerdo"), resultante de la mencionada huelga en Estados Unidos, aplica a películas cinematográficas y contenido dramático guionado producido para televisión y plataformas, y fue ratificado por los miembros de SAG-AFTRA el 5 de diciembre de 2023[142]. Este Acuerdo incluye previsiones especificas relacionadas con (a) las réplicas

[137] Salvador Dalí Museum. (23 de enero de 2019). *Dalí Lives: Museum brings artist back to life with AI.* https://thedali.org/press-room/dali-lives-museum-brings-artists-back-to-life-with-ai/
[138] Billock, J. (2019, 9 mayo). With a little help from A.I., the Dali Museum brings the famed surrealist to life. *Smithsonian Magazine.* https://www.smithsonianmag.com/travel/with-little-help-from-ai-dali-museum-brings-famed-surrealist-to-life-180972127/
[139] https://goodbysilverstein.com/
[140] https://goodbysilverstein.com/work/play/dali-lives
[141] The Dalí Museum. YouTube. (2019). La traducción es propia.
[142] Conforme informó el sindicato en su sitio web https://www.sagaftra.org/sag-aftra-members-approve-2023-tvtheatrical-contracts-tentative-agreement

digitales y la alteración de la imagen de los intérpretes, (b) las réplicas digitales y la alteración de la imagen de los actores de fondo, y (c) la utilización de inteligencia artificial generativa para la creación de 'intérpretes sintéticos'.

(a) Réplicas digitales y la alteración de la imagen de los intérpretes

El Acuerdo establece las condiciones para la creación y uso de replicas digitales, diferenciando aquellas que tienen origen en una relación contractual laboral o de prestación de servicios ('*Employment-Based Digital Replica*' o EBDR) en las cuales el representado participa activamente, de aquellas replicas digitales de un intérprete real[143] creadas para generar la impresión de que se trata del propio representado y usadas para interpretar el rol de un personaje, realizadas sin la existencia de ningún acuerdo con dicho intérprete para la producción en la cual se utilizará ('*Independently Created Digital Replica*' o ICDR).

La diferencia principal radica en que en el primer caso hay una relación contractual existente entre el intérprete y el productor (o el tercero que este designe), por lo que el sujeto retratado participa físicamente de la creación de su personificación virtual; mientras que en el segundo caso no existe acuerdo alguno que prevea la participación del intérprete para la creación de la réplica digital a usar en la producción audiovisual, por lo que esta suele ser generada utilizando materiales preexistentes. En ambos casos, las réplicas digitales serán utilizadas para retratar al artista en escenas o material en el que en realidad no actuó ni participó.

El Acuerdo establece los requisitos del consentimiento requerido para la creación y uso de las réplicas digitales en cada caso particular:

- **Creación de la réplica digital en los casos de EBDR:** el consentimiento debe ser claro y notorio[144], y requiere ser firmado de manera individual, ya sea

[143] El término usado en el acuerdo es "natural", en inglés "*natural performer*".

[144] Con respecto al consentimiento claro y notorio, o como se establece en el idioma original del Acuerdo: *'clear and conspicuous'*, la Comisión Federal de Comercio de los Estados Unidos ha publicado recientemente las guías sobre el uso de endosos ('*endorsement'* en inglés) y testimonios en publicidad, en la cual ha provisto una definición de este concepto. Estas guías al hacer referencia al artículo 45(a) del Título 15 del Código Federal de los Estados Unidos referido al comercio dicen: *"(f) Para los fines de esta parte, "claro y notorio" significa que una divulgación es difícil de pasar por alto (es decir, fácilmente perceptible) y fácilmente comprensible para los consumidores comunes. Si la representación de una comunicación que requiere una expresión de consentimiento se realiza a través de medios visuales, esta divulgación debe realizarse al menos en la parte visual de la comunicación; si la representación se hace por medios sonoros, la divulgación deberá hacerse al menos en la parte audible de la comunicación; y si la representación se hace por medios tanto visuales como sonoros, la divulgación deberá hacerse en la parte visual y audible de*

mediante la firma de un documento separado a tales fines o mediante la incorporación de una firma adicional en la cláusula o previsión dentro del contrato que manifieste el consentimiento del retratado.

- **Uso de la réplica digital en los casos de EBDR:**
  - Cuando el uso está relacionado con la producción audiovisual en la que el intérprete trabajó, se requiere consentimiento a menos que el material permanezca sustancialmente como estaba originalmente guionado, interpretado o grabado.
  - Cuando se trata de un uso relacionado a un proyecto distinto al de la producción para la cual se contrató al intérprete, se requiere un consentimiento separado y una negociación de los términos de la nueva autorización, es decir, que en estos casos el consentimiento debe otorgarse al momento del uso y no en el contrato original, salvo que en esa oportunidad sea posible proporcionar una descripción razonablemente específica del uso previsto para cada proyecto en el cual se pretende usar el material a futuro.

  Tanto cuando se trate de la creación como del uso de la réplica digital, en los casos de EBDR se requiere incluir una descripción razonablemente específica del uso previsto y se prevé que si el consentimiento es requerido una vez fallecido el intérprete, este puede ser otorgado por un representante autorizado o, si no se puede encontrar representante, por el propio sindicato.
- **Creación y uso de la réplica digital en los casos de ICDR:** es necesario que se obtenga previamente el consentimiento escrito del intérprete, el cual debe ser también claro y notorio, y se negocien los términos de la autorización. No se requiere el consentimiento cuando dicho uso se encuentre protegido por la

la comunicación. Es más probable que una divulgación presentada simultáneamente en la parte visual y audible de una comunicación sea clara y llamativa. Una divulgación visual, por su tamaño, contraste, ubicación, duración de su aparición y otras características, debe destacarse de cualquier texto u otros elementos visuales que la acompañen para que sea fácilmente advertida, leída y comprendida. Una divulgación audible debe presentarse en un volumen, velocidad y cadencia suficientes para que los consumidores comunes la escuchen y comprendan fácilmente. En cualquier comunicación que utilice un medio electrónico interactivo, como las redes sociales o Internet, la divulgación debe ser inevitable. La divulgación no debe contradecirse, mitigarse o ser inconsistente con cualquier otra cosa en la comunicación. Cuando un endoso se dirige a una audiencia específica, como los adultos mayores, los "consumidores comunes" incluyen a los miembros de ese grupo". Véase Comisión Federal de Comercio de los Estados Unidos. (26 julio de 2023). *Guides concerning the use of endorsements and testimonials in advertising.* Federal Register. https://www.federalregister.gov/documents/2023/07/26/2023-14795/guides-concerning-the-use-of-endorsements-and-testimonials-in-advertising#citation-21-p48093. La traducción es propia.

Primera Enmienda a la Constitución de los Estados Unidos[145], por ejemplo, cuando se trate de comentarios, críticas, sátira o parodia, cuando se utilice fines educativos o en un docudrama, u otro trabajo histórico o biográfico, en la medida que dicho uso se encuentre protegido por la mencionada Primera Enmienda.

- **Alteración digital de una interpretación:** es necesario obtener el consentimiento del intérprete para alterar digitalmente material grabado en el que este se encuentre representado, salvo que el material permanezca sustancialmente como estaba originalmente guionado, interpretado o grabado. En este caso también el consentimiento debe ser claro y notorio, y requiere ser firmado de manera individual, ya sea mediante la firma de un documento separado a tales fines o mediante la incorporación de una firma adicional en la cláusula o previsión dentro del contrato que manifieste el consentimiento del retratado. Asimismo, se requiere incluir una descripción razonablemente específica del uso previsto y se prevé que si el consentimiento es requerido una vez fallecido el intérprete, este puede ser otorgado por un representante autorizado o, si no lo hubiese, por el propio sindicato. Se establecen algunas excepciones al requisito del consentimiento en materia de alteración de la imagen grabada, principalmente destinada a permitir las tareas de postproducción

(b) Réplicas digitales y la alteración de la imagen de los actores de fondo

Cuando hablamos de la réplica digital de un actor de fondo nos referimos a la reproducción virtual de la voz o imagen que se crea utilizando medios tecnológicos con la participación física del sujeto en cuestión, con el propósito de representar al actor de fondo en una escena en la que este en realidad no apareció. Las previsiones relacionadas a la creación, uso o alteración de la réplica digital de los actores de fondo establecen claramente que no serán de aplicación cuando se trate de técnicas de revestimiento de multitudes o "*crowd tiling*".

[145] Según explica el sitio oficial de la Casa Blanca, la primera enmienda protege la libertad de expresión, de prensa, de reunión, y el derecho de solicitar al gobierno compensación por agravios. Véase https://www.whitehouse.gov/es/acerca-de-la-casa-blanca/nuestro-gobierno/la-constitucion/#:~:text=La%20primera%20enmienda%20garantiza%20que,al%20gobierno%20compensaci%C3%B3n%20por%20agravios.

El consentimiento que se requiere para las réplicas digitales de los actores de fondo, tanto para la creación como para el uso, es similar al establecido en el punto anterior, siendo que debe ser también claro y notorio, y requiere ser firmado de manera individual, ya sea mediante la firma de un documento separado a tales fines o mediante la incorporación de una firma adicional en la cláusula o previsión dentro del contrato que manifieste el consentimiento del retratado. Aquí también se diferencia entre los usos para una producción audiovisual en la que el intérprete trabajó o para un proyecto distinto para el cual se lo contrató. En este último caso, en particular se establece que no se utilizará la réplica digital en lugar de contratar a los actores de fondo necesarios para cumplir con los máximos de cobertura aplicables al proyecto, y que no se utilizará la réplica digital del actor de fondo para evitar la participación de ese intérprete en la producción. Estas últimas previsiones tienen una clara intención de proteger a los intérpretes de abusos en el uso de las réplicas digitales y evitar que el rol que estos cumplen se vuelva obsoleto.

(c) Intérpretes sintéticos

El Acuerdo hace referencia también a lo que define como 'intérpretes sintéticos', estos son activos digitales creados mediante la aplicación de inteligencia artificial generativa y que tienen como objetivo crear, y crean, la impresión de que se trata de un intérprete real[146] que no es reconocible como ningún intérprete real identificable, ni utiliza la voz de una persona real. Estos intérpretes sintéticos no son réplicas digitales, por lo que no existe detrás ningún contrato con intérpretes reales por su creación o uso en relación con el rol que ocupan en la producción.

Con relación a esta figura en particular, se deja asentado que las partes reconocen la importancia del desempeño humano en películas y el impacto potencial en el empleo que puede tener el uso de intérpretes sintéticos para roles que de otro modo serían desempeñados por humanos. Una vez más se denota el peso del sindicato en las negociaciones. En línea con lo anterior, se prevé un compromiso de parte del productor de notificar al sindicato cuando se utilice un intérprete sintético en lugar de contratar un intérprete real, dando lugar también a la oportunidad de negociar de buena fe respecto de una compensación adecuada para dicho rol con un intérprete real. Esto último no aplica cuando se trate de personajes no humanos.

[146] El término usado en el acuerdo es "natural", en inglés "*natural performer*".

En aquellos casos en que para la creación de estos intérpretes sintéticos se utilicen en los sistemas de inteligencia artificial generativa indicaciones o '*prompts'* que individualicen el nombre o algún rasgo físico distintivo de un intérprete real, el productor deberá obtener el consentimiento de dicho intérprete real y negociar con este las condiciones de uso del intérprete sintético resultante dentro de una producción audiovisual. Lo anterior aplicará a cada uno de los intérpretes reales identificados en las indicaciones otorgadas al software en los casos en que más de un sujeto sea mencionado, por ejemplo, cuando el intérprete sintético tome de referencia los ojos de un intérprete real individualizado y la boca de otro. Se exceptúa la necesidad de obtener este consentimiento cuando este uso se encuentre protegido por la Primera Enmienda a la Constitución de los Estados Unidos, tal como se mencionó anteriormente.

Si bien este histórico acuerdo representa un enorme avance para la protección de los derechos de los intérpretes ante el auge de una tecnología que los afecta directamente, algunas de las previsiones del Acuerdo despiertan ciertas preocupaciones. Excepciones amplias como la relacionada a la Primera Enmienda prenden las alertas de cualquier jurista, sobre todo sabiendo el peso que está disposición tiene en el territorio norteamericano. Asimismo, la vaguedad de algunas cláusulas como por ejemplo la excepción planteada en materia de alteraciones ("salvo que el material permanezca sustancialmente como estaba originalmente guionado, interpretado o grabado") probablemente den trabajo a los tribunales que tengan que interpretar y definir los parámetros de esta salvedad.

4.3. Esfuerzos por combatir los usos perjudiciales de las réplicas digitales

A medida que las tecnologías de *deepfake* avanzan, aumenta la necesidad de contar con herramientas para distinguir el contenido sintético del real. Como se ha mencionado anteriormente, en los últimos años los softwares de alteración de imagen se han domesticado a tal nivel que hoy se puede tener acceso a ellos desde cualquier dispositivo móvil y sin necesidad de contar con conocimientos técnicos para su uso. Es esperable que esto venga acompañado de un aumento en la exposición del público general a las réplicas digitales y con ello crezca el riesgo a sufrir los efectos negativos de los usos perjudiciales de estas tecnologías.

Los *deepfakes* proliferan en las redes sociales, que son no solamente un espacio para compartir el contenido sintético sino también para crearlo. Quizás la calidad de los

'filtros'[147] de estas plataformas no es suficiente como para defraudar al espectador, pero no deben ser descartados tan rápidamente de la discusión. Recientemente se viralizó en la red social TikTok un filtro que permite reemplazar el rostro de una persona por el de la cantante Taylor Swift[148]. Los usuarios de la plataforma estaban asombrados con la calidad de los resultados, que si bien no eran suficientes para hacerse pasar por la artista, en cuestión de segundos el filtro lograba transformar su fisonomía para replicar la de la megaestrella. En los videos que utilizan el filtro se observan principalmente dos preguntas entre los usuarios de la plataforma: ¿habrá autorizado la artista el uso de su imagen de esta manera?, y si los usuarios de una red social tienen acceso a esta herramienta de manera gratuita, ¿cuáles son los límites de lo que se podría hacer con un software más sofisticado?

Queda en evidencia que el fácil acceso a estas tecnologías y el riesgo de que sean usadas para generar un perjuicio requiere tomar ciertas medidas para proteger a los usuarios de los servicios de Internet. Las redes sociales de a poco han incorporado ciertas previsiones en sus términos y condiciones de uso destinadas a regular el uso de estas tecnologías en sus plataformas. A continuación se hace una breve mención a las políticas relevantes en la materia en las redes sociales más usadas.

(a) X/Twitter

Una de las primeras en resaltar la importancia de regular de cierta forma el contenido sintético dentro de la plataforma fue la red social X/Twitter, la que en octubre de 2019 solicitó el aporte de los usuarios en el tema. "*Cuando ingresas a Twitter para ver lo que sucede en el mundo, queremos que tengas un contexto sobre el contenido que estás viendo y con el que interactúas. Los intentos deliberados de engañar o confundir a las personas a través de medios manipulados socavan la integridad de la conversación*" leía el comunicado que acompañaba al primer borrador de los términos y condiciones de uso publicados por la plataforma en materia de contenido sintético[149]. La versión final de las

[147] Los filtros son funciones que suelen tener las redes sociales de fotos y videos –como Instagram, TikTok o Snapchat– que permiten a los usuarios incorporar superposiciones de diseños a sus fotos o videos de manera inmediata. Algunos filtros permiten incluso interactuar con contenido de realidad aumentada mediante el cual el usuario puede integrar elementos virtuales en el mundo real. Un ejemplo de filtros de *deepfake* son aquellos que reemplazan el rostro del usuario por los de una celebridad u otra persona.
[148] https://vm.tiktok.com/ZM6buxRLP/
[149] *Help us shape our approach to synthetic and manipulated media.* (11 de noviembre de 2019). Twitter Blog. https://blog.twitter.com/en_us/topics/company/2019/synthetic_manipulated_media_policy_feedback . La traducción es propia.

políticas para limitar el impacto de los *deepfakes* fue publicada en febrero de 2020 y ha recibido varias actualizaciones hasta el momento.

En general, X/Twitter no permite "*compartir medios sintéticos, manipulados o fuera de contexto que puedan engañar o confundir a las personas y provocar daños*"[150]. La plataforma entiende que los medios sintéticos y manipulados son "*cualquier foto, audio o video que haya sido alterado o fabricado significativamente de una manera que pretenda engañar a las personas o cambiar su significado original*"[151].

Adicionalmente se prevé la facultad de X/Twitter de "*etiquetar publicaciones que contengan medios engañosos para ayudar a las personas a comprender su autenticidad y brindar contexto adicional*"[152]. Las políticas de la plataforma establecen expresamente que, siempre que se cumplan el resto de las provisiones para el uso de los servicios, no se considerarán contrarios a las políticas de X/Twitter los memes[153] o la sátira, ni tampoco las animaciones, ilustraciones y dibujos animados, siempre y cuando no causen una confusión significante respecto a la autenticidad del contenido. Asimismo, se establece que no serán contrarios a esta regla los comentarios, reseñas, opiniones o reacciones, ni el contradiscurso.

La plataforma establece distintas sanciones ante la violación de estas políticas, como por ejemplo la eliminación del contenido cuando presenta un riesgo grave de daño a personas o comunidades, su individualización con información adicional que detente el tenor del contenido sintético incluido en la publicación –esto puede implicar desde la incorporación de una etiqueta o advertencia que lo identifique como contenido sintético hasta reducir la visibilidad del posteo o impedir que los usuarios interactúen con este–, e incluso la posibilidad de tomar medidas contra la propia cuenta como reducir su visibilidad, bloquearla o hasta suspenderla.

X/Twitter siempre se ha destacado entre las plataformas por ser un espacio dónde prima la libertad de expresión y el control de contenido suele ser mínimo. Resulta interesante la forma en que ha abarcado el tema de los *deepfakes*, ya que si bien se prohíbe

[150] Our synthetic and manipulated media policy. (Abril de 2023). X Help Center. https://help.twitter.com/en/rules-and-policies/manipulated-media. La traducción es propia.
[151] Twitter Blog (2019).
[152] Twitter Blog (2019). La traducción es propia.
[153] La Real Academia Española define a los 'memes' como imágenes, videos o textos, por lo general distorsionado con fines caricaturescos, que se difunde principalmente a través de Internet. Véase https://dle.rae.es/meme

compartir cierto tipo de contenido sintético, en líneas generales se recurre a otras medidas que procuran más que nada informar al usuario sobre su naturaleza dejando en evidencia que se trata de contenido no genuino. En este sentido, ante la detección de posteos que incluyen contenido sintético, las políticas de X/Twitter establecen que además de aplicar una etiqueta o advertencia a la publicación, podrán mostrar una advertencia a las personas antes de que la compartan o cuando indiquen que les guste el posteo, o acompañar el posteo de un enlace a explicaciones o aclaraciones adicionales, todas ellas medidas destinadas a combatir directamente la difusión no intencional de información falsa.

(b) Meta (Facebook/Instagram)

Las políticas de Meta en esta materia manifiestan claramente sus intenciones, diciendo que no hay lugar en sus plataformas para contenido multimedia manipulado cuando dicha manipulación no sea evidente y pueda engañar a las personas, estableciendo que cuando este tipo de contenido sea detectado será eliminado[154].

Meta recomienda no publicar[155] videos que se editaron o sintetizaron de manera tal que un usuario promedio de la plataforma no dilucidaría dicha manipulación e interpretaría el contenido como auténtico, como así tampoco videos que sean producto de inteligencia artificial o *machine learning*, incluidas las técnicas de aprendizaje profundo (por ejemplo, un video *deepfake*), que fusionen, combinen, reemplacen o superpongan contenido en un video, creando un contenido que parece auténtico cuando no lo es. Sin perjuicio de lo anterior, se deja expresa constancia en las políticas de la plataforma que esto no aplicará a contenido creado en carácter de parodia o sátira, por supuesto respetando el principio de libertad de expresión[156].

Aquellos videos que no lleguen a cumplir estos requisitos, pero que se identifique o se reporte que contienen información falsa, serán revisados por los verificadores de datos independientes que trabajan con la plataforma. Si el contenido es calificado por el verificador como falso o parcialmente falso, este no se eliminará directamente sino más bien se tomarán medidas para disminuir su exposición –como por ejemplo reducir su distribución en la sección de noticias, mostrarlo más abajo en el

[154] Conforme establecen las 'Políticas de Contenido multimedia manipulado' de la empresa. Véase Meta. (s. f.). *Contenido multimedia manipulado.* Transparency Center. https://transparency.fb.com/es-la/policies/community-standards/manipulated-media/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fmanipulated_media

[155] Meta. (s. f.).

[156] Meta. (s. f.).

feed del usuario, cubrirlo de modo que los usuarios puedan elegir si quieren verlo o no, o rechazar su promoción como anuncio– y se incorporarán avisos que alerten al usuario de la falsedad del contenido[157]. Monika Bickert, jefa de Gestión de Políticas Globales en Facebook, ha explicado que "*[e]ste enfoque es fundamental para nuestra estrategia […]. Si simplemente elimin——áramos todos los videos manipulados marcados como falsos por los verificadores de datos, los videos aún estarían disponibles en otras partes de Internet o del ecosistema de redes sociales. Al dejarlos publicados y etiquetarlos como falsos, brindamos a las personas información y contexto importantes*"[158].

A partir del 11 de enero de 2024 entró en vigencia una nueva política de Meta en relación con los anuncios sobre temas sociales, elecciones y política que utilicen imágenes o videos que fueron alterados digitalmente. Esta nueva política establece que el anunciante deberá declarar el uso de una imagen, un video o un audio que parece real y que se creó o alteró digitalmente con inteligencia artificial, u otros métodos, en las piezas publicitarias, cuando: (i) muestre a una persona real diciendo o haciendo algo que no dijo ni hizo; (ii) muestre a una persona de aspecto realista que no existe o un evento de aspecto realista que no ocurrió, o altere imágenes de un evento real que sí ocurrió; (iii) muestre un evento realista que supuestamente ocurrió, pero mediante una imagen, un video o una grabación de audio del evento que no son reales[159]. En estos casos Meta agregará un aviso indicando que el anuncio contiene contenido alterado digitalmente.

(c)YouTube

YouTube aún no cuenta con políticas internas respecto al uso y difusión de *deepfakes*, lo cual resulta sorprendente siendo que es una de las plataformas donde circula gran parte de este tipo de contenido. Si bien hace tiempo que YouTube tiene políticas sobre información errónea o falsa[160], las cuales hacen referencia a contenido manipulado mediante medios técnicos, queda claro por los ejemplos que provee el sitio de ayuda de YouTube que estas restricciones no están particularmente destinadas a controlar *deepfakes*.

---

[157] Bickert, M. (6 de enero de 2020). Enforcing against manipulated media. *Meta.* https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/

[158] Bickert (2020).

[159] *Ayudar a las personas a entender cuándo se usa IA o métodos digitales en los anuncios sobre temas sociales o política.* (8 de noviembre de 2023). Meta. https://www.facebook.com/gpa/blog/political-ads-ai-disclosure-policy

[160] YouTube. (s. f.). *Políticas sobre información errónea.* Ayuda de YouTube. https://support.google.com/youtube/answer/10834785?hl=es-419

"*Creemos en tomarnos el tiempo para hacer las cosas bien, en lugar de esforzarnos por ser los primeros*"[161] anuncia un comunicado emitido en noviembre de 2023 dónde la plataforma manifiesta su intención de establecer en los próximos meses políticas claras para regular el contenido sintético dentro de YouTube. En el comunicado la plataforma adelanta que una de las medidas que se incorporará apunta a informar a los usuarios cuando están ante contenido sintético, exigiendo que los creadores revelen que el video contiene material alterado o sintético. Esta se manifestará de dos formas: mediante la incorporación de una etiqueta en el panel de descripción del video o en los casos más sensibles, cuando el contenido trate temas delicados se aplicará una etiqueta más notoria visible al reproducir el video. La plataforma se reserva la facultad de eliminar contenido que viole las Normas de la Comunidad de YouTube. Asimismo, se prevé que el contenido creado con las propias herramientas de inteligencia artificial generativa de la plataforma llevará también esta etiqueta.

Otra de las medidas que se anunciaron es la posibilidad de solicitar la eliminación de contenido alterado o sintético que "*simule a un individuo identificable, incluido su rostro o voz*"[162]. El comunicado aclara que no todo el contenido denunciado será eliminado de la plataforma, sino que se deberá evaluar una variedad de factores a la hora de tomar acción, como por ejemplo analizar si se trata de contenido con carácter de parodia o sátira, o si se trata de una persona pública o celebridad en cuyo caso los parámetros a aplicar pueden variar.

Lo propuesto por YouTube parece estar alineado con el resto de las plataformas analizadas, centrándose básicamente en la transparencia respecto a la naturaleza del contenido y proveyendo a los usuarios de herramientas accesibles para realizar denuncias.

(d) TikTok

TikTok es una de las redes sociales más populares entre los jóvenes y se destaca por mantenerse a la vanguardia de la tecnología de alteración de imagen, siendo constantemente reconocida por sus filtros[163]. La plataforma china realizó una actualización

[161] Flannery O'Connor, J., & Moxley, E. (14 de noviembre de 2023). Our approach to responsible AI innovation. *YouTube Official Blog*. https://blog.youtube/inside-youtube/our-approach-to-responsible-ai-innovation/
[162] Flannery O'Connor (2023). La traducción es propia.
[163] Véase nota 147.

de sus Normas de Comunidad en marzo de 2023[164] y uno de los cambios destacados fue la incorporación de una sección especialmente destinada a regular el uso de material manipulado y contenidos sintéticos. Esta establece que si bien la plataforma fomenta la creatividad que se origina mediante el uso inteligencia artificial y otras tecnologías digitales, también reconoce que esto puede dificultar que los usuarios distingan entre realidad y ficción y los riesgos que esto conlleva. Por ello prevé que el contenido que incluya medios sintéticos o manipulados que muestre escenas realistas deberá informar claramente respecto a su naturaleza ya sea mediante la inclusión de una advertencia en el propio video o su descripción[165].

Las políticas de TikTok son claras cuando expresan que no se permiten medios sintéticos que contengan la imagen de ninguna figura privada real, aunque sí permiten cierto margen de acción cuando se trata de la imagen de una celebridad o figura pública, salvo que el contenido se utilice para endosos (*endorsement*) políticos o comerciales o si viola alguna de las políticas de la plataforma. En todo caso para ser considerado una figura pública el sujeto retratado debe ser mayor de edad. Si bien las políticas de TikTok en relación con el contenido sintético no hacen referencia a la libertad de expresión, esto último claramente tiene que ver con este derecho.

En adición a los esfuerzos de las plataformas para contrarrestar el mal uso de estas tecnologías, queda en evidencia que la necesidad de crear métodos automatizados de detección de *deepfakes* es imperante.

En el año 2019 varias empresas del sector tecnológico[166], lideradas por Facebook (hoy Meta), lanzaron el '*Deepfake Detection Challenge*' (DFDC o Desafío de Detección de Ultrafalsos en español) un desafío para promover el desarrollo de softwares de detección de videos *deepfake*. Más de 2.000 participantes enviaron más de 35.000 modelos para ser considerados en la competencia[167]. Los programas fueron desarrollados en base a

[164] Vincent, J. (21 de marzo de 2023). TikTok bans deepfakes of nonpublic figures and fake endorsements in rule refresh. *The Verge.* https://www.theverge.com/2023/3/21/23648099/tiktok-content-moderation-rules-deepfakes-ai

[165] TikTok. (Marzo de 2023). *Integrity and Authenticity.* https://www.tiktok.com/community-guidelines/en/integrity-authenticity/

[166] Facebook, Partnership on AI, Microsoft y académicos de Technical University of Munich, University of Naples Federico II, Cornell Tech, MIT, University of Oxford, UC Berkeley, University of Maryland, College Park y State University of New York en Albany.

[167] Meta. (12 de junio de 2020). *Deepfake Detection Challenge Results: An open initiative to advance AI.* https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/

un conjunto de videos elaborados por Facebook y puestos a disposición de los competidores.

"La detección de Deepfakes a escala requiere métodos escalables, y la visión artificial o los modelos multimodales son particularmente adecuados para este desafío. Sin embargo, estos modelos requieren datos de entrenamiento y, aunque es posible crear fácilmente varios Deepfakes convincentes, producir los cientos de miles de videos Deepfake necesarios para entrenar estos modelos suele ser costo prohibitivo. Para acelerar los avances en el estado del arte de la detección de Deepfake, hemos construido y publicado abiertamente el conjunto de datos de detección de Deepfake más grande hasta la fecha"[168] informa el documento de investigación publicado por el equipo de Facebook en donde explican las características de la base de datos preparada por la empresa. El modelo que tuvo mejor rendimiento logró una precisión del 65% al ser aplicado a una base de datos privada (*black box dataset*) que no había sido compartida previamente con los desarrolladores[169]. El objetivo de este segundo filtro era aplicar los softwares de detección desarrollados por los participantes a contenido que aún no habían sido expuestos y cuyas características no podrían prever, replicando los desafíos que se presentan en el mundo real, donde los programas deben poder detectar videos *deepfake* aun cuando estos utilicen técnicas nuevas o desconocidas[170].

En noviembre de 2022 la empresa Intel presentó un novedoso software de detección de réplicas digitales llamado FakeCatcher que alega tener una tasa de precisión del 96%[171]. La tecnología presentada "*utiliza técnicas de fotopletismografía remota para observar el sutil "flujo sanguíneo" en los píxeles de una imagen, examina las señales de múltiples fotogramas y luego pasa las señales a través de un clasificador. El clasificador determina si el vídeo en cuestión es real o falso*"[172]

De a poco comienzan a surgir nuevos softwares del estilo, lo que demuestra que si bien la inteligencia artificial puede causar ciertos problemas, también puede ser la

[168] Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., & Ferrer, C. C. (2020). The DeepFake Detection Challenge (DFDC) dataset. *arXiv (Cornell University).* https://doi.org/10.48550/arxiv.2006.07397. La traducción es propia.
[169] Meta (2020).
[170] Meta (2020).
[171] *Intel Presenta un Detector de Deepfake.* (14 de noviembre de 2022). Intel Newsroom. https://www.intel.la/content/www/xl/es/newsroom/news/intel-introduces-real-time-deepfake-detector.html
[172] *Intel and Intel Labs Develop New AI Methods to Restore Trust in Media.* Intel. https://www.intel.com/content/www/us/en/research/blogs/trusted-media.html. La traducción es propia.

solución. Resulta evidente con estos ejemplos que además de una clara necesidad de herramientas tecnológicas que ayuden a detectar el contenido sintético, es preciso contar con instrumentos legales eficientes que protejan al público en general de los abusos de estas tecnologías.

4.4. Situación regulatoria actual

Regular nuevas tecnologías siempre es un desafío. Los tiempos del proceso legislativo y la rigidez de las normas resultantes muchas veces no son compatibles con el dinamismo de estas herramientas que se encuentran en constante desarrollo. Pensemos que hubiese sucedido si hubiésemos regulado la inteligencia artificial hace cinco o diez años, probablemente ese instrumento legal hoy sería en gran parte obsoleto, ya que los avances de esta tecnología han superado toda previsión.

Luego de aquella primera publicación en Reddit, las legislaciones en materia de *deepfake* no tardaron en aparecer. En 2019 tanto Estados Unidos como China promulgaron los primeros instrumentos legales en la materia. Hoy podemos encontrar leyes que procuran regular las réplicas digitales también en la Unión Europea, Reino Unido y Corea del Sur.

(a) China

China fue el primer país en regular los *deepfakes*. En enero de 2020 entró en vigencia el 'Reglamento sobre la gestión de servicios de información de audio y vídeo en línea'[173] preparado por la Administración del Ciberespacio de China (CAC por sus siglas en inglés), el Ministerio de Cultura y Turismo, y la Administración Nacional de Radio y Televisión. Si bien este documento no se ocupa exclusivamente de la regulación de contenido sintético, establece ciertas obligaciones para los proveedores y usuarios de servicios de información de audio y vídeo en línea relacionadas con el uso de nuevas tecnologías para crear, publicar o transmitir contenido falso (*deepfakes*).

[173] La norma fue consultada en el sitio oficial de la Administración del Ciberespacio de China, http://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm, y traducida para su lectura con el traductor integrado del navegador Google Chrome. A fin de corroborar la traducción, se consultó también el sitio China Law Translate, un sitio de traducción colaborativa de legislación china al idioma inglés dirigido por Jeremy Daum, miembro del Centro Paul Tsai sobre China en la Facultad de Derecho de Yale, https://www.chinalawtranslate.com/en/provisions-on-the-management-of-online-a-v-information-services/

En particular:

- Establece la obligación de identificar el material sintético como tal, etiquetándolo de manera visible.
- Prohíbe el uso de nuevas tecnologías o aplicaciones, como aquellas de aprendizaje profundo y realidad virtual, para crear, publicar o transmitir información falsa (*fake news*).
- Obliga a los proveedores de servicios de información de audio y vídeo en línea a fortalecer la gestión de la información publicada por los usuarios, estableciendo técnicas para identificar aquellos materiales contrarios a la ley, como así también materiales falsos.
- Cuando se identifique la producción, publicación o transmisión del contenido mencionado en el punto anterior, se obliga a los proveedores de servicios de información de audio y vídeo en línea a detener su transmisión y eliminarlo, evitando la difusión de dicha información, dejando registro del hecho y reportándolo a las autoridades correspondientes.

Esta normativa pone el foco en el deber de informar respecto a la naturaleza sintética del contenido, evitando así la difusión de información falsa y rumores[174], mas no hace referencia alguna al consentimiento detrás de la creación y difusión de dicho material. En un documento publicado junto a esta norma, un representante de la CAC expresó que el rápido desarrollo de los servicios de información de audio y vídeo en línea *"conlleva riesgos ocultos, como la difusión de información ilegal y errónea y la infracción de los derechos e intereses legítimos de las personas, especialmente con la aplicación de nuevas tecnologías y nuevas aplicaciones como los deepfake"*[175] y remarcó que la preocupación se centra en que estos *"puede[n] usarse para participar en actividades ilegales, poner en peligro la seguridad nacional, socavar la estabilidad social, alterar el orden social, infringir los derechos e intereses legítimos de las personas, causando riesgos para la*

[174] El artículo 13 de esta norma establece la obligación de instaurar mecanismos para disipar rumores generados a raíz de material producido mediante sistemas o aplicaciones de aprendizaje profundo o realidad virtual.

[175] *La persona relevante a cargo de la Administración del Ciberespacio de China respondió a las preguntas de los periodistas sobre el «Reglamento sobre la administración de servicios de información de audio y vídeo en línea»*. (29 noviembre de 2019). Administración del Ciberespacio de China. http://www.cac.gov.cn/2019-11/29/c_1576561821173892.htm La traducción al inglés se realizó con el traductor integrado del navegador Google Chrome. La traducción al español es propia.

seguridad política, la seguridad nacional y la seguridad pública, y afectando negativamente la estabilidad social"[176].

En enero de 2023 una nueva normativa destinada particularmente a regular los *deepfakes* entró en vigor en el territorio chino. Las 'Disposiciones sobre la administración de servicios de información de Internet de síntesis profunda'[177] preparadas por la CAC, el Ministerio de Industria y Tecnología de la Información, y el Ministerio de Seguridad Pública, establecen reglas para el uso y gestión no sólo de lo que se denomina tecnología de síntesis profunda (*deepfake*), sino también para los proveedores de los sistemas que permitan el uso de estas tecnologías y quienes les presten asistencia técnica, con el objeto de promover los valores socialistas fundamentales, salvaguardar la seguridad nacional y el interés público, y proteger los derechos e intereses legítimos de los ciudadanos, personas jurídicas y otras organizaciones[178].

Esta nueva norma refiere a las réplicas digitales como 'tecnologías de síntesis profunda' e identifica con este término a aquellas tecnologías que utilizan 'algoritmos de secuenciación generativa', como los de aprendizaje profundo y realidad virtual, para crear texto, imágenes, audio, video, escenas virtuales u otra información, incluyendo expresamente las que permitan generar, manipular o reemplazar rostros, editar atributos personales, manipular posturas, generar o editar características biométricas en imágenes y videos; como así también realizar reconstrucciones tridimensionales, simulaciones digitales y generar o editar personajes digitales y escenas virtuales; entre otros.

En particular dispone:

(i) Prohibiciones

- Prohíbe el uso de los servicios de síntesis profunda para producir, reproducir, publicar o transmitir información contraria a la ley o para participar en actividades ilegales.
- Prohíbe el uso de los servicios de síntesis profunda para producir, reproducir, publicar o transmitir información falsa (*fake news*).

[176] Administración del Ciberespacio de China (2019). La traducción al inglés se realizó con el traductor integrado del navegador Google Chrome. La traducción al español es propia.
[177] La norma fue consultada en el sitio oficial de la Administración del Ciberespacio de China, https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm, y traducida para su lectura con el traductor integrado del navegador Google Chrome. A fin de corroborar la traducción, se consultó también el ya mencionado sitio China Law Translate, https://www.chinalawtranslate.com/en/deep-synthesis/.
[178] Disposiciones sobre la administración de servicios de información de Internet de síntesis profunda. (25 de noviembre de 2022). China. Artículo 1°.

(ii) Obligaciones de los proveedores de servicios de síntesis profunda (PSSP)

- Establece la responsabilidad de los PSSP de procurar la seguridad de la información, aplicando sistemas de gestión a tal fin como por ejemplo el registro de usuarios, la revisión de algoritmos, la revisión de la información publicada, la prevención de fraude en las redes de telecomunicaciones, la seguridad de los datos y la protección de la información personal de los usuarios.
- Establece que los PSSP deberán validar la identidad de los usuarios y no podrán proveer servicios a aquellos usuarios cuya identidad no haya sido validada.
- Recae sobre los PSSP la obligación de revisar los datos ingresados por los usuarios y los resultados obtenidos por el sistema, mediante la aplicación de medidas técnicas o métodos manuales. Cuando se detecte información ilegal o dañina, deberán emplear medidas para eliminarla de conformidad con la que establezca la ley, dejando registro del hecho e informando a las autoridades correspondientes. Ante dicho suceso, los PSSP deberán tomar medidas frente a los usuarios infractores, como por ejemplo dar advertencias, restringir el uso o acceso a determinadas funciones, suspender el servicio o cerrar la cuenta.
- Los PSSP deberán instaurar mecanismos para disipar rumores, los cuales se deberán aplicar de inmediato cuando se detecte que se utilizaron servicios de síntesis profunda para producir, reproducir, publicar o transmitir información falsa, debiendo dejar registro del hecho e informar a las autoridades correspondientes.
- Cuando los PSSP y los servicios de soporte técnico proporcionen funciones para editar información biométrica, como rostros y voces, deberán solicitar a los usuarios que notifiquen a las personas cuya información personal se está editando y obtengan su consentimiento para hacerlo.
- Los PSSP deberán emplear medidas técnicas para incorporar al contenido símbolos que informen que este ha sido producido o editado por los usuarios de sus servicios.
- Asimismo, los PSSP deberán incorporar al contenido una etiqueta visible en una posición o ubicación razonable que alerte al público sobre su naturaleza, cuando los resultados obtenidos con los servicios provistos pueden causar

confusión o engañar al público. En particular estas etiquetas se deberán incluir en los materiales que resulten del uso de servicios que generan imágenes o videos de personas virtuales mediante la generación, manipulación o intercambio de rostros, manipulación de gestos o cambios significativos de las características personales.

(iii) Otras disposiciones

- Se deberá establecer un sistema para la presentación de quejas de los usuarios, debiéndose tratarlas con celeridad y otorgando una respuesta en todos los casos. Asimismo, los PSSP deberán publicar información respecto al procesamiento de dichas quejas y los plazos de respuesta.
- Las tiendas de aplicaciones de Internet y otras plataformas de distribución de aplicaciones deberán implementar mecanismos de gestión de seguridad, como por ejemplo revisar las aplicaciones de manera previa a su oferta, verificar las medidas de seguridad de las aplicaciones de tecnología de síntesis profunda y los procedimientos de presentación de quejas puestos a disposición de los usuarios. Ante cualquier violación deberán tomar las medidas correspondientes como por ejemplo emitir advertencias, suspender el servicio, excluir o eliminar la aplicación de la tienda.

A grandes rasgos, esta nueva norma continúa la línea de la anterior, reiterando algunas obligaciones ya mencionadas en el texto que entró en vigencia en 2020, como por ejemplo la prohibición de usar estos servicios o tecnologías para la difusión de noticias falsas o la necesidad de incluir un aviso que deje en manifiesto la naturaleza del material. Sin perjuicio de ello, este nuevo instrumento legal incorpora elementos interesantes que reflejan los esfuerzos de las autoridades chinas para contrarrestar los efectos de una tecnología en desarrollo que tiene un gran potencial para generar daño. Las réplicas digitales o *deepfake* se han encontrado últimamente en el epicentro del debate social y están demostrando ser un terreno complejo de regular[179]. Este nuevo texto legislativo tiene propuestas que parecieran ser atinadas, como por ejemplo establecer un mecanismo de denuncia accesible a los usuarios o exigir –al menos en ciertos casos– el consentimiento de la persona retratada. Sin embargo, contiene también algunas previsiones que en la práctica serían difíciles de aplicar, como por ejemplo las obligaciones relacionadas a evitar

[179] *Entra en vigor la normativa china para regular los deepfakes y el contenido generado por inteligencia artificial.* (1° de octubre de 2023). Reason Why. https://www.reasonwhy.es/actualidad/china-regulacion-deepfakes-etiquetado-consentimiento-inteligencia-artificial

la propagación o divulgación de contenido identificado como falso o dañino siendo que controlar la difusión de cualquier material una vez que este ha sido publicado en línea es intrínsecamente difícil[180]. Si bien normas como esta suelen abrir paso para que otros países repliquen los esfuerzos y se inspiren en sus textos, las particularidades culturales y las regulaciones locales en materia de tecnología, hacen que algunas de las previsiones de esta ley sean complejas de replicar en otros territorios, como por ejemplo la obligación de autenticar la identidad de los usuarios o de revisar el contenido creado con los servicios de síntesis profunda, ya que podría entrar en conflicto con disposiciones relacionadas a la libertad de expresión.

En agosto de 2023 entraron en vigencia las 'Medidas provisionales para la gestión de servicios de inteligencia artificial generativa'[181] que aplican al uso de inteligencia artificial generativa para proporcionar servicios que generen texto, imágenes, audio, video y otros contenidos al público dentro del territorio de la República Popular China[182]. Esta norma reitera la obligación de informar respecto de la naturaleza del contenido sintético[183], según lo establecido por las 'Disposiciones sobre la administración de servicios de información de Internet de síntesis profunda' antes comentadas.

(b) Estados Unidos

Desde la aparición del primer *deepfake* en 2017, en Estados Unidos cada año ingresan al Congreso varios proyectos de ley que proponen alguna regulación para la creación y uso de réplicas digitales. Sin embargo, a nivel federal este país no cuenta aún con ninguna legislación aprobada en la materia. En lo que va del 118° Congreso de los Estados Unidos, cuyas sesiones iniciaron el 3 de enero de 2023 y finalizarán el 3 de enero de 2025, se han ingresado tres proyectos de ley que proponen regular esta tecnología[184].

[180] Hine, E., & Floridi, L. (2022). New deepfake regulations in China are a tool for social stability, but at what cost? *Nature Machine Intelligence*, *4*(7), 608-610. https://doi.org/10.1038/s42256-022-00513-4

[181] La norma fue consultada en el sitio oficial de la Administración del Ciberespacio de China, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm, y traducida para su lectura con el traductor integrado del navegador Google Chrome. A fin de corroborar la traducción, se consultó también el ya mencionado sitio China Law Translate, https://www.chinalawtranslate.com/en/generative-ai-interim/.

[182] Medidas provisionales para la gestión de servicios de inteligencia artificial generativa (10 de julio de 2023). China. Artículo 2.

[183] Medidas provisionales para la gestión de servicios de inteligencia artificial generativa (2023). China. Artículo 12.

[184] 'Preventing Deep Fake Scams Act' H.R.5808, 'DEEPFAKES Accountability Act' H.R.5586 y 'Preventing Deepfakes of Intimate Images Act' H.R.3106.

El primer proyecto en ingresar al Congreso fue la '*Malicious Deep Fake Prohibition Act of 2018*'[185] (Ley de Prohibición de Ultra Falso Malicioso de 2018, en español) que proponía agregar al Código de los Estados Unidos[186] un artículo referido al delito de fraude en conexión con registros audiovisuales falsos que parezcan realistas, penando la creación con intención de comercialización y la distribución de *deepfakes* que faciliten una conducta criminal o ilícita.

Quizás una de las propuestas más relevantes hasta el momento ha sido la '*Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019*'[187] (Ley de Defensa de todas y cada una de las personas de apariencias falsas manteniendo la explotación sujeta a rendición de cuentas de 2019, en español), también conocida como '*DEEPFAKES Accountability Act*' (podría traducirse como Ley de Responsabilidad de Ultrafalsos) pero el proyecto no prosperó. En septiembre de 2023 se presentó una segunda versión del texto normativo[188] que además de algunos agregados interesantes –como por ejemplo una sección que establece ciertos requisitos para las plataformas en línea–, contiene modificaciones en su texto original basadas en el mejor entendimiento de esta tecnología, su funcionamiento y sus aplicaciones que se ha obtenido en los últimos cuatro años. El Cuadro 3 debajo presenta un resumen de las provisiones más destacadas del proyecto.

Cuadro 3: resumen de la 'DEEPFAKES Accountability Act' de 2023.

DEEPFAKES Accountability Act of 2023 (H. R. 5586)	
Fecha de presentación	20 de septiembre de 2023.
Definiciones	• ***Deepfake*:** cualquier grabación de video, película cinematográfica, grabación de sonido, imagen electrónica o fotografía, o cualquier representación tecnológica del habla o conducta que parezca representar auténticamente cualquier discurso o conducta de una persona que en realidad no participó en dicho discurso o conducta; y cuya producción dependió sustancialmente de medios técnicos, en lugar de la capacidad de otra persona para hacerse pasar por dicha persona física o verbalmente.

[185] Malicious Deep Fake Prohibition Act of 2018, S. 3805, 115th Congress (2017-2018). https://www.congress.gov/bill/115th-congress/senate-bill/3805

[186] El '*United States Code*' o '*U.S. Code*' es una compilación de la mayoría de las leyes federales vigentes de los Estados Unidos, organizado por materia. La primera versión del Código fue publicada en 1926 y ha sido modificado numerosas veces desde entonces.

[187] Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019, H. R. 3230, 116th Congress (2019-2020). https://www.congress.gov/bill/116th-congress/house-bill/3230

[188] Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023, H. R. 5586, 118th Congress (2023-2024). https://www.congress.gov/bill/118th-congress/house-bill/5586

	• **Registro Tecnológico Avanzado de Personificación Falsa:** todo *deepfake* que una persona razonable, habiendo considerado las cualidades visuales o de audio del registro y la naturaleza del canal de distribución en el que aparece el registro, creería que exhibe con precisión cualquier comportamiento de una persona viva o fallecida que en realidad esta no haya realizado, y cuya exhibición es sustancialmente probable que promueva un acto criminal o resulte en una interferencia indebida en un procedimiento oficial, un debate de política pública, o una elección; y que haya sido producido sin consentimiento del retratado o sus herederos.
Naturaleza del contenido	Se establece la obligación de que el material que represente a una persona sin su consentimiento contenga tecnologías que identifiquen claramente que dicho registro incluye elementos visuales o de audio alterados, o que ha sido creado en su totalidad mediante inteligencia artificial generativa o tecnologías similares.
Transparencia	Establece que aquel material que represente a una persona sin su consentimiento deberá cumplir ciertos requisitos para garantizar la trasparencia de su naturaleza. Deberá incluir: • al menos: (a) una declaración verbal claramente articulada, o (b) una declaración escrita claramente legible que aparezca en la parte inferior de la imagen durante toda su duración, que identifique que el registro contiene elementos visuales y de audio alterados, y una descripción concisa del alcance de dicha alteración; y • un enlace, ícono o similar para indicar que el contenido ha sido alterado o es producto de inteligencia artificial generativa o una tecnología similar.
Infracciones	Incorpora consecuencias penales y civiles para quienes no cumpla con los requisitos de transparencia, o los alteren a fin de eliminarlos u ocultarlos.
Privacidad	Prevé la posibilidad de que el accionante solicite que las actuaciones no sean públicas cuando considere que el contenido del material puede generarle un daño.
Asistencia a la víctima	Incluye un apartado dedicado a medidas de asistencia a la víctima de *deepfakes*, en particular prevé la asignación de un coordinador para la recepción de denuncias de víctimas de representaciones de naturaleza íntima y sexual.
Desarrolladores de software	Establece que cualquier persona que, con fines comerciales, desarrolle un producto que razonablemente crea que se utilizará para producir *deepfakes*, deberá: • garantizar que dicho producto tenga la capacidad técnica para insertar identificadores digitales de la procedencia del contenido y las declaraciones exigidas por el presente proyecto para garantizar la transparencia de la naturaleza del mismo; e • incluir al producto términos de uso u otras divulgaciones análogas, que requieran que el usuario reconozca afirmativamente sus obligaciones legales en relación con el contenido a producir con dicho producto.
Detección	Prevé la creación de un grupo de trabajo dentro de la Dirección de Ciencia y Tecnología del Departamento de Seguridad Nacional que se encargará, entre otras cosas, de: • promover los esfuerzos del gobierno de los Estados Unidos para combatir las implicaciones de seguridad nacional de los *deepfakes*; e • investigar y desarrollar tecnologías para detectar, o de otro modo contrarrestar y combatir los *deepfakes* y otros métodos avanzados de manipulación de imágenes.
Plataformas en línea	Establece que los proveedores de plataformas en línea deberán: • garantizar que dicha plataforma tenga la capacidad técnica para insertar identificadores digitales de la procedencia del contenido y las declaraciones exigidas por el presente proyecto para garantizar la transparencia de la naturaleza del mismo, en cualquier *deepfake* que se distribuya en la plataforma; y • contar con un sistema para detectar *deepfakes* en el contenido distribuido en dicha plataforma. Se entiende como "plataforma en línea" cualquier sitio web público, servicio en línea, aplicación en línea o aplicación móvil que se opera con fines comerciales y proporciona un foro comunitario para contenido generado por el usuario, incluido un

	sitio de red social, servicio de agregación de contenido o servicio para compartir vídeos, imágenes, juegos, archivos de audio u otro contenido.

Fuente: elaboración propia en base al texto de la norma.

A nivel estadual, varias jurisdicciones dentro de los Estados Unidos han promulgado normas que regulan la creación de réplicas digitales. La mayoría de ellas han optado por regular ciertos casos específicos en lugar de establecer lineamientos generales para el uso de esta tecnología. El Cuadro 4 detalla la legislación en materia de *deepfakes* que ha sido aprobada hasta el momento en los distintos estados.

Cuadro 4: legislación en materia de réplicas digitales en los estados de EE.UU.

California	
AB 602[189] (Presentado en febrero 2019 y promulgado en octubre 2019)	• Establece que un individuo puede accionar contra quien haya: ▪ creado y divulgado intencionalmente material sexualmente explícito conociendo o debiendo haber razonablemente conocido que el individuo representado en ese material no dio su consentimiento para su creación o divulgación; o ▪ divulgado intencionalmente material sexualmente explícito que la persona representada no creó, conociendo que este no dio su consentimiento para la creación de dicho contenido. • Prevé ciertas excepciones, como por ejemplo cuando el material sea de interés público, tenga valor político o periodístico, se trate de una crítica o comentario protegido de algún modo por la Constitución de California o la de los Estados Unidos. • Aclara expresamente que dicho material no tendrá valor periodístico basado solamente en el hecho de que el individuo representado sea una figura pública. • No acepta como defensa la inclusión de una leyenda o *disclaimer* que lea que la persona representada no consintió en el uso de su imagen o no participó en la creación del material.
SB 1216[190] (Presentado en febrero 2022 y promulgado en septiembre 2022)	Prevé que el Secretario de Operaciones Gubernamentales deberá evaluar, entre otras cosas, el impacto de la proliferación de *deepfakes* y los riesgos, incluidos aquellos relacionados a la privacidad, asociados con la implementación de tecnologías de falsificación de contenido digital y *deepfakes* en el gobierno, las empresas y los residentes del estado de California. Asimismo, ordena evaluar las mejores prácticas para prevenir la falsificación de contenido digital y los *deepfake*, analizando en particular si la adopción de un estándar de procedencia de contenido digital podría ayudar a reducir la proliferación de falsificaciones de contenido digital y *deepfakes*.
Georgia	
SB 337[191] (Presentado en enero 2020 y	Pena a quien conociendo el contenido de una transmisión o publicación y sin el consentimiento de la persona representada transmite o publica electrónicamente o provoca la transmisión o publicación electrónica de una fotografía o video que muestra desnudez o alguna conducta sexualmente explícita de un adulto, incluyendo

[189] Depiction of individual using digital or electronic technology: sexually explicit material: cause of action, Assembly Bill No. 602, California Legislature 2019-2020 Regular Session. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB602

[190] An act to add and repeal Section 11547.5 of the Government Code, relating to technology, Senate Bill No. 1216, California Legislature 2021-2022 Regular Session. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB1216

[191] Invasion of Privacy; prohibition against the transmission of photography depicting nudity; include falsely created videographic or still images, SB 337, Georgia General Assembly 2019-2020 Regular Session. https://www.legis.ga.gov/legislation/57062

promulgado en agosto 2020)	un video o imagen creada falsamente, con la finalidad de acosar o causar daños financieros a la persona retratada.
SB 78[192] (Presentado en febrero 2021 y promulgado en julio 2021)	Pena a quien conociendo el contenido de una transmisión o publicación y sin el consentimiento de la persona representada transmite o publica electrónicamente o provoca la transmisión o publicación electrónica de una fotografía o video que muestra desnudez o alguna conducta sexualmente explícita de un adulto, incluyendo un video o imagen creada falsamente, en un sitio web, un sitio de intercambio de archivos entre pares (*peer-to-peer*), galería de miniaturas (*thumbnails*), publicación de galería de películas, listas vinculadas, cámaras web en vivo, páginas web o tablero de mensajes que anuncia o promueve su servicio mostrando, anticipando o distribuyendo una conducta sexualmente explícita, con la finalidad de acosar o causar daños financieros a la persona retratada.
Hawái	
SB 309[193] (Presentado en enero 2021 y promulgado en junio 2021)	Agrega dentro de los delitos contra la intimidad la creación, divulgación o amenaza de divulgación de una imagen o un video de una persona ficticia representada desnuda o participando en una conducta sexual, que incluya las características físicas reconocibles de una persona real, de modo que la imagen o el video parezca que representa a dicha persona y no a una persona ficticia, con la intención de generar un daño sustancial en la salud, seguridad, negocios, vocación, carrera, educación, condición financiera, reputación o relaciones personales del sujeto representado, o como un acto de venganza.
Luisiana	
SB 426[194] (Presentado en abril 2022 y promulgado en junio 2022)	• Establece dentro de los escenarios de apropiación indebida de la identidad, la utilización de la réplica digital de una persona en la presentación pública de una obra audiovisual guionada o en una presentación en vivo de una obra dramática, cuando dicho uso tiene como objetivo crear –y crea– la impresión de que el intérprete representado está en realidad interpretando el rol de un personaje ficticio. • Al definir el concepto de "identidad", además del nombre, la voz, la firma, la fotografía, la imagen y la semejanza, la norma incluye expresamente a la réplica digital de un individuo.
SB 175[195] (Presentado en abril 2023 y promulgado en junio 2023)	Establece un régimen legal para "*deepfakes* ilegales", penando: • a quien cree o posea a sabiendas material *deepfake* que represente a un menor participando en una conducta sexual, como así también a quien anuncie, distribuya, exhiba, intercambie, promueva o venda dicho material; • a cualquier persona que, con conocimiento de que el material es un *deepfake* no consentido que representa a una persona participando de una conducta sexual, anuncie, distribuya, exhiba, intercambie, promueva o venda dicho material.
Minnesota	
HF 1370[196]	• Prevé la posibilidad de accionar contra la difusión no consensuada de un *deepfake* cuando:

[192] Invasion of Privacy; prohibition on electronically transmitting or posting nude or sexually explicit photographs or videos for purposes of harassing the depicted person; revise, SB 78, Georgia General Assembly 2021-2022 Regular Session. https://www.legis.ga.gov/legislation/59239

[193] Relating To Privacy, SB309, Legislature of the State of Hawaii 2021 Regular Session. https://www.capitol.hawaii.gov/session/archives/measure_indiv_Archives.aspx?billtype=SB&billnumber=309&year=2021

[194] Allen Toussaint Legacy Act (2022).

[195] Criminalizes deepfakes involving minors and defines the rights to digital image and likeness, SB 175, Louisiana 2023 Regular Session. https://legiscan.com/LA/bill/SB175/2023

[196] Cause of action for nonconsensual dissemination of deep fake sexual images established, crime of using deep fake technology to influence an election established, and crime for nonconsensual dissemination of deep fake sexual images established, HF 1370, Minnesota Legislature 2023-2024 Regular Session. https://www.revisor.mn.gov/bills/text.php?number=HF1370&type=bill&version=3&session=ls93&session_year=2023&session_number=0

(Presentado en febrero 2023 y promulgado en mayo 2023)	▪ una persona difundió un *deepfake* sabiendo que el individuo representado no dio su consentimiento para su difusión pública; ▪ el *deepfake* representa de manera realista cualquiera de los siguientes: (i) partes íntimas de otro individuo presentadas como las partes íntimas del individuo representado, (ii) partes íntimas generadas artificialmente y presentadas como partes íntimas del individuo representado, o (iii) el individuo representado participando en un acto sexual; y ▪ el individuo representado es identificable a partir del propio material o de la información personal mostrada en relación con este. • El hecho de que el individuo representado haya dado su consentimiento para la creación del *deepfake* o para su transmisión privada no exime de responsabilidad a la persona que haya difundido dicho material con conocimiento de que el individuo representado no consintió su difusión pública.
Nueva York	
S 5959[197] (Presentado en mayo 2019 y promulgado en noviembre 2020)	Pena el uso de la réplica digital de un artista fallecido en una obra audiovisual guionada como personaje de ficción o en la interpretación en vivo de una obra musical sin consentimiento previo.
S1042/A3596[198] (Presentado en enero 2023 y promulgado en septiembre 2023)	Pena la difusión o publicación de una imagen o video que represente a una persona con partes íntimas expuestas o participando en una conducta sexual, incluso cuando se trate de una imagen o video creado o alterado mediante digitalización[199], cuando dicha persona pueda ser identificada a partir del material en sí mismo o de la información mostrada en conexión con este, y con la intención de causar daño al bienestar emocional, financiero o físico de dicha persona.
Texas	
SB 751[200] (Presentado en febrero 2019 y promulgado en junio 2019)	Dentro de los treinta días anteriores a una elección pena la creación, publicación y distribución de un video *deepfake* con la intención de dañar a un candidato o influir en el resultado de la misma.
SB 1361[201] (Presentado en marzo 2023 y promulgado en junio 2023)	Pena la producción y distribución por medios electrónicos de un video *deepfake* que aparente representar a una persona con sus partes íntimas expuestas o participando en actividades sexuales, sin el consentimiento efectivo de la persona retratada.

[197] An act to amend the civil rights law, in relation to establishing the right of publicity and to providing a private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual, S5959, The New York State Senate 2019-2020 Legislative Session. https://www.nysenate.gov/legislation/bills/2019/S5959#:~:text=2019%2DS5959%20%2D%20Summary-,Establishes%20the%20right%20of%20publicity%20and%20provides%20for%20a%20private,explicit%20depiction%20of%20an%20individual

[198] Prohibits unlawful dissemination or publication of intimate images created by digitization and of sexually explicit depictions of an individual; repealer, Senate Bill S1042A, The New York State Senate 2023-2024 Legislative Session. https://www.nysenate.gov/legislation/bills/2023/S1042/amendment/A

[199] La norma define el término "digitalización" como la alteración de una imagen de manera realista utilizando imagen/es de una persona, distinta de la persona representada, o imágenes generadas por computadora.

[200] Relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election, SB 751, Texas Legislature 86th Legislative Session (2019). https://capitol.texas.gov/BillLookup/History.aspx?LegSess=86R&Bill=SB751

[201] Relating to the unlawful production or distribution of sexually explicit videos using deep fake technology; creating a criminal offense, SB 136, Texas Legislature 88th Legislative Session (2023). https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=SB1361

Virginia	
HB 2678[202] (Presentado en enero 2019 y promulgado en marzo 2019)	• Pena la difusión y venta de videos o imágenes creadas por cualquier medio, incluyendo aquellas creadas falsamente, que representen a una persona totalmente desnuda, o en estado de desnudez, con la intención de coaccionarla, acosarla o intimidarla, cuando dicha persona sepa o tenga motivos para saber que no tiene licencia o autorización para difundir o vender dicho material. • Prevé expresamente que los proveedores de servicios de Internet, proveedores de servicios de correo electrónico o cualquier otro servicio, sistema o software de acceso a la información que proporcione o permita el acceso de varios usuarios a un servidor informático para cometer actos prohibidos en virtud de esta norma, no serán responsable por los daños causados por el contenido proporcionado por otra persona.
Washington	
SB 5152[203] (Presentado en enero 2023 y promulgado en mayo 2023)	• Establece la posibilidad de que candidatos a cargos electivos soliciten medidas cautelares u otras similares prohibiendo la publicación de material en el que, usando medios sintéticos[204], se haya alterado su apariencia, acciones o discurso en comunicaciones electorales, facultándolos también para accionar por daños y perjuicios. • Permite como defensa alegar que el material incluía una leyenda indicando que se trata de una imagen o video manipulado. • Establece que podrán ser considerados responsables por los daños causados los patrocinadores de la comunicación electoral, mas no el medio de comunicación utilizado, salvo que este último hubiese eliminado la leyenda que divulga que el material ha sido manipulado o que hubiese cambiado el contenido de una comunicación electoral de manera tal que califique como contenido sintético. Esto último aplica asimismo a proveedores o usuarios de servicios informáticos interactivos[205].

Fuente: elaboración propia en base a la normativa de cada estado.

Del análisis de las normas citadas se destacan dos situaciones en particular en las cuales las distintas jurisdicciones parecieran hacer foco en materia de regulación de *deepfakes*: el uso para representar escenas de tenor sexual y su uso en el contexto de una elección. Con las elecciones presidenciales como motivación principal, el sitio web Bloomberg Law reporta que al menos siete estados más tratarán proyectos en materia de réplicas digitales y sus usos en campañas políticas durante 2024[206].

[202] Unlawful dissemination or sale of images of another; penalty, HB 2678, Virginia Legislature 2019 Regular Session. https://lis.virginia.gov/cgi-bin/legp604.exe?191+sum+HB2678

[203] Defining synthetic media in campaigns for elective office, and providing relief for candidates and campaigns, SB 5152, Washington State Legislature 2023-2024 Regular Session. https://app.leg.wa.gov/billsummary/?billNumber=5152&year=2023&initiative=False

[204] El texto normativo entiende "medios sintéticos" como toda imagen, audio o video de la apariencia, discurso o conducta de un individuo que ha sido manipulado intencionalmente con el uso de técnicas de redes generativas adversarias u otra tecnología digital de manera que se cree una imagen. audio o vídeo realista pero falso de algo que realmente no ocurrió.

[205] La norma define "servicio informático interactivo" como cualquier servicio de información, sistema o proveedor de software de acceso que permite el acceso de múltiples usuarios a un servidor informático, incluido específicamente servicio que proporciona acceso a Internet y dichos sistemas operados u ofrecidos por bibliotecas o instituciones educativas.

[206] Williams, Z. (22 de diciembre de 2023). More States to Push Laws Banning AI Election Deepfakes in 2024. *Bloomberg Law*. https://news.bloomberglaw.com/artificial-intelligence/more-states-to-push-laws-banning-ai-election-deepfakes-in-2024

A diferencia de lo que prevé la *DEEPFAKES Accountability Act* a nivel federal, las normas aprobadas por los distintos estados prohíben la creación, uso o distribución según el caso de réplicas digitales no consentidas en determinados casos, pero no hacen referencia alguna a los usos consentidos, ni establecen obligaciones de informar respecto al origen del material o su naturaleza.

(c) Unión Europea

La Unión Europea no cuenta con una ley que regule el uso y explotación de réplicas digitales de manera individualizada, aunque sí tiene algunas previsiones al respecto en otras normas que tratan temas de inteligencia artificial y regulan el entorno digital. Una de ellas se encuentra en la 'Ley de Inteligencia Artificial' originalmente sancionada por el Parlamento Europeo en 2021[207] y reformada en junio de 2023[208]. El texto original de la norma incluía un solo artículo en donde se hacía mención a los contenidos ultrafalsos (*deepfakes*), el cual se encontraba dentro de las obligaciones de transparencia establecidas para determinados sistemas de inteligencia artificial y hacía referencia a la obligación de informar sobre la naturaleza del contenido sintético, estableciendo ciertas excepciones a esta obligación cuando se tratara de usos legítimos como el uso en el ejercicio del derecho a la libertad de expresión.

La reforma de 2023 trajo varios cambios, entre ellos incorporó una definición del término 'ultrafalsificación' estableciendo que se entiende por este "*un contenido de sonido, imagen o vídeo manipulado o sintético que puede inducir erróneamente a pensar que es auténtico o verídico, y que muestra representaciones de personas que parecen decir o hacer cosas que no han dicho ni hecho, producido utilizando técnicas de inteligencia artificial, incluido el aprendizaje automático y el aprendizaje profundo*"[209].

Otra novedad es que el texto actualizado ahora hace mención expresa al consentimiento del retratado al referirse a las representaciones de personas que parecen

[207] Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206&qid=1706173872479

[208] Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 — C9-0146/2021 — 2021/0106(COD)), https://eur-lex.europa.eu/eli/C/2024/506/oj

[209] Enmiendas a la Ley de Inteligencia Artificial (2023). Enmienda 203, artículo 3.1.44 quinquies.

decir o hacer cosas que no han dicho ni hecho[210], detalle que no se había incluido en la redacción original. Asimismo, agrega una previsión especial para los casos en los que el contenido sintético forme parte de obras cinematográficas, estableciendo que en el caso de usos claramente creativos, satíricos, artísticos o ficticios, de imágenes de videojuegos y de obras o formatos análogos, el cumplimiento de la obligación de transparencia e información antes referida podrá realizarse de manera que no obstaculice la presentación de la obra, aunque debiendo siempre ser clara y visible[211]. En todos los casos este deber de información debe cumplirse en la primera interacción o exposición del contenido y ser accesible también para personas vulnerables, como las personas con discapacidad o los niños[212]. El nuevo texto incorpora también la obligación de proveer a los usuarios con procedimientos de intervención o de denuncia de contenido ultrafalso[213].

Otro de los instrumentos legales comunitarios que hacen referencia a los *deepfakes* es la 'Ley de Servicios Digitales'[214], aprobada por el Parlamento Europeo en octubre de 2022, que pretende regular el entorno en línea a fin de garantizar la seguridad y los derechos de los usuarios de servicios digitales. Dentro de las obligaciones de las plataformas en línea y los motores de búsqueda en línea de 'muy gran tamaño'[215] establece algunas relacionadas a la reducción de riesgos, entre ellas se incluye una relacionada a los *deepfake*. El artículo 35.1.k establece el deber de informar respecto a la naturaleza del contenido sintético mediante indicaciones destacadas, como también la obligación de proporcionar a los usuarios una funcionalidad que permita realizar estas demarcaciones de manera sencilla.

En ambos casos el foco de la regulación se pone en el deber de informar, en la obligación de identificar al contenido ultrafalso como tal. En el caso de la Ley de Inteligencia Artificial, si bien en materia de réplicas digitales el texto reformado es

[210] Enmiendas a la Ley de Inteligencia Artificial (2023). Enmienda 486, artículo 52.3.
[211] Enmiendas a la Ley de Inteligencia Artificial (2023). Enmienda 487, artículo 52.3 bis, que reemplaza el segundo párrafo del artículo 52.3.
[212] Enmiendas a la Ley de Inteligencia Artificial (2023). Enmienda 488 a artículo 52.3 ter, incorporado en la reforma.
[213] Enmiendas a la Ley de Inteligencia Artificial (2023). Enmienda 488 a artículo 52.3 ter, incorporado en la reforma.
[214] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1706350038236
[215] El artículo 33.1 de la citada ley define a las plataformas en línea y los motores de búsqueda en línea de muy gran tamaño como aquellos que tengan un promedio mensual de destinatarios del servicio activos en la Unión Europea igual o superior a cuarenta y cinco millones y a las que se designe como tales.

considerablemente mejor e incorpora excepciones que otras legislaciones no prevén –como la relacionada a los usos en la industria audiovisual–, aun así tiene varias falencias. Quizás una de las más importantes viene dada por el poco énfasis realizado en materia de consentimiento.

(d) Reino Unido

En octubre de 2023 la '*Online Safety Act*'[216] (Ley de seguridad en línea, en español) obtuvo Sanción Real y pasó a ser ley en el territorio del Reino Unido. Este proyecto que se está discutiendo, en distintas versiones, desde 2019, propone controlar el contenido ilegal y dañino que circula en Internet, recayendo en las plataformas el deber de cuidado de sus usuarios. Según su artículo 1° "*[e]sta Ley establece un nuevo marco regulatorio cuyo objetivo general es hacer que el uso de los servicios de Internet […] sea más seguro para las personas en el Reino Unido".*

El alcance de esta norma es bastante amplio y establece obligaciones para proveedores de una gran diversidad de servicios en línea (redes sociales, motores de búsqueda, foros, juegos, chat, citas en línea y mensajería). Entre ellas establece la obligación de los proveedores de 'servicios de usuario a usuario'[217] de establecer procedimientos que permitan denunciar contenido, que sean de fácil acceso, sencillos de usar –incluso para niños– y trasparentes[218]. En general se debe garantizar que los usuarios y terceras personas afectadas que se encuentren en el Reino Unido puedan denunciar contenido ilícito.

Si bien esta norma no regula de manera expresa las réplicas digitales, en un artículo[219] que agrega a la 'Ley de delitos sexuales de 2003' referido al delito de enviar material que contenga los genitales de una persona, se prevé que este material incluye también aquellas imágenes que sean generadas o alteradas mediante gráficos por

[216] A Bill to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes (Online Safety Act 2023), 2023 c. 50, Sesiones 2021-22 y 2022-23. https://www.legislation.gov.uk/ukpga/2023/50/introduction/enacted

[217] En su artículo 3 la ley define los 'servicios de usuario a usuario' como aquellos servicios de Internet mediante los cuales el contenido que es generado por un usuario directamente en el servicio, o subido o compartido en este, puede ser encontrado por otro usuario. A los fines de esta definición, no importa si el contenido es efectivamente compartido con otro usuario o usuarios siempre que el servicio tenga una funcionalidad que permita dicho intercambio; como así tampoco importa qué proporción del contenido del servicio tenga estas características.

[218] Online Safety Act (2023). Artículo 72(6).

[219] Online Safety Act (2023). Artículo 187.

computadora o de cualquier otra manera, que aparenten ser una fotografía o un video, como así también los datos almacenados por cualquier medio que sean capaces de convertirse en una fotografía, video o imagen como las antes descriptas. Se entiende entonces que compartir réplicas digitales con tenor sexual está penado por dicha ley.

(e) Corea del Sur

En el año 2020 se incorporó a la 'Ley sobre casos especiales relativos a la sanción de delitos sexuales'[220] de Corea del Sur un artículo que regula la distribución de material audiovisual falso (*deepfakes*). Este pena a quien edite, sintetice o procese fotografías, videos o audio del rostro, cuerpo o voz de una persona con fines de difundirlo en contra de su voluntad y de forma que pueda provocar deseo sexual en terceros o vergüenza a la persona retratada. El artículo castiga este comportamiento incluso luego de la muerte del sujeto representado en el material y establece una pena un poco mayor para los casos en que este delito sea cometido por medio de redes de información y comunicación con el objeto de obtener ganancias. Cuando una persona cometa estos delitos de manera habitual, corresponderá una pena agravada.

Al igual que otros casos ya analizados, Corea del Sur no cuenta con una regulación específica de *deepfakes*, sino que prohíbe un uso en particular. A diferencia de lo que sucede por ejemplo en Reino Unido que aplica una restricción similar, en esta norma sí se hace referencia al consentimiento del sujeto retratado, penando aquellos casos en los que no se cuenta con este. Resulta interesante el agregado final del artículo que plantea la recurrencia como agravante, ya que dada la naturaleza del delito no sería de extrañar que esto ocurriese.

En diciembre de 2023 la Asamblea Nacional de Corea del Sur aprobó[221] una reforma de la 'Ley de elección de funcionarios públicos'[222] que incorpora la prohibición de usar *deepfakes* en campañas políticas desde noventa días antes de las elecciones. La reforma incluye también la obligación de los creadores de *deepfakes* en el contexto de una

[220] Ley sobre casos especiales relativos a la sanción de delitos sexuales. Ley No. 11556 (18 de diciembre de 2012). Corea del Sur. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=63351&type=lawname&key=ACT+ON+SPECIAL+CASES+CONCERNING+THE+PUNISHMENT+OF+SEXUAL+CRIMES

[221] *Nat'l Assembly passes revised bill banning deepfakes in campaigns.* (20 de diciembre de 2023). KBS WORLD. https://world.kbs.co.kr/service/news_view.htm?lang=e&id=Po&Seq_Code=182572

[222] Ley de elección de funcionarios públicos. Ley No. 7681 (4 de agosto de 2005). Corea del Sur. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=60172&type=lawname&key=Public+Official+Election+Act

campaña, sin restricción temporal, a advertir cuando el material incluye contenido sintético[223].

El uso de réplicas digitales en campañas políticas no es una novedad en este país, siendo que en las elecciones presidenciales de 2022 tanto Yoon Suk Yeol –actual presidente– como el candidato de la oposición, Lee Jae-myung, utilizaron réplicas digitales de sus personas en videos de campaña. "AI Yoon" fue una sensación durante las últimas elecciones y un elemento esencial a la hora de traccionar el voto joven. Se trata de una réplica digital del actual presidente, que si bien se ve igual a este, prolijamente peinado y con su traje impecable, utiliza lenguaje atrevido y juvenil a fin de atraer la atención de aquel segmento de votantes más jóvenes[224].

(f) América Latina

En nuestra región, salvo en México[225], no se detectaron proyectos de ley que propongan una regulación para las réplicas digitales como está sucediendo en otras partes del mundo.

En particular en Argentina se detectaron tres proyectos de ley presentados entre noviembre y diciembre de 2023 que proponen reformar el artículo 128 del Código Penal de la Nación que pena la producción, posesión y distribución –entre otros– de pornografía infantil. En líneas generales, los proyectos proponen ampliar el texto de la norma para incorporar incluso aquellos casos en que se trate de una representación real o simulada de un menor[226], aun cuando no se represente a ningún menor en particular, e

[223] 90-day ban on deepfake political ads passes parliamentary special committee. (5 de diciembre de 2023). *The Korea Times.* https://www.koreatimes.co.kr/www/nation/2023/12/113_364513.html

[224] Deepfake democracy: South Korean candidate goes virtual for votes. (14 de febrero de 2022). *France 24.* https://www.france24.com/en/live-news/20220214-deepfake-democracy-south-korean-candidate-goes-virtual-for-votes

[225] El diputado Miguel Torruco Garza ha presentado ante la legislatura mexicana un proyecto de ley para incorporar al Código Penal Federal un artículo penando "*a quien modifique videos, audios, rostro de personas, grabaciones de voz y/o de escenarios ficticios, con la intención de hacerlos pasar como reales, en detrimento de las actividades personales y profesionales de alguna persona física o moral*". Véase González, F. (15 de noviembre de 2023). Crear deepfakes con IA en México podría costar hasta ocho años de cárcel. *WIRED.* https://es.wired.com/articulos/crear-deepfakes-con-ia-en-mexico-podria-costar-hasta-ocho-anos-de-carcel; Cámara de Diputados LXV Legislatura México (8 de enero de 2024). *Busca iniciativa sancionar uso delictivo de la tecnología denominada inteligencia artificial. Boletín No. 5793 https://comunicacionsocial.diputados.gob.mx/index.php/boletines/-busca-iniciativa-sancionar-uso-delictivo-de-la-tecnologia-denominada-inteligencia-artificial*

[226] Véase Milman, G. (2 de noviembre de 2023). Proyecto de Ley 4411-D-2023. *Código Penal. Modificación del artículo 128, sobre el uso de técnicas de inteligencia artificial para la difusión de imágenes de contenido sexual.* https://www.hcdn.gob.ar/diputados/gmilman/proyecto.html?exp=4411-D-2023; Romero, J. C. (14 de diciembre de 2023). Proyecto de Ley 2469-S-2023. *Modificación al artículo 128 del Código Penal, Ley 11179, respecto de sancionar delitos contra la integridad sexual a través del uso de inteligencia artificial*

independientemente de si el material tiene carácter realista o no[227]. Adicionalmente, se detectó un proyecto que propone incorporar dentro de la descripción de violencia digital prevista en la Ley 26.485 de Protección Integral a las Mujeres (artículo 6 inciso i) "*la obtención, reproducción y difusión por técnicas de Inteligencia Artificial o cualquier otro medio tecnológico, sin consentimiento de material real, total o parcialmente falso, editado, intimo o de desnudez, que se le atribuya a las mujeres*"[228]. Si bien todas las propuestas mencionadas son muy recientes pareciera que todas ellas apuntan a regular un uso en particular de las réplicas digitales, aquel que perjudica la integridad sexual y la honra del retratado.

4.5. Breve análisis estructural de la legislación existente

Un informe del Panel para el futuro de la Ciencia y la Tecnología (STOA) [229] del Parlamento Europeo identifica cinco dimensiones dentro del ciclo de vida de un *deepfake*: tecnología, creación, circulación, objetivo y audiencia; y plantea que los encargados de elaborar política pública en materia de réplicas digitales deberían tener en cuenta estas dimensiones a fin de procurar mitigar los efectos adversos asociados a su mal uso.

La dimensión 'tecnología' hace referencia a la tecnología detrás de los *deepfakes* y se enfoca en quienes la producen y suministran. La dimensión 'creación' refiere justamente a la creación de material sintético y las aplicaciones de los programas –software– que se utilizan para tal fin, mientras que la dimensión 'circulación' se enfoca en la distribución y circulación de estos materiales, incluyendo por lo general disposiciones destinadas a los intermediarios de servicios de Internet y las plataformas. Por su parte, la dimensión 'objetivo' se centra en el sujeto afectado por la réplica digital, la víctima; mientras que la dimensión 'audiencia' se enfoca en los usuarios y cómo estos se comportan ante los *deepfakes*.

(IA) o cualquier mecanismo tecnológico. https://www.senado.gob.ar/parlamentario/comisiones/verExp/2469.23/S/PL;

[227] Véase Lospennato, S. G. (3 de noviembre de 2023). Proyecto de Ley 4436-D-2023. *Código Penal. Modificación del Artículo 128, sobre el uso de técnicas de inteligencia artificial para la difusión de imágenes de contenido sexual*. https://www.hcdn.gob.ar/comisiones/permanentes/clpenal/proyecto.html?exp=4436-D-2023

[228] Véase Milman, G. (2 de noviembre de 2023). Proyecto de Ley 4410-D-2023. *OLIMPIA - Ley 27736 - Modificación del artículo 4, incorporando la utilización de la inteligencia artificial para la difusión de imágenes de contenido sexual.* https://www.hcdn.gob.ar/comisiones/permanentes/cmujeresydiv/proyecto.html?exp=4410-D-2023

[229] Huijstee, M. V., Boheemen, P. V., Das, D., Nierling, L., Jahnel, J., Karaboga, M., & Fatun, M. (2021). *Tackling deepfakes in European policy*. Publications Office of the European Union. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

Yinuo Geng del Centro de Seguridad Nacional y el Derecho de la Universidad de Georgetown ha analizado[230] las distintas normas que incluyen previsiones relacionadas a las réplicas digitales en Estados Unidos, la Unión Europea y China, y ha identificado diferentes métodos para analizar la regulación de estas tecnologías dividiendo la legislación existente en la materia en tres categorías:

- según qué parte del ciclo de vida de los *deepfakes* los legisladores intentan regular, tomando de referencia las dimensiones planteadas por el STOA;
- según se regulen determinados usos o se aplique un enfoque basado en evaluación de riesgos; o
- según se regule el tema en específico o dentro del marco de una norma más amplia, como por ejemplo aquellas referidas a la inteligencia artificial en general.

En base a esto, el Cuadro 5 debajo propone un breve análisis de la estructura de las legislaciones citadas en el presente.

Cuadro 5: breve análisis estructural de la legislación existente.

Territorio	¿Qué parte del ciclo regula?	¿Regula determinados usos o aplica enfoque basado en evaluación de riesgos?	¿Regulación específica o dentro de otra norma?
China	Apunta a las tres primeras etapas del ciclo de vida de un *deepfake*, tecnología, creación y circulación, siendo que las obligaciones que se establecen se centran en la identificación de los usuarios, el etiquetado del contenido sintético y la responsabilidad de las plataformas y proveedores de servicios de Internet.	Podemos decir que utiliza un enfoque basado en evaluación de riesgos, considerando que las previsiones de las normas citadas no se enfocan en casos particulares sino que son más bien amplias.	Posee regulación específica en la materia.
Estados Unidos	En general las normas de los distintos estados están enfocadas más en proteger tanto a los usuarios como a las víctimas del mal uso de estas tecnologías, por lo que se podría decir que el foco está puesto en las dimensiones objetivo y audiencia.	Se regulan determinados usos.	A nivel federal existen propuestas que regulan el tema en particular. A nivel estadual prima la regulación de la materia dentro de normas más amplias o referidas a otros temas.
Unión Europea	Se centra en la creación y circulación, poniendo el foco en la identificación de la naturaleza del contenido.	Utiliza un enfoque basado en evaluación de riesgos.	El tema se regula dentro del marco de normas más amplias.

[230] Geng, Y. (2023). Comparing "Deepfake" Regulatory Regimes in the United States, the European Union, and China. *Georgetown Law Technology Review*, 7 (1), 157-178.

Reino Unido	En este caso el foco se puede decir que se encuentra en la etapa de circulación y la dimensión objetivo, ya que si bien busca proteger a los sujetos afectados por estas tecnologías, también establece obligaciones para las plataformas donde se difunde el contenido.	Se regulan determinados usos.	El tema se regula dentro del marco de una norma más amplia.
Corea del Sur	Se centra en la protección del usuario y el sujeto representado, es decir, en las dimensiones objetivo y audiencia.	Se regulan determinados usos.	El tema se regula dentro del marco de normas referidas a otros temas.

Fuente: elaboración propia en base al texto de Geng, Y. (2023) y la normativa de cada país.

5. Parámetros y lineamientos para la regulación de réplicas digitales

Como se ha observado, ya son varias las jurisdicciones que se han ocupado de regular al menos ciertos aspectos de las réplicas digitales y el contenido sintético, habiendo también otras más con proyectos en tratativas sobre los cuales seguramente habrá novedades en el corto plazo. Con las elecciones presidenciales de 2024 en Estados Unidos motivando la presentación de proyectos de ley en el país y los avances en materia de regulación de *deepfakes* que han ocurrido en los últimos meses de 2023, pareciera que estamos ante un punto de inflexión.

Es evidente que la tendencia mundial es regular ciertas aplicaciones de la inteligencia artificial, sobre todo aquellas cuyo mal uso pueden generar daño a los particulares y a la sociedad en general. En lo que respecta a las réplicas digitales, los recursos tradicionales existentes para proteger la imagen personal ya no están siendo lo suficientemente acertados para salvaguardar los derechos de las personas ante las aplicaciones de estas nuevas tecnologías, sobre todo cuando se trata de usos en el entorno digital. Si bien las víctimas del mal uso de los *deepfakes* tienen hoy ciertos recursos para defenderse, estas defensas no resultan prácticas a la hora de hacer valer sus derechos en línea, lo que deja en evidencia la necesidad de un instrumento legal que provea soluciones eficaces.

Las herramientas hoy existentes se enfrentan principalmente a dos problemas a la hora de defender los derechos de los titulares contra el contenido que circula en Internet: el anonimato y la difusión. Los usuarios malintencionados que abusan de estas tecnologías suelen esconderse detrás del anonimato y muchas veces puede ser difícil –o incluso imposible– identificarlos, encontrándose el afectado ante un infractor 'invisible' que escapa a la responsabilidad y queda impune[231]. Por su parte la difusión trae consigo dos problemáticas más, por un lado, si no se actúa rápidamente es casi imposible eliminar contenido que ha sido subido a Internet, sobre todo si este se ha viralizado, es decir, si ha sido compartido por numerosos usuarios; por el otro, la realidad es que incluso cuando se pruebe que un contenido es falso y se termine eliminando, el daño al titular de la imagen ya está hecho[232]. A la hora de proponer parámetros y lineamientos para la regulación de las réplicas digitales es importante tener presente tanto su naturaleza, como la del entorno

[231] Huijstee *et al.* (2021).
[232] Huijstee *et al.* (2021).

en el cual estas se usan y difunden. Por lo tanto, una propuesta para la regulación de réplicas digitales debe incluir tanto medidas preventivas a fin de evitar que se vulneren los derechos del sujeto retratado y proteger al espectador, como así también medidas reactivas o correctivas de rápido accionar y útiles ante un incumplimiento.

La presente propuesta de regulación tiene dos objetivos: permitir que las personas tengan control de su imagen en línea, en particular cuando esta sea recreada digitalmente, como así también establecer desincentivos para el mal uso de las herramientas que permiten crear y difundir estas réplicas. El abuso de la inteligencia artificial es una realidad con la que convivimos y no podemos obviar que cada vez más personas están siendo víctimas de los *deepfakes*. Esto no es solamente un problema de las figuras públicas, quienes están más expuestas a los abusos de su imagen personal, sino que nos afecta a todos. Herramientas *ex post* como las medidas cautelares, por más ágiles que sean, ya no son suficientes, sino que es preciso contar con recursos que sean accesibles, rápidos y apropiados para hacer frente a los abusos que ocurren en línea.

Considerando todo lo anterior, se proponen las siguientes medidas:

- **Registro declarativo de la imagen personal**

A los fines de acreditar la identidad del sujeto retratado y gestionar de manera directa y práctica sus derechos, se podría implementar un registro de imagen similar al instaurado en la mencionada Isla de Guernsey. Este registro debería tener carácter declarativo constituyéndose principalmente con fines probatorios, nunca se podría hablar de un registro constitutivo cuando el derecho de base tiene carácter personalísimo y por lo tanto nace con la misma persona. Asimismo, debería ser facultativo, no suponiendo una limitante para el ejercicio de los derechos por parte del titular.

Un registro de este estilo permitiría a los interesados inscribir no solo su retrato, sino además la descripción de cualquier otro rasgo característicos que lo identifique, siguiendo la línea de la interpretación amplia de imagen que ha sido adoptada por la doctrina y jurisprudencia. Se podría implementar asimismo para registrar la imagen de un grupo o conjunto, lo cual podría resultar una herramienta muy interesante para la defensa de la identidad de colectivos como conjuntos musicales, compañías artísticas o equipos deportivos.

Siendo que el objeto del registro es la imagen de los sujetos, se podrían aprovechar los recursos existentes a fin de alivianar la carga de los titulares de derecho y reducir así

los costos administrativos. Por ejemplo, dado que el Registro Nacional de las Personas[233] (RENAPER) posee en sus bases de datos el retrato de todos los habitantes del país, un sistema de registro de imagen integrado con RENAPER podría facilitar la implementación de este sistema, siendo que toda persona que posea un documento nacional de identidad (DNI) emitido en el país podría valerse de estos datos ya existentes para defender sus derechos.

Aquellas personas que no cuenten con un DNI, como por ejemplo los no residentes, deberían registrarse en el sistema propuesto si desean acceder a los beneficios del registro, como así también aquellas que deseen proteger características que los identifiquen distintas a su rostro.

- **Consentimiento**

La creación, uso y difusión de una réplica digital debe requerir del consentimiento del retratado. De acuerdo con lo desarrollado previamente (ver 3.3), este consentimiento debería ser previo, expreso, libre, inequívoco, informado, específico y externalizado mediante una declaración o una clara acción afirmativa. En línea con la normativa vigente, se debería prever asimismo la posibilidad de que este consentimiento sea libremente revocable.

En caso de fallecimiento del sujeto en cuestión, el consentimiento debe poder ser prestado por sus derechohabientes.

- **Licenciamiento**

A fin de aprovechar las oportunidades comerciales que presentan las réplicas digitales, sobre todo con miras a los avances de la tecnología inmersiva en el entorno virtual, estas deben poder ser licenciadas. Es importante recordar que se trata de representaciones de la imagen de una persona, por lo que si bien se puede conceder ciertas autorizaciones para crear, usar y difundir una réplica digital, los límites de estos permisos deben ser claros y específicos.

En este sentido, los contratos de licenciamiento de réplicas digitales deberían establecer expresamente su alcance, es decir, cuáles son los usos permitidos, los medios

[233] El RENAPER es un organismo autárquico y descentralizado, dependiente del Ministerio de Interior, que tiene a su cargo la identificación y la documentación de las personas dentro de la República Argentina. En particular, se ocupa de la emisión del Documento Nacional de Identidad (DNI) y el Pasaporte. Conforme informa el sitio web https://www.argentina.gob.ar/interior/registro-nacional-de-las-personas/institucional

abarcados, el territorio autorizado y el plazo durante el cual la autorización estará vigente, caso contrario, su interpretación será restrictiva.

Cuando la autorización relacionada a la réplica digital forme parte de un contrato más amplio, debe considerarse una buena práctica que la manifestación del consentimiento sea firmada de manera individualizada. Esto puede materializarse incorporando un anexo que requiera la firma del sujeto a representar, o firmando este en particular la cláusula que incluye dichas previsiones. De esta forma se pueden evitar confusiones en cuanto a la existencia del consentimiento.

- **Identificación del contenido**

Considerando la capacidad de las réplicas digitales para pasar por reales y el potencial que tienen para generar un daño al titular de la imagen, es importante que cuando se cree, use o difunda –incluso de manera legítima– contenido sintético que contiene la réplica digital de una persona, o hasta cuando este represente a una persona que no existe realmente, dicho contenido esté debidamente identificado como falso o sintético. La correcta identificación de las réplicas digitales como tales permitirá la libre existencia de contenido sintético con fines de crítica, sátira o parodia u otro uso encuadrado dentro de la protección provista por la libertad de expresión.

A fin de cumplir con esto, los PSI deberán posibilitar que los usuarios identifiquen el contenido sintético mediante la aplicación de etiquetas preestablecidas que indiquen que este ha sido generado con herramientas de inteligencia artificial. Asimismo, deberá exigirse a los desarrolladores de sistemas que permitan la creación de réplicas digitales que se incluya en ellos herramientas tecnológicas, como identificadores digitales, para identificar que el material creado es de naturaleza sintética.

- **Sistema de denuncia en línea**

Siguiendo la línea de las medidas implementadas en los países que ya han aprobado legislación en la materia, se propone la instauración de un sistema sencillo y accesible para la denuncia de réplicas digitales no consentidas detectadas en línea, similar al sistema de *notice and take down* (notificación y retiro, en español) planteado por la Ley de Derechos de Autor de la Era Digital (DMCA por sus siglas en inglés) de los Estados Unidos. De manera similar e incluso aprovechando los recursos ya existentes en las plataformas para cumplir con lo requerido por la DMCA, se podría implementar un sistema de denuncias en línea que permita a los usuarios poner en conocimiento del PSI la existencia de

contenido que viola sus derechos, ya sea que se trate de una réplica digital generada sin consentimiento del retratado o utilizada para fines o de manera no autorizada por este.

Estas denuncias tendrán carácter de declaración jurada y requerirán los datos personales de los usuarios que las presenten, como así también la identificación y una breve descripción del contenido que se pretende dar de baja. Los PSI deberán revisar la denuncia de manera expedita, y tomar medidas para limitar el acceso al contenido denunciado en caso de que la resolución de la contienda se demore. Se deberá permitir al titular del contenido denunciado la posibilidad de bajarlo o defenderse, alegando lo que considere necesario y acompañando la prueba que acredite que poseía el consentimiento del retratado para generar, difundir, explotar o de otro modo utilizar la réplica digital.

El registro de imagen antes propuesto facilitaría la presentación de la denuncia, ya que ayudaría al denunciante a acreditar su derecho, evitaría abusos de los sistemas de denuncia y agilizaría la labor del PSI a la hora de resolver la contienda.

Los PSI deberán diferenciar su accionar ante el contenido denunciado aplicando un enfoque basado en riesgos. Por ejemplo aquellos materiales que impliquen riesgo de desinformación o tengan como fin defraudar a los usuarios de la plataforma deberán ser suspendidos inmediatamente hasta tanto se resuelva la denuncia presentada. Asimismo, deberán considerarse como usos legítimos aquellos amparados por la libertad de expresión siempre y cuando no se genere un perjuicio al honor, dignidad o intimidad del representado.

Cuando la denuncia proviene de un tercero, es decir, una persona que no es el sujeto representado en el contenido sintético, este deberá informar las razones que fundan su protesta. Si dicho contenido no estuviese debidamente identificado como sintético, el PSI deberá analizar el caso, contactar al titular del material a fin de solicitar se expida al respecto y realizar sus mejores esfuerzos para discernir si realmente se trata de una réplica digital o no. En caso de que lo sea y el titular del material cuente con las autorizaciones necesarias, bastará que este agregue las etiquetas correspondientes.

La regulación debe establecer parámetros mínimos para garantizar la protección de los titulares de derecho, mas los PSI podrán establecer criterios más estrictos.

- **Alcance de la protección**

A fin de que la regulación propuesta sea eficiente a la hora de proteger la identidad virtual de una persona, se debe prever una concepción amplia de 'imagen', tal como lo ha establecido la doctrina y jurisprudencia. En este sentido, sin perjuicio del registro antes mencionado, el sujeto debe poder acceder a las herramientas propuestas para defender sus derechos cuando la representación permita que la persona sea reconocible, incluso cuando no se trate de una representación digital que replique su imagen. Es decir, que estos instrumentos podrían ser utilizados también en aquellas situaciones en las que el contenido sintético haga clara alusión a una persona en particular sin representarla, o cuando se haya usado algún elemento específico de una persona real para crear una persona ficticia, ya sea 'alimentando' al software de inteligencia artificial de imágenes o mediante indicaciones (*prompts*) que individualicen el nombre o algún rasgo físico distintivo de una persona real.

- **Neutralidad tecnológica**

Cuando se regulan tecnologías novedosas y versátiles, es importante prever los cambios que puedan suceder a futuro procurando que la norma no quede obsoleta con el paso del tiempo. El ya mencionado Proyecto de Ley de Protección de Datos Personales prevé lo que denomina como principio de neutralidad tecnológica, el que establece que el texto de la norma será aplicable a cualquier tratamiento de datos personales *"con independencia de las técnicas, procesos o tecnologías actuales o futuras- que se utilicen para dicho efecto"*[234]. Asimismo, el también ya referido Acuerdo entre SAG-AFTRA y AMPTP para los contratos de televisión y salas de cine (*theatrical*) de 2023 cuando define el concepto de inteligencia artificial generativa agrega que lo previsto aplicará también a cualquier tecnología que sea consistente con la definición establecida, independientemente del nombre que tenga.

La regulación propuesta debería prever expresamente el principio de neutralidad tecnológica a fin de proteger la imagen de las personas con independencia de la tecnología utilizada para generar, reproducir o distribuir la réplica digital.

- **Usos prohibidos**

Los usos indebidos de las réplicas digitales pueden generar un gran daño al sujeto representado, es por ello que cuando se trata de usos ilícitos que atentan por ejemplo contra

[234] Fernández y Rossi (2023). Artículo 5.

la integridad sexual de las personas, involucran la imagen de menores o incitan a la violencia, deberá prohibirse y penarse su creación, uso y difusión.

- **Penalización de la suplantación de identidad digital**

A fin de procurar una protección comprensiva de la imagen de las personas en línea, se debería incorporar al Código Penal de la Nación el delito de suplantación de identidad digital que abarque la suplantación de identidad mediante el uso de réplicas digitales, la utilización no consensuada de la imagen o datos filiatorios de una persona en Internet, como así también el uso de estos para crear una identidad falsa en el entorno virtual.

Las medidas propuestas, además de estar alineadas con los parámetros establecidos a nivel internacional, proveen herramientas prácticas, rápidas y de fácil acceso para los usuarios de servicios de Internet, incluyendo medidas de prevención proactivas como la obligación de identificar el contenido falso y reactivas como el sistema de denuncias. Por supuesto el afectado contará además siempre con la posibilidad de recurrir a los métodos tradicionales de resolución de conflictos y las acciones previstas en los códigos de fondo para la defensa de sus derechos e intereses, mas las barreras que imponen el anonimato y la difusión pueden desincentivar el uso de estas medidas en favor de las propuestas en el presente.

6. Conclusión

Las réplicas digitales se han convertido en un nuevo activo digital separado de la concepción tradicional de la imagen personal. Si bien hoy las aplicaciones de estas representaciones pueden parecer limitadas, no sería extraño que en poco tiempo poseer una réplica digital fuese una cotidianidad. Las tecnologías inmersivas, si bien aún encuentran cierta resistencia, apuntan a una presencia virtual activa de las personas, presentando herramientas que permitirían trasladar nuestras vivencias al mundo digital.

Los últimos años han dejado de manifiesto que, gracias a la aplicación de inteligencia artificial, los avances en la tecnología suceden a ritmos nuca antes evidenciados. No ha tomado más que un quinquenio para que las réplicas digitales se conviertan en una preocupación para las potencias mundiales. Incluso aquellas jurisdicciones que reaccionaron rápidamente a estos usos de las tecnologías de alteración de imagen han debido ajustar lo reglado al poco tiempo mediante la sanción de nuevas normas más comprensivas del funcionamiento de estas tecnologías, sus aplicaciones y riesgos.

Como se mencionó anteriormente, nunca es fácil regular nuevas tecnologías y no llamaría la atención que existan voces que disientan con el camino propuesto en el presente, sin embargo la inacción está generando un perjuicio a los individuos y a la sociedad. Medidas que contemplen las particularidades tanto de las réplicas digitales como de Internet, pueden ayudar a mitigar los daños causados por los abusos de los *deepfakes* y la exposición a contenido sintético que pasa desapercibido. La propuesta implica poner en manos de las personas herramientas que les permitan gestionar de manera directa sus derechos en línea, facilitando así su protección.

Si bien el término *deepfake* tiene mala reputación y pareciera poseer una connotación negativa, esto está muy lejos de la realidad. Las réplicas digitales presentan una infinidad de posibilidades que aún no se han explorado y que pueden ser tremendamente beneficiosas. Recién estamos explorando la superficie de las aplicaciones de estas tecnologías, pensemos por ejemplo cómo podría mejorar la experiencia de los alumnos aprender historia de los propios próceres que la trazaron o los beneficios terapéuticos que podría tener entablar conversaciones con un ser querido que ya no está presente. Entretenimiento, educación, salud, aún queda mucho por descubrir en el mundo de las réplicas digitales.

Ante esto y frente a una tecnología que aún está en desarrollo, es importante establecer reglas concretas para evitar abusos, pues si bien los beneficios son claros, también lo son los riesgos. En particular la peligrosidad de las réplicas digitales tiene dos aristas, ya que puede perjudicar tanto al sujeto retratado como al espectador. Tal cual se expuso durante el presente, sobran los ejemplos de casos en los cuales estas tecnologías han sido mal usadas y han generado un daño. La proliferación de softwares que permiten crear representaciones digitales de la imagen de terceros, cada vez más sencillos de utilizar y generando notablemente mejores resultados, se está convirtiendo en un problema.

Las herramientas legales que hoy poseemos en materia de derecho a la imagen son principalmente reactivas y no están preparadas para responder con la inmediatez que se requiere. Hacer frente a un activo digital que tiene una capacidad inherente para confundir al espectador exige además medidas preventivas que expongan la naturaleza de estos materiales.

La propuesta realizada en el presente no apunta a prohibir las réplicas digitales ni a cercenar la libertad de expresión o realizar censura previa del contenido que circula en línea, sino que procura plantear parámetros y lineamientos para la regulación de este tipo de contenido siendo comprensiva de las particularidades que presentan estos nuevos activos digitales y el entorno en el que circulan, permitiendo a la vez dar lugar a la crítica, la parodia y la expresión creativa. Internet no tiene fronteras y no podemos ser ajenos a lo que sucede en línea. Argentina necesita *aggiornar* su derecho y estar preparada para los cambios que se vienen.

Bibliografía

Doctrina

Blackshaw, I. (2010). The island of Guernsey to introduce new IP image right. *The International Sports Law Journal*, (1-2), 135.

Ceballos Delgado, J. M. (2011). Aspectos generales del derecho a la propia imagen. Revista La propiedad inmaterial, (15), 61-83.

Fallis, D. (2020). The epistemic threat of deepfakes. *Philosophy & Technology*, *34*(4), 623-643.

Geng, Y. (2023). Comparing "Deepfake" Regulatory Regimes in the United States, the European Union, and China. *Georgetown Law Technology Review*, 7 (1), 157-178.

Gómez, F. L. (2013). El derecho a la imagen de niños, niñas y adolescentes en Chile. Una mirada crítica a la luz del derecho internacional de los derechos humanos y de los estatutos normativos iberoamericanos de protección integral de la infancia y de la adolescencia. *Revista Chilena de Derecho*, *40*(3), 929–952.

Greenlee, M. (2021). Gun to Your Head: How Deepfakes and Other Non-Consensual Synthetic Media Hold Individual Autonomy Hostage. *UMKC L. Rev.*, *90*, 431.

Hine, E., & Floridi, L. (2022). New deepfake regulations in China are a tool for social stability, but at what cost? *Nature Machine Intelligence*, *4*(7), 608-610.

Huijstee, M. V., Boheemen, P. V., Das, D., Nierling, L., Jahnel, J., Karaboga, M., & Fatun, M. (2021). *Tackling deepfakes in European policy*. Publications Office of the European Union.

Johnson, E. E. (2017). Disentangling the right of publicity. *Northwestern University Law Review*, 111(4), 891-944.

Peyrano, G. F. (7 de julio de 2003). *El principio del consentimiento en el «sistema de protección de los datos personales». Condiciones de validez y posibilidad de revocación del consentimiento prestado. El derecho de oposición.* SAIJ.

Pilnik, F. (16 de diciembre de 2021). *Comentarios sobre la suplantación de identidad digital.* SAIJ.

Rothman, Jennifer E., The Inalienable Right of Publicity (12 de noviembre de 2012). 101 *Georgetown Law Journal* 185 (2012), Loyola-LA Legal Studies Paper No. 2012-46.

Tariq, S., Jeon, S., & Woo, S. S. (Abril 2022). Am I a Real or Fake Celebrity? Evaluating Face Recognition and Verification APIs under Deepfake Impersonation Attack. In *Proceedings of the ACM Web Conference 2022* (pp. 512-523).

Twomey, J. G., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G. (2023). Do deepfake videos undermine our epistemic Trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. *PLOS ONE*, *18*(10), e0291668.

Ullrich, Q. J. (2021). Is This Video Real? The Principal Mischief of Deepfakes and How the Lanham Act Can Address It. *Columbia Journal of Law & Social Problems*, *55*, 1.

Jurisprudencia nacional

Cámara Nacional de Apelaciones del Trabajo. 19988/2013. Braunstein Tamara Iliana c/ Palermo Films S.A. y otro s/diferencias de salarios. 21 de febrero de 2017.

Cámara Nacional de Apelaciones en lo Civil. Sala A. 22520/2019. Alzugaray, Mirna Fernanda c/ Taraborelli Automobile SA s/ daños y perjuicios. 16 de julio de 2021.

Cámara Nacional de Apelaciones en lo Civil. Sala B. 95667/2016. Ozu, Pablo c/ Olivan, Maria Julia y otro s/daños y perjuicios. 25 de abril de 2022.

Cámara Nacional de Apelaciones en lo Civil. Sala D. 20382/2015. Attardo, Raul Daniel c/ Editorial Los Alamos SA s/daños y perjuicios. 16 de diciembre de 2021.

Cámara Nacional de Apelaciones en lo Civil. Sala G. 74733/2012. Pitra Melina Marisol c/ Donom S.A. s/ daños y perjuicios. 22 de noviembre de 2017.

Cámara Nacional de Apelaciones en lo Civil. Sala J. 60235/2017. Vargas, Ricardo Andrés c/ THX Medios S.A. s/ daños y perjuicios. 10 de Junio de 2019.

Cámara Nacional de Apelaciones en lo Civil. Sala K. 66872/2018. De La Fuente, Rodrigo Fernando c/ Artear S.A. s/ daños y perjuicios. 16 de marzo de 2021.

Cámara Nacional de Apelaciones en lo Civil. Sala L. 47711/2013. Hess Mariana Beatriz c/ Hagelstron Josefina y otros s/ daños y perjuicios. 2 de diciembre de 2022.

Corte Suprema de Justicia de la Nación Argentina. Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A. s/ Daños y Perjuicios. 11 de diciembre de 1984.

Jurisprudencia internacional

España

Emilio Aragón Álvarez c/ Proborín, S.L., Sentencia Constitucional Nº 81/2001, Tribunal Constitucional de España Sala Segunda, Recurso de amparo 922/1998 (26 de marzo de 2001).

Tribunal Constitucional de España. Sala Segunda. Sentencia 117/1994. 25 de abril de 1994.

Tribunal Supremo. Sala de lo Civil. Sentencia 1779/2016. a 21 de abril de 2016.

Estados Unidos

Cohen v. Herbal Concepts, 63 N.Y.2d 379, 482 N.Y.S.2d 457, 472 N.E.2d 307 (N.Y. 1984).

Haelan Labs., Inc. v. Topps Chewing Gum, Inc. 202 F.2d 866. Corte de Apelaciones de los Estados Unidos Segundo Circuito. (16 de febrero de 1953).

Lohan v. Take-Two Interactive Software, Inc., 73 N.Y.S.3d 780, 97 N.E.3d 389, 2018 N.Y. Slip Op. 2208, 31 N.Y.3d 111 (N.Y. 2018).

Italia

Corte Suprema de Casación de Italia. Sección Civil I. Sentencia N° 1748. 29 de enero de 2016.

Reino Unido

Douglas & ors v Hello! Ltd & ors (No 3). Cámara de los Lores KHL 21 (2 de mayo de 2007).

Fenty v Arcadia Group Brands Ltd. Tribunal de Apelación de Inglaterra y Gales, División Civil 3 (22 de enero de 2015)

Hull City (AFC) Tigers Limited v The Commissioners for HMRC. United Kingdom First Tier Tribunal (Tax Chamber) 227 (22 de marzo de 2019)

Sports Club plc v Inspector of Taxes. Special Commissioners STC (SCD) 443 (8 de junio de 2000)

Internacional

Escué Zapata vs. Colombia. Corte Interamericana de Derechos Humanos (4 de julio de 2007).

Reklos and Davourlis v Greece, n° 1234/05, Tribunal Europeo de Derechos Humanos Sección Primera, § 38 (15 de enero de 2009).

Tristán Donoso vs. Panamá. Corte Interamericana de Derechos Humanos (27 de enero de 2009)

von Hannover v Germany (no 2), Tribunal Europeo de Derechos Humanos Gran Sala (7 de febrero 2012).

Legislación nacional

Código Civil y Comercial de la Nación. 7 de octubre de 2014 (Argentina).

Código Contravencional de la Ciudad de Buenos Aires (28 de Octubre de 2004).

Código Penal de la Nación Argentina Ley N° 11.179 (30 de septiembre de 1921). Argentina.

Ley 11.723 Régimen Legal de la Propiedad Intelectual (30 de septiembre de 1933). Argentina.

Proyectos de ley

Fernández, A. y Rossi, A. O. (30 de junio de 2023). Proyecto de Ley 0012-PE-2023. *Mensaje Nro: 0087/23 y Proyecto de Ley. Régimen de protección de datos personales. Derogación de las Leyes 25326 y 26343.*

Lospennato, S. G. (3 de noviembre de 2023). Proyecto de Ley 4436-D-2023. *Código Penal. Modificación del Artículo 128, sobre el uso de técnicas de inteligencia artificial para la difusión de imágenes de contenido sexual*.

Milman, G. (2 de noviembre de 2023). Proyecto de Ley 4410-D-2023. *OLIMPIA - Ley 27736 - Modificación del artículo 4, incorporando la utilización de la inteligencia artificial para la difusión de imágenes de contenido sexual.*

Milman, G. (2 de noviembre de 2023). Proyecto de Ley 4411-D-2023. *Código Penal. Modificación del artículo 128, sobre el uso de técnicas de inteligencia artificial para la difusión de imágenes de contenido sexual.*

Romero, J. C. (14 de diciembre de 2023). Proyecto de Ley 2469-S-2023. *Modificación al artículo 128 del Código Penal, Ley 11179, respecto de sancionar delitos contra la integridad sexual a través del uso de inteligencia artificial (IA) o cualquier mecanismo tecnológico.*

Legislación internacional

Asia

Disposiciones sobre la administración de servicios de información de Internet de síntesis profunda (25 de noviembre de 2022). China.

Ley de elección de funcionarios públicos. Ley No. 7681 (4 de agosto de 2005). Corea del Sur.

Ley sobre casos especiales relativos a la sanción de delitos sexuales. Ley No. 11556 (18 de diciembre de 2012). Corea del Sur.

Medidas provisionales para la gestión de servicios de inteligencia artificial generativa (10 de julio de 2023). China.

Reglamento sobre la gestión de servicios de información de audio y vídeo en línea (18 de noviembre de 2019). China.

Europa

A Bill to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes (Online Safety Act 2023), 2023 c. 50, Sesiones 2021-22 y 2022-23.

Código Civil (1° de enero de 1803). Francia.

Código Civil (16 de marzo de 1942). Italia.

Código Penal (1° de septiembre de 1990). Francia.

Código Penal (13 de noviembre de 1998). Alemania.

Código Penal Ley Orgánica 10/1995 (23 de noviembre de 1995). España.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. 4 de noviembre de 1950.

Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 — C9-0146/2021 — 2021/0106(COD)).

Ley de Derechos de Autor y Derechos Conexos (9 de septiembre de 1965). Alemania.

Ley Fundamental para la República Federal de Alemania (23 de mayo de 1949). Alemania.

Ley N° 633 sobre la Protección del Derecho de Autor y los Derechos Conexos (22 de abril de 1941). Italia.

Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. 5 de mayo de 1982 (España).

Ordenanza sobre derechos de imagen (2012). Bailía de Guernsey.

Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, COM/2021/206 final.

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales).

Estados Unidos

Allen Toussaint Legacy Act, SB 426, Louisiana State Legislature 2022 Regular Session.

An act to add and repeal Section 11547.5 of the Government Code, relating to technology, Senate Bill No. 1216, California Legislature 2021-2022 Regular Session.

An act to amend the civil rights law, in relation to establishing the right of publicity and to providing a private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual, S5959, The New York State Senate 2019-2020 Legislative Session.

Cause of action for nonconsensual dissemination of deep fake sexual images established, crime of using deep fake technology to influence an election established, and crime for nonconsensual dissemination of deep fake sexual images established, HF 1370, Minnesota Legislature 2023-2024 Regular Session.

Criminalizes deepfakes involving minors and defines the rights to digital image and likeness, SB 175, Louisiana 2023 Regular Session.

Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019, H. R. 3230, 116th Congress (2019-2020).

Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023, H. R. 5586, 118th Congress (2023-2024).

Defining synthetic media in campaigns for elective office, and providing relief for candidates and campaigns, SB 5152, Washington State Legislature 2023-2024 Regular Session.

Depiction of individual using digital or electronic technology: sexually explicit material: cause of action, Assembly Bill No. 602, California Legislature 2019-2020 Regular Session.

Invasion of Privacy; prohibition against the transmission of photography depicting nudity; include falsely created videographic or still images, SB 337, Georgia General Assembly 2019-2020 Regular Session.

Invasion of Privacy; prohibition on electronically transmitting or posting nude or sexually explicit photographs or videos for purposes of harassing the depicted person; revise, SB 78, Georgia General Assembly 2021-2022 Regular Session. https://www.legis.ga.gov/legislation/59239

Malicious Deep Fake Prohibition Act of 2018, S. 3805, 115th Congress (2017-2018).

New York Civil Rights Law (1909)

Prohibits unlawful dissemination or publication of intimate images created by digitization and of sexually explicit depictions of an individual; repealer, Senate Bill S1042A, The New York State Senate 2023-2024 Legislative Session.

Relating To Privacy, SB309, Legislature of the State of Hawaii 2021 Regular Session.

Relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election, SB 751, Texas Legislature 86th Legislative Session (2019).

Relating to the unlawful production or distribution of sexually explicit videos using deep fake technology; creating a criminal offense, SB 136, Texas Legislature 88th Legislative Session (2023).

Senate Bill S5959D. 2019-2020 Legislative Session (New York 2020)

Unlawful dissemination or sale of images of another; penalty, HB 2678, Virginia Legislature 2019 Regular Session.

Latinoamérica

Código Civil del Perú (24 de julio de 1984). Perú.

Código Penal (12 de noviembre de 1874). Chile.

Código Penal (3 de abril de 1991). Perú.

Código Penal Ley N° 1.160/97 (26 de noviembre de 1997). Paraguay.

Constitución de la República de Paraguay (20 de junio de 1992). Paraguay.

Constitución de la República Oriental del Uruguay (2 de febrero de 1967). Uruguay.

Constitución Política de la República de Chile (21 de octubre de 1980). Chile.

Constitución Política de la República Federativa del Brasil (5 de octubre de 1988). Brasil.

Constitución Política del Perú (29 de diciembre de 1993). Perú.

Ley 23. Sobre derechos de autor (28 de enero de 1982). Colombia.

Ley 9.739. Derechos de autor (17 de diciembre de 1937). Uruguay.

Ley Federal del Derecho de Autor (24 de diciembre de 1996). México.

Otras fuentes consultadas

¿Qué es la pornovenganza y cómo me protejo? (2023, diciembre). Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-y-como-protegerse-de-la-pornovenganza

90-day ban on deepfake political ads passes parliamentary special committee. (5 de diciembre de 2023). *The Korea Times*. https://www.koreatimes.co.kr/www/nation/2023/12/113_364513.html

Au, L. (3 de diciembre de 2019). *China targets 'deepfake' content with new regulation.* TechNode. https://technode.com/2019/12/03/china-targets-deepfake-content-with-new-regulation/

Ayudar a las personas a entender cuándo se usa IA o métodos digitales en los anuncios sobre temas sociales o política. (8 de noviembre de 2023). Meta. https://www.facebook.com/gpa/blog/political-ads-ai-disclosure-policy

Baroja, A. G. (14 de junio de 2023). Las redes sociales ganan terreno en el consumo de noticias y TikTok sigue su ascenso entre los jóvenes. *El País.* https://elpais.com/comunicacion/2023-06-14/las-redes-sociales-ganan-terreno-en-el-consumo-de-noticias-y-tiktok-sigue-su-ascenso-entre-los-jovenes.html

Bickert, M. (6 de enero de 2020). Enforcing against manipulated media. *Meta.* https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/

Billock, J. (2019, 9 mayo). With a little help from A.I., the Dali Museum brings the famed surrealist to life. *Smithsonian Magazine.* https://www.smithsonianmag.com/travel/with-little-help-from-ai-dali-museum-brings-famed-surrealist-to-life-180972127/

Breznican, A. (30 de diciembre de 2019). An oral history of Carrie fisher's return in the rise of skywalker. *Vanity Fair*. https://www.vanityfair.com/hollywood/2019/12/carrie-fisher-oral-history-rise-of-skywalker-star-wars

Cámara de Diputados LXV Legislatura México (8 de enero de 2024). *Busca iniciativa sancionar uso delictivo de la tecnología denominada inteligencia artificial. Boletín No. 5793 https://comunicacionsocial.diputados.gob.mx/index.php/boletines/-busca-iniciativa-sancionar-uso-delictivo-de-la-tecnologia-denominada-inteligencia-artificial*

Cho, B., Le, B. M., Kim, J., Woo, S., Tariq, S., Abuadbba, A., & Moore, K. (Octubre 2023). Towards understanding of deepfake videos in the wild. In *Proceedings of the 32nd ACM International Conference on Information and Knowledge Management* (pp. 4530-4537). https://www.researchgate.net/publication/373686936_Towards_Understanding_of_Deepfake_Videos_in_the_Wild

Ciber 4 All Team. (19 de diciembre de 2023). *IA, deepfake y la evolución del fraude del CEO.* Tarlogic Cybersecurity Experts. https://www.tarlogic.com/es/blog/ia-deepfake-fraude-del-ceo/

Cohen, L. (2024, 29 enero). *Taylor Swift searches blocked on X after fake explicit images spread.* Reuters. https://www.reuters.com/technology/taylor-swift-searches-blocked-x-after-fake-explicit-images-spread-2024-01-28/

Collier, K. (14 de julio de 2023). Actors vs. AI: Strike brings focus to emerging use of advanced tech. *NBC News*. https://www.nbcnews.com/tech/tech-news/hollywood-actor-sag-aftra-ai-artificial-intelligence-strike-rcna94191

Comisión Federal de Comercio de los Estados Unidos. (26 julio de 2023). *Guides concerning the use of endorsements and testimonials in advertising.* Federal Register. https://www.federalregister.gov/documents/2023/07/26/2023-14795/guides-concerning-the-use-of-endorsements-and-testimonials-in-advertising#citation-21-p48093.

Conforme establecen las 'Políticas de Contenido multimedia manipulado' de la empresa. Véase Meta. (s. f.). *Contenido multimedia manipulado.* Transparency Center. https://transparency.fb.com/es-la/policies/community-standards/manipulated-media/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fmanipulated_media

Coscarelli, J. (19 de abril de 2023). An A.I. Hit of Fake 'Drake' and 'The Weeknd' Rattles the Music World. *The New York Times.* https://www.nytimes.com/2023/04/19/arts/music/ai-drake-the-weeknd-fake.html

Damiani, J. (3 de septiembre de 2019). A voice deepfake was used to scam a CEO out of $243,000. *Forbes.* https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=33417c842241

De La Cuadra, B. (5 de abril de 2001). Emilio Aragón, Desamparado. *El País.* https://elpais.com/diario/2001/04/06/agenda/986508006_850215.html

Deepfake democracy: South Korean candidate goes virtual for votes. (14 de febrero de 2022). *France 24.* https://www.france24.com/en/live-news/20220214-deepfake-democracy-south-korean-candidate-goes-virtual-for-votes

Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., & Ferrer, C. C. (2020). The DeepFake Detection Challenge (DFDC) dataset. *arXiv (Cornell University).* https://doi.org/10.48550/arxiv.2006.07397.

El bailarín Joaquín Cortés gana una batalla legal contra Cacaolat. (28 de julio de 2002). Elmundo.es. https://www.elmundo.es/elmundo/2002/07/28/cultura/1027867605.html

El proyecto del Código Penal ya ingresó al Congreso. (2019, 26 marzo). Argentina.gob.ar. https://www.argentina.gob.ar/noticias/codigo-penal-congreso

Engler, J., & Love, M. (28 de junio de 2022). *New Allen Toussaint Legacy Act creates a right of publicity in Louisiana.* Louisiana Law Blog. https://www.louisianalawblog.com/intellectual-property/new-allen-toussaint-legacy-act-creates-a-right-of-publicity-in-louisiana/

Entra en vigor la normativa china para regular los deepfakes y el contenido generado por inteligencia artificial. (1° de octubre de 2023). Reason Why. https://www.reasonwhy.es/actualidad/china-regulacion-deepfakes-etiquetado-consentimiento-inteligencia-artificial

Flannery O'Connor, J., & Moxley, E. (14 de noviembre de 2023). Our approach to responsible AI innovation. *YouTube Official Blog.* https://blog.youtube/inside-youtube/our-approach-to-responsible-ai-innovation/

Gajewski, R. (1° de octubre de 2022). Bruce Willis' Rep Refutes Report That He Sold His Digital Likeness to Deepfake Company. *The Hollywood Reporter.* https://www.hollywoodreporter.com/business/digital/bruce-willis-refutes-report-digital-likeness-deepfake-1235231331/

Global deepfake software industry trends analysis report 2024, forecast to 2032 (broken down by type, end user, regional analysis, and competitive landscape). (23 de noviembre 2023). Absolute Reports. https://www.absolutereports.com/global-deepfake-software-industry-25803343

González, F. (15 de noviembre de 2023). Crear deepfakes con IA en México podría costar hasta ocho años de cárcel. *WIRED.* https://es.wired.com/articulos/crear-deepfakes-con-ia-en-mexico-podria-costar-hasta-ocho-anos-de-carcel

Guest, P. (26 de octubre de 2023). The UK's controversial Online Safety Act is now law. *Wired.* https://www.wired.co.uk/article/the-uks-controversial-online-safety-act-is-now-law

Heikkilä, M. (31 de enero de 2024). *Tres lecciones a partir de los «deepfakes» porno de Taylor Swift.* MIT Technology Review. https://www.technologyreview.es/s/16137/tres-lecciones-partir-de-los-deepfakes-porno-de-taylor-swift

Help us shape our approach to synthetic and manipulated media. (11 de noviembre de 2019). Twitter Blog. https://blog.twitter.com/en_us/topics/company/2019/synthetic_manipulated_media_policy_feedback. La traducción es propia.

Intel and Intel Labs Develop New AI Methods to Restore Trust in Media. Intel. https://www.intel.com/content/www/us/en/research/blogs/trusted-media.html.

Intel Presenta un Detector de Deepfake. (14 de noviembre de 2022). Intel Newsroom. https://www.intel.la/content/www/xl/es/newsroom/news/intel-introduces-real-time-deepfake-detector.html

Intellectual Property Office. (s. f.). *What are image rights.* Intellectual Property Office Serving the Bailiwick of Guernsey. https://ipo.guernseyregistry.com/article/103037/What-are-Image-Rights

La persona relevante a cargo de la Administración del Ciberespacio de China respondió a las preguntas de los periodistas sobre el «Reglamento sobre la administración de servicios de información de audio y vídeo en línea». (29 noviembre de 2019). Administración del Ciberespacio de China. http://www.cac.gov.cn/2019-11/29/c_1576561821173892.htm

Meta. (12 de junio de 2020). *Deepfake Detection Challenge Results: An open initiative to advance AI.* https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/

Nat'l Assembly passes revised bill banning deepfakes in campaigns. (20 de diciembre de 2023). KBS WORLD. https://world.kbs.co.kr/service/news_view.htm?lang=e&id=Po&Seq_Code=182572

Our synthetic and manipulated media policy. (Abril 2023). X Help Center. https://help.twitter.com/en/rules-and-policies/manipulated-media.

Reuters Institute for the Study of Journalism (2023). Digital News Report 2023 https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023

SAG-AFTRA members approve 2023 TV/Theatrical Contracts Tentative agreement. (5 de diciembre de 2023). SAG-AFTRA. https://www.sagaftra.org/sag-aftra-members-approve-2023-tvtheatrical-contracts-tentative-agreement

Salvador Dalí Museum. (23 de enero de 2019). *Dalí Lives: Museum brings artist back to life with AI.* https://thedali.org/press-room/dali-lives-museum-brings-artists-back-to-life-with-ai/

Shanfeld, E. (1° de noviembre de 2023). Scarlett Johansson Takes Legal Action Against AI App That Ripped Off Her Likeness in Advertisement. *Variety.* https://variety.com/2023/digital/news/scarlett-johansson-legal-action-ai-app-ad-likeness-1235773489/

Sobornos, mujeres y noticias falsas: el CEO de Cambridge Analytica confesó en una cámara oculta los métodos que salpican a Facebook. (20 de marzo de 2018). *Infobae.* https://www.infobae.com/america/eeuu/2018/03/19/sobornos-mujeres-y-noticias-falsas-el-ceo-de-cambridge-analytica-confeso-en-una-camara-oculta-los-metodos-que-salpican-a-facebook/

Sum and Substance Ltd (2023). *Sumsub Identity Fraud Report 2023*. https://sumsub.com/guides-reports/identity-fraud-report-2023/

Tabany, S. (30 de julio de 2023). Huelga en Hollywood: pese al reclamo, los estudios redoblan la apuesta a la IA. *El Economista.* https://eleconomista.com.ar/internacional/huelga-hollywood-pese-reclamo-estudios-redoblan-apuesta-ia-n64674

The Dalí Museum. (8 de mayo de 2019). *Behind the Scenes: Dalí Lives* [Archivo de Vídeo] YouTube. https://www.youtube.com/watch?v=BIDaxl4xqJ4

TikTok. (Marzo 2023). *Integrity and Authenticity*. https://www.tiktok.com/community-guidelines/en/integrity-authenticity/

Vincent, J. (21 de marzo de 2023). TikTok bans deepfakes of nonpublic figures and fake endorsements in rule refresh. *The Verge*. https://www.theverge.com/2023/3/21/23648099/tiktok-content-moderation-rules-deepfakes-ai

Watercutter, A. (14 de febrero de 2023). Keanu Reeves will never surrender to the machines. *WIRED*. https://www.wired.com/story/keanu-reeves-chad-stahelski-interview/.

Weatherbed, J. (25 de enero de 2024). Trolls have flooded X with graphic Taylor Swift AI fakes. *The Verge*. https://www.theverge.com/2024/1/25/24050334/x-twitter-taylor-swift-ai-fake-images-trending?ref=404media.co

Williams, Z. (22 de diciembre de 2023). More States to Push Laws Banning AI Election Deepfakes in 2024. *Bloomberg Law*. https://news.bloomberglaw.com/artificial-intelligence/more-states-to-push-laws-banning-ai-election-deepfakes-in-2024

YouTube. (s. f.). *Políticas sobre información errónea.* Ayuda de YouTube. https://support.google.ceom/youtube/answer/10834785?hl=es-419