Daños derivados de la inteligencia artificial generativa: el alcance de la responsabilidad civil por el uso y creación de sistemas de IA destinados a la generación de *deepfakes*

Por Giuliana A. Forastiero [1]

Sumario: I.- Introducción. II.- Potenciales daños a la persona derivados de la creación de *deepfakes* y derechos involucrados. III.- Alcance de la legitimación pasiva. III.1.- La creación de *deepfakes* como actividad riesgosa: ¿resulta pertinente aplicar una regulación uniforme para los diversos usos de la Inteligencia Artificial? III.2.- Responsabilidad civil derivada de daños causados por el uso de sistemas de inteligencia artificial generadores de *deepfakes*. III.3.- Responsabilidad civil de quienes se encuentran involucrados en el desarrollo de los sistemas de IA generadores de *deepfakes*. IV.- Conclusión. V.- Bibliografía.

Resumen: El auge de la IA generativa ha suscitado una serie de desafíos legales, en particular respecto al alcance de la responsabilidad civil derivada del uso y creación de sistemas generadores de *deepfakes*, por los cuales se pueden causar daños significativos, como psicológicos, espirituales y a la integridad personal. La extensión de la responsabilidad de los usuarios, programadores y desarrolladores debe abordarse considerando que no todos los usos de la IA pueden ser regulados de manera uniforme. Si bien la creación de *deepfakes* parecería ser una actividad riesgosa (factor de atribución objetivo), el contexto de su generación podría eliminar su riesgosidad (responsabilidad subjetiva); a su vez, se podría excluir la responsabilidad de los programadores y desarrolladores aplicando el criterio de "prohibición de regreso", propio de la teoría de la imputación objetiva. El sistema jurídico argentino cuenta con las herramientas para abordar esto, mas debería existir una regulación específica.

Abstract: The generative AI boom has given rise to numerous legal challenges, particularly regarding the scope of civil liability derived from the use and creation of deepfake-generating systems, by which

[1] Estudiante de Derecho, Universidad Austral.

Palabras clave: Daños – inteligencia artificial generativa – *deepfakes* – responsabilidad civil – actividad riesgosa – responsabilidad objetiva – responsabilidad subjetiva.

Keywords: Harm – generative artificial intelligence – deepfakes – civil liability – risky activity – strict liability – personal liability.

significant harm can be caused, including at the psychological, spiritual, and personal integrity levels. The extent of liability for users, programmers, and developers must be addressed considering that not all applications of AI can be uniformly regulated. While the creation of deepfakes may be regarded as a risky activity (strict liability), the contextual circumstances surrounding their generation could eliminate such risky nature (personal liability); furthermore, the liability of programmers and developers might be excluded by invoking the doctrine that the negligent contribution to the commission of a crime should go unpunished, which is specific to the strict liability theory. The Argentine legal system has the necessary tools to approach this; however, specialized regulation is required.

I.- Introducción[2]

En la era de la información, el desarrollo tecnológico ha impulsado, paradójicamente, la existencia de una era de la posverdad[3], la cual encuentra su apogeo en los avances de la inteligencia artificial (IA), especialmente, de la IA generativa, dentro de las cuales se hallan las técnicas destinadas a la creación de *deepfakes*.

El término *deepfake* combina las palabras en inglés *deep* (profundo) y *fake* (falso). Se trata de fabricaciones digitales hiperrealistas –pero, como indica su nombre, falsas–, generalmente imágenes, grabaciones de video o audio, creadas utilizando técnicas de IA: las técnicas de aprendizaje profundo,[4] en particular redes generativas adversativas (en inglés, "GANs"[5]). Por medio de esta tecnología es posible, entre otras innumerables aplicaciones, superponer imágenes o videos, "insertando" el rostro de una persona en el cuerpo de otra[6]; alterar un video de una persona para que visual y auditivamente parezca que hizo o dijo algo que jamás ocurrió[7], y crear contenido audiovisual completamente nuevo, como personas que en realidad no existen[8]. Como se ve, se puede generar tanto contenido como la imaginación lo permita, con un nivel de calidad altísimo, que el ojo humano no logra identificar como falso, sino más bien percibe como real.

No obstante, los *deepfakes* podrían resultar de gran utilidad en diversos ámbitos, tales como el educativo, artístico y cinematográfico (por ej., pueden ser empleados para "rejuvenecer" a los actores[9]). En definitiva, el progreso de la IA generativa no debe ser temido, sino más bien gestionado; en pos de maximizar sus beneficios y

---

[2] El presente escrito fue presentado en el Concurso de Monografías n.° 2 de las XXIX Jornadas Nacionales de Derecho Civil, en el cual obtuvo el segundo premio.
Agradezco al Dr. Franco Andrés Melchiori por su valiosa orientación y sus sugerencias durante el desarrollo de este trabajo. También agradezco al Dr. Ramón Daniel Pizarro por brindarme la oportunidad de publicar este artículo.

[3] RAMOS CHÁVEZ, Alejandro, "Información líquida en la era de la posverdad", *Revista General de Información y Documentación*, Vol. 28, 2018, p. 286.

[4] JODKA, Sara H., "Manipulating reality: the intersection of deepfakes and the law" (2024), *Reuters*, https://www.reuters.com/legal/legalindustry/manipulating-reality-intersection-deepfakes-law-2024-02-01/, (disponible en Internet el 07-VIII-2024).

[5] Sobre esto, cfr. UDDIN MAHMUD, Bahar y SHARMIN, Afsana, "Deep Insights of Deepfake Technology: A Review", *Dhaka University Journal of Applied Science & Engineering*, Vol. 5, 2020, pp. 16-18.

[6] A modo de ejemplo: https://www.youtube.com/watch?v=eseGwoxiqNs (Disponible el 28-VII-2024).

[7] A modo de ejemplo: https://www.youtube.com/watch?v=bE1KWpoX9Hk (Disponible el 28-VII-2024).

[8] A modo de ejemplo: https://thispersondoesnotexist.com/ (Disponible el 28-VII-2024).

[9] Véase MURPHY G., CHING D., TWOMEY J. y LINEHAN C., "Face/Off: Changing the face of movies with deepfakes", *PLoS ONE*, Vol. 18, 2023, pp. 1-3.

minimizar sus potencialidad dañosa, resulta fundamental enmarcar jurídicamente su utilización.

El presente escrito tiene como objeto analizar el alcance de la responsabilidad civil derivada del uso y creación de los sistemas de IA destinados a la generación de *deepfakes*. Al efecto, se demostrará la relevancia de la cuestión identificando los potenciales daños a la persona y derechos comprometidos; se determinará la relación causal en dos dimensiones: primero, respecto a quienes utilizan estos sistemas de IA, y segundo, a quienes se encuentran involucrados en su desarrollo, y finalmente se dilucidará el *quid* de la variación del factor de atribución en función a los diferentes tipos y usos que se les den a los sistemas de IA, especialmente a los destinados a la creación de *deepfakes*.

II.- Potenciales daños a la persona derivados de la creación de *deepfakes* y derechos involucrados

Los sistemas de IA con los que se crean los *deepfakes* están disponibles para todo aquel que posea conexión a internet. Es decir, la mayor parte de la población puede crear contenido digital falso, no solo de uno mismo, sino también de otros individuos. A modo de ejemplo, un hecho que captó el interés de la sociedad fue la difusión de *deepfakes* sexualmente explícitos (no consentidos) de Taylor Swift en la red social X[10]. Este visibilizó una problemática relativamente poco discutida: el 96% de los *deepfakes* son de contenido pornográfico[11], y por la falta de regulación y tratamiento del tema, los afectados se ven desalentados a buscar justicia[12].

De todos modos, el estudio y regulación de esta tecnología no debe limitarse a esta clase de *deepfakes*, pues la IA puede generar diferentes tipos de contenido cuyos efectos podrían resultar igual de perniciosos. En particular, estos pueden manifestarse como daños a la persona –además de posibles daños patrimoniales, cuya determinación depende en gran medida de las circunstancias concretas, por ello no serán abordados en el presente escrito–; si bien el alcance de los daños a la persona debe ser evaluado en cada caso, procederé a explicar aquellos que estimo más probables a ocurrir.

Para empezar, se debe mencionar el menoscabo de la integridad personal (art. 1738 del Código Civil y Comercial), la cual "comprende la indemnidad de todos los

[10] GILBOURNE, Jade, "Taylor Swift deepfakes: a legal case from the singer could help other victims of AI pornography", *The Conversation*, 31 de enero de 2024, https://theconversation.com/taylor-swift-deepfakes-a-legal-case-from-the-singer-could-help-other-victims-of-ai-pornography-222113 (Disponible el 2-VIII-2024).

[11] PECHENIK GIESEKE, Anna, "'The New Weapon of Choice': Law's Current Inability to Properly Address Deepfake Pornography", *Vanderbilt Law Review*, Vol. 73, 2020, p. 1482.

[12] STURGES, Julia, "Taylor Swift, Deepfakes, and the First Amendment: Changing the Legal Landscape for Victims of Non-Consensual Artificial Pornography", *The Georgetown Journal of Gender and the Law*, Vol. 25, 2024, pp. 9-10.

En Argentina, por la falta de regulación se derivó un caso (penal) de *deepfake* a una unidad contravencional; la deficiencia de tratamiento de la cuestión desalienta a buscar justicia en otros ámbitos del derecho, por ej., en el fuero civil. Al respecto véase INFOBAE, "Escándalo en una escuela de Córdoba: un alumno utilizó IA para crear imágenes pornográficas de sus compañeras", 3 de julio de 2024, https://www.infobae.com/sociedad/2024/07/03/escandalo-en-una-escuela-de-cordoba-un-alumno-utilizo-ia-para-crear-imagenes-pornograficas-de-sus-companeras/ (Disponible el 2-VIII-2024).

derechos de los cuales puede ser titular una persona"[13]. Así, la creación de *deepfakes* podría provocar una afectación al derecho a la identidad personal (art. 1740 CCyC) en tanto se le atribuyan a la persona cuya imagen se utiliza, calidades y características dinámicas (creencias, opiniones, acciones…) que permitan individualizarla en la valoración de los demás[14], como por ej. un *deepfake* de un individuo realizando comentarios racistas. A su vez, se lesionaría el derecho a la intimidad (art. 19 CN; arts. 52, 1740 y 1770 CCyC) de los afectados, pues la creación de *deepfakes* implica la "manipulación e instrumentalización por otros [de la esfera de vida propia, intangible e inaccesible para los demás]"[15].

Ahora bien, con respecto a los *deepfakes* en los cuales se muestra a una persona realizando actos generalmente considerados "ofensivos" o "humillantes", estos suponen una manifiesta afectación al derecho al honor (arts. 52 y 1740 CCyC) en su dimensión objetiva (reputación). Tal es el caso del *deepfake* del actual presidente de Filipinas en el que se lo ve consumiendo estupefacientes[16], el cual fue viralizado días antes del "State of the Nation Address". La creación de esta clase de *deepfakes* "pone en riesgo la integridad de la democracia y los procesos electores, [al igual que] la estabilidad social"[17]. Por otra parte, el uso de la IA para crear *deepfakes* de esta naturaleza puede devenir en un agravio al honor en sentido subjetivo; por ej., la generación de *deepfakes* pornográficos resulta para las víctimas (en su percepción de sí) "deshumanizante [cosificante], [y simplemente] degradante (…) verse a sí mismo siendo representado de manera falsa"[18].

Ahora bien, ¿qué ocurre cuando los *deepfakes* parecerían ser satíricos, artísticos o, en general, "creativos"? Ciertamente –además de afectar al derecho a la identidad personal y a la intimidad–, aunque no se acredite un daño a la reputación, "se tutela el honor cuando se ha afectado el sentimiento de la propia dignidad [honra], (…) [incluso si, por ejemplo,] los terceros, masivamente, no han creído la verdad de la imputación"[19].

En esa línea, resulta fundamental aclarar que, incluso si no se acreditase el menoscabo a la identidad, a la privacidad ni al honor, la mera creación de *deepfakes* sin el consentimiento de la persona involucrada para ello[20] resulta violatorio del derecho a la imagen (art. 53 CCyC), en tanto el individuo pueda ser

[13] ALFERILLO, Pascual E., "Capítulo 1: Responsabilidad civil. Sección 4ª: Daño resarcible", en Jorge Horacio ALTERINI (dir.) e Ignacio Ezequiel ALTERINI (coord.), *Código Civil y Comercial: Tratado exegético*, 3ª ed., La Ley, Buenos Aires, 2019, Tomo VIII, p. 265.

[14] TOBÍAS, José W., "Capítulo 3: Derechos y actos personalísimos", en Jorge Horacio ALTERINI (dir.) e Ignacio Ezequiel ALTERINI (coord.), *Código Civil y Comercial: Tratado exegético*, 3ª ed., La Ley, Buenos Aires, 2019, Tomo I, p. 622.

[15] TOBÍAS (n. 14), p. 559.

[16] https://www.youtube.com/watch?v=VPA1pPktJrE (Disponible el 7-VIII-2024).

[17] CORVALÁN, Juan G., REQUEJO, Roberto y CARRO, María Victoria, *El impacto de la inteligencia artificial generativa y los deepfakes en los procesos electorales*, La Ley, 2024-B.

[18] PASCALE, Emily, "Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse", *Syracuse Law Review*, Vol. 73, 2023, p. 340.

[19] TOBÍAS (n. 14), p. 605.

[20] Cfr. DE CUCCO ALCONADA, María Carmen, *El derecho a la imagen y las redes sociales*, Sistema Argentino de Información Jurídica (SAIJ), 2018.

diferenciado e identificado[21], incluso aunque "[la imagen] se 'falsifique' con todas las apariencias de autenticidad ['*de cualquier modo que lo haga*']"[22].
Por otra parte, la creación de *deepfakes* puede provocar otros tipos de daños a la persona, como daños psicológicos; lesiones de tal gravedad, que implican "la disminución de sus aptitudes para obtener ganancias"[23], podrían acaecer cuando estos son de contenido explícito, pues estos poseen la aptitud para producir en los afectados ansiedad y depresión extremas[24], las cuales tienden a manifestarse en la incapacidad para trabajar[25]. En esa línea, la creación de cierto contenido falso provocaría una lesión a los sentimientos del sujeto –sufrimiento y menoscabo de la paz– es decir, daño espiritual (art. 1738 CCyC)[26].

III.- Alcance de la legitimación pasiva
1.-La creación de *deepfakes* como actividad riesgosa: ¿resulta pertinente aplicar una regulación uniforme para los diversos usos de la Inteligencia Artificial?
En primer lugar, la causación de los daños responde (materialmente) a la acción del usuario de generar los *deepfakes* mediante sistemas de IA. A su vez, en función a la teoría de la causalidad adecuada, resulta acorde (jurídicamente) al curso natural y ordinario de las cosas (art. 1727 CCyC) que la creación de ciertos *deepfakes* provoque en la persona cuya imagen se utilizó, los daños previamente analizados. En efecto, se evidencia que "el criterio de previsibilidad es el eje central de la causalidad jurídica" y, con este, surge el deber primordial de prevenir la producción de daños (art. 1710 CCyC)[27].
En ese sentido, resulta fundamental analizar si corresponde aplicar una regulación uniforme para los diversos usos de la IA, pues con base en esa conclusión se determinará si la generación de *deepfakes* en todos los casos se puede clasificar (o no) como "actividad riesgosa" y, en efecto, si el criterio de imputación resulta objetivo –para atribuir responsabilidad basta con acreditar el nexo causal entre la acción y el daño, siendo el único eximente la causa ajena, y no el cumplimiento de las técnicas de prevención (art. 1757 CCyC)– o, en su defecto, subjetivo –se debe, además de acreditar el nexo causal, demostrar que se obró con culpa o dolo (arts. 1721 y 1724 CCyC)–.
En primer lugar, la teoría del riesgo creado (receptada en el art. 1757 CCyC) entiende que "si bien el conjunto de la sociedad se beneficia con [ciertos] adelantos, no resulta justo que sean los ciudadanos quienes deban absorber el daño que con motivo de su utilización se ocasione, sino que debe afrontar dichas consecuencias dañosas quien introduce ese riesgo"[28]. Con respecto a los *deepfakes*, en tanto estos son generados mediante "sistemas operados por la [IA]", en principio se ven

[21] ANDRADA, Alejandro Dalmacio, *Responsabilidad civil de los medios de comunicación: El factor de atribución*, Juris, Rosario, 1998, pp. 186 y 451.
[22] TOBÍAS (n. 14), p. 657.
[23] UBIRÍA, Fernando Alfredo, *Derecho de daños en el Código Civil y Comercial de la Nación*, Abeledo Perrot, Ciudad Autónoma de Buenos Aires, 2015, p. 341.
[24] A modo de ejemplo: https://www.youtube.com/watch?v=LkGnPeY6Csk (Disponible el 5-VIII-2024).
[25] CITRON, Danielle K., "Sexual Privacy", *The Yale Law Journal*, Vo. 128, 2019, p. 1926.
[26] UBIRÍA (n. 23), p. 313.
[27] UBIRÍA (n. 23), p. 146.
[28] CALVO COSTA, Carlos A., *Derecho de las obligaciones*, 3ª Edición, Hammurabi, Buenos Aires, 2020, p. 824.

incluidos "en el elenco de actividades riesgosas", establecido en las XXVII Jornadas Nacionales de Derecho Civil[29].

No obstante, podría cuestionarse si resulta apropiado otorgarles a todos los usos de la IA el mismo tratamiento de "actividad riesgosa", pues el término "IA" es sumamente amplio e incluye una gran variedad de tecnologías distintas, "cuyo impacto y riesgo es sustantivamente distinto. En efecto, no causa el mismo riesgo un vehículo (…) autónomo que un sistema de texto predictivo en mi correo electrónico. (…) [Por lo que] resultaría ineficiente aplicar un régimen de responsabilidad estricta [objetiva] único a aplicaciones cuya actividad suponen un riesgo nulo para el usuario de dicha tecnología"[30]. Ciertamente, "La diversidad de usos [de la IA] hace imposible determinar regulaciones generales. [Su] amplitud, profundidad y capilaridad (…) requiere un sistema normativo que entienda la especificidad de los casos particulares"[31].

Para ello, corresponde analizar las implicancias de que una actividad sea considerada "riesgosa", pues "todo momento anterior a la causación de un perjuicio (…) supone una situación de riesgo. [Por eso,] en cuanto factor objetivo de atribución el concepto mismo de riesgo [debe afinarse]"[32]. El Proyecto de Código Civil de 1998 regulaba la "actividad *especialmente* riesgosa" (art. 1665). Si bien el CCyC contiene una fórmula más laxa, una interpretación sensata lleva a adoptar un criterio estricto; para considerar a una actividad como tal, esta "debe evidenciar un riesgo grave, importante, relevante [y] perceptible"[33]. De lo contrario, se desnaturalizaría la figura al "incluir (…) la casi totalidad de los supuestos de responsabilidad civil (…) lo cual llevaría al sistema a un rigor insostenible. (…) [Sería incluso] absurdo y sin precedentes en el derecho comparado"[34].

Esta es la línea de pensamiento que parece seguir el Reglamento (UE) 2024/1689 ("Ley de Inteligencia Artificial de la Unión Europea"), el cual clasifica a los sistemas de IA en distintos tipos en función al riesgo, pudiendo reconocerse cuatro diferentes categorías: 1) los de "riesgo mínimo", que comprenden a "la gran mayoría de los sistemas de IA, [los cuales] *no plantean riesgos* y, por lo tanto, pueden seguir utilizándose, y no estarán regulados por el Reglamento [ej.: filtros de *spam*]"[35]; 2) los de "riesgo limitado", los cuales "estarán sujetos a obligaciones de transparencia muy leves, como la divulgación de que su contenido se ha generado mediante la IA"[36], siendo ejemplos de estos los *chatbots* y ciertos tipos de *deepfakes* (sobre lo

---

[29] XXVII Jornadas Nacionales de Derecho civil, Conclusiones de la Comisión n.°3, Rosario, 2019, https://drive.google.com/file/d/1FDqjvrsFsB9b_2nwBK61N0peL0vsSToA/view (Disponible el 15-VII-2024).

[30] ARAYA PAZ, Carlos, "Desafíos legales de la inteligencia artificial en Chile", *Revista chilena de derecho y tecnología*, Vol. 9, 2020, p. 276.

[31] ARGENCON, "Argencon propone un marco regulatorio para desarrollar a la Argentina como referente internacional en Inteligencia Artificial", 5 de agosto de 2024, https://www.argencon.org/argencon-propone-un-marco-regulatorio-para-desarrollar-a-la-argentina-como-referente-internacional-en-inteligencia-artificial/ (Disponible el 6-VIII-2024).

[32] OSSOLA, Federico Alejandro, *Responsabilidad civil*, Abeledo Perrot, Ciudad Autónoma de Buenos Aires, 2016, p. 120

[33] PIZARRO, Ramon D., *Responsabilidad civil por actividades riesgosas o peligrosas en el nuevo Código*, La Ley 2015-D 993.

[34] PIZARRO (n. 33).

[35] Consejo Europeo y Consejo de la Unión Europea, "Reglamento de Inteligencia Artificial", https://www.consilium.europa.eu/es/policies/artificial-intelligence/ (Disponible el 3-VIII-2024).

[36] Consejo Europeo y Consejo de la Unión Europea (n. 35).

cual se desarrollará *a posteriori*); 3) los de "alto riesgo", sujetos a normas más estrictas, su clasificación debe limitarse a aquellos sistemas que tengan un efecto perjudicial considerable en la salud, la seguridad y los derechos fundamentales de las personas (Considerando 46), y 4) los de "riesgo inaceptable", cuya utilización se encuentra absolutamente prohibida.

Esto demuestra que para la UE no todos los sistemas de IA implican el mismo riesgo y que la regulación varía según el nivel de peligrosidad asociado con cada sistema en cuestión. De todas maneras, considero que dicha ley incurre en una contradicción: al referirse a la mayoría de los sistemas de IA como "de riesgo mínimo", el *nomen iuris* sugiere que –trasladándolo a nuestro ordenamiento jurídico– estos deberían tratarse en el marco de la "actividad riesgosa". Sin embargo, el mismo Consejo de la UE aclara que en estos sistemas *no* hay riesgo (ya sea porque es inexistente o irrelevante), y que por eso mismo la norma no los regula . De esta forma, las tecnologías de "riesgo mínimo" no pueden ser consideradas propiamente como actividades tal índole, no siendo aplicable en su caso el factor de atribución objetivo de responsabilidad. Por lo expuesto, no resulta pertinente aplicar una regulación uniforme para los diversos usos de la IA.

2.-Responsabilidad civil derivada de daños causados por el uso de sistemas de inteligencia artificial generadores de *deepfakes*

Continuando con el análisis del derecho comparado, el Reglamento europeo indica que el uso de los sistemas de IA generadores *deepfakes* crea un "riesgo limitado" en tanto "el contenido [sea] evidentemente creativo[37], satírico[38], artístico[39]…", e impone –tanto al usuario como el proveedor (lo cual se analizará *a posteriori*)– el "revelar de forma clara y distinguible que el contenido ha sido creado o manipulado artificialmente" (Considerando 134). Al imponer como única obligación (sin legislar más al respecto) el cumplimiento de un deber de transparencia, se interpreta que el riesgo no posee la relevancia suficiente para que –en el ordenamiento jurídico argentino– la actividad se considere riesgosa (por tanto, el factor de atribución de responsabilidad del usuario sería subjetivo). En estos casos, es por contexto de la creación del *deepfake* (y no por la intención con la que se genera) –es decir, por la naturaleza de su contenido y por el cumplimiento del deber de transparencia– que el componente "engaño", determinante de la peligrosidad, se ve definitivamente eliminado y, con este, el riesgo.

Sin embargo, cuando el contenido del *deepfake* no es de la naturaleza expuesta en el párrafo anterior, el cumplimiento del deber de transparencia (que de todos modos debería atenderse), no resulta suficiente para eliminar el riesgo. Por ej., cuando se crea un *deepfake* "político" (como el del presidente de Filipinas), su mera existencia –por más de que se indique que fue creado con IA– posee una gran potencialidad dañosa. Así, en estos casos, el uso de dichos sistemas implicaría la realización de una "actividad riesgosa", por lo que la responsabilidad del usuario sería objetiva.

[37] Por ejemplo, en ámbitos –entre otros– de entretenimiento o educativos, como el caso de un profesor que crea un *deepfake* para enseñarle este sistema a sus alumnos.
[38] Por ejemplo, un *deepfake* del rostro de una persona en el cuerpo de un animal.
[39] A modo de ejemplo: https://www.youtube.com/watch?v=64UN-cUmQMs.

3.-Responsabilidad civil de quienes se encuentran involucrados en el desarrollo de los sistemas de IA generadores de *deepfakes*

En primer lugar, resulta menester esclarecer quiénes se ven comprendidos bajo el título "involucrados en el desarrollo del sistema de IA". En las recomendaciones del Parlamento Europeo (P9_TA(2020)0276) sobre el régimen de responsabilidad civil en materia IA, se sugiere hacer "responsables a las diferentes personas de toda la cadena de valor que crean, mantienen o controlan el riesgo asociado al sistema" (Recomendación n.°7), es decir, a los "operadores" (Rec. n.°10), tanto "finales" como "iniciales" (Rec. n.°12). En ese sentido, por "operador final" debe entenderse "o bien [al] usuario/poseedor del sistema [lo cual ya fue analizado *a priori*], o bien [al] propio desarrollador del sistema que se vale de los datos que obtiene cuando [este] está funcionando." y por "operador inicial", al "programador que ofrece su sistema como servicio y se mantiene vinculado a él por medio del trabajo continuado sobre [este]"[40]. Así, quienes se encuentran "involucrados en el desarrollo del sistema de IA" –a diferencia de quienes lo utilizan (los usuarios)– serían los programadores y los desarrolladores que se benefician con su funcionamiento.

En ese sentido, el art. 1758 CCyC "contempla una amplia legitimación pasiva (…). Debe entenderse: que quien 'realiza' la actividad es tanto quien la genera como quien la controla, potencia o fiscaliza [y] que quien 'se sirve u obtiene provecho' de ella, comprende cualquier tipo de beneficio"[41]. Corresponde aclarar que, de existir más de un obligado, la responsabilidad será solidaria si la causa fuente es única –por ej., si el *deepfake* fue creado entre dos o más usuarios–, y será concurrente si hay diversidad de fuentes –por ej., entre el usuario y el programador, si correspondiese[42]–. En este marco, se evidencia que la normativa argentina resulta compatible con el derecho comparado.

Respecto a la determinación del alcance de la responsabilidad de estos sujetos, se debe partir de que la causalidad material no basta para concluir que el autor tenga que afrontar la reparación del daño producido, sino que esta deberá ser dilatada o restringida. De ese ajuste, surge la causalidad jurídica, "es decir, la que el derecho computa a los fines pertinentes de la responsabilidad, y la extensión del resarcimiento"[43].

Resulta fundamental destacar esto último: la "causalidad adecuada" en su esfera "jurídica" está destinada a calcular la extensión del resarcimiento. En esa línea, Claus Roxin explicaba "La teoría de la adecuación (…) no es (…) una teoría causal, sino una teoría de la imputación"[44]. En función a esta teoría –receptada doctrinalmente en el derecho civil argentino[45]– surge la necesidad de distinguir, en primer lugar, la cuestión de si existe una relación (física) causa-efecto entre el demandado y el daño ("causalidad material", o "causalidad" a secas), y "verificado al

[40] ZORNOZA SOMOLINOS, Alejandro, "Breves apuntes a la propuesta de reglamento del parlamento europeo sobre responsabilidad civil en materia de inteligencia artificial", *Revista de Derecho, Empresa y Sociedad*, Nro. 17, 2020, p. 100.

[41] UBIRÍA (n. 23), pp. 434-435.

[42] UBIRÍA (n. 23), p. 435.

[43] LLAMBÍAS, Jorge Joaquín, RAFFO BENEGAS, Patricio, SASSOT, Rafael A., *Manual de derecho civil: obligaciones*, 14ª ed., Abeledo Perrot, Buenos Aires, 2005, p. 119.

[44] ROXIN, Claus, *Derecho penal: parte general*, trad. de la 2ª ed. alemana de Diego-Manuel Luzon Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal, Civitas, Madrid, 1997, Tomo I, p. 360.

[45] Sobre esto cfr. CALVO COSTA, Carlos A., *La causalidad adecuada en el derecho de daños: ¿causalidad real o criterio de imputación objetiva?*, La Ley 2021-A.

menos un vínculo *sine qua non*, aparecerá la segunda cuestión (…), que se refiere a verificar si resulta razonable considerar al demandado como el antecedente que desencadenó el daño [es decir, si este le puede ser imputado al agente] y que, según la doctrina que tomemos, es conocido como 'causalidad jurídica' o, aun con mayor propiedad, como 'imputación objetiva'"[46].

Ciertamente, de no ser por la creación de estos programas informáticos, los daños no podrían haber acaecido; lo que caracteriza a la producción de estos perjuicios es que derivan del uso de sistemas de IA desarrollados por otras personas, quienes con su creación introdujeron un riesgo grave en la comunidad, lo cual "[impone de manera] imperiosa la adopción de severas medidas de protección"[47]. En ese sentido, la Ley de IA de la UE, obliga también a los programadores y desarrolladores (Considerando 134) a cumplir con el deber de transparencia. Por supuesto, la manifestación de este deber de prudencia (art. 1725 CCyC) para prevenir daños (art. 1710 CCyC) deberá ser determinada por cada país; no obstante, diversos Estados –como China– han impuesto la obligación de incorporar una "marca de agua" a todo el contenido generado mediante el uso de sus sistemas de IA, en pos de revelar la falsedad del material[48].

De todas maneras, el cumplimiento de las técnicas de prevención no es eximente de la responsabilidad en los términos del art. 1758 CCyC. Analógicamente (aunque estos casos de *deepfakes* no traten una relación de consumo), respecto a la responsabilidad de los portales de anuncios (por ej., de Mercado Libre), la jurisprudencia nacional indica que el criterio de imputación de responsabilidad es subjetivo[49] en tanto estos "[ocupen] una posición neutra entre el cliente vendedor y los potenciales compradores, [y no desempeñen] un papel activo que [les permita] adquirir conocimiento o control de los datos relativos a esas ofertas"[50]. Es decir, como la plataforma actúa como mera intermediaria (rol pasivo), solo "[será responsable] cuando [haya] tomado efectivo conocimiento de la ilicitud del contenido publicado si tal conocimiento no es seguido de un actuar diligente"[51]. En contraposición, los sistemas de IA con los que se crean los *deepfakes* no resultan ser un mero "enlace", sino que –como se mencionó– son determinantes en la causación del daño. Por lo tanto, se refuerza el argumento de que su responsabilidad sería, en principio, objetiva.

Sin embargo, en los supuestos en los cuales la responsabilidad del usuario es subjetiva (por haber mitigado el riesgo), en pos de determinar la extensión de la responsabilidad de los sujetos involucrados en el desarrollo del sistema de IA, se podría recurrir a uno de los criterios correctivos de la imputación objetiva: la "prohibición de regreso", por la cual se "excluye la imputación a un sujeto [programadores y desarrolladores, por más de que el proceso causal puesto en

---

[46] PRIETO MOLINERO, Ramiro J., "Causalidad e imputación objetiva en la responsabilidad civil", *Revista de Responsabilidad Civil y Seguros*, Nro. 6, 2014, p. 18.

[47] ZAVALA DE GONZÁLEZ, Matilde, "La noción de actividades riesgosas en el Proyecto del Código Civil", J.A. 1988-I, p. 906.

[48] ZOU, Mimi [Oxford Martin School], *'China's Deepfake Regulations: navigating security, misinformation and innovation' Prof Mimi Zou* [Archivo de video], 1 de junio de 2023, https://www.youtube.com/watch?v=_bfoq5y6Rsw (Disponible el 8-VIII-2024).

[49] CNCiv., Sala M, "Iglesia Mesiánica Mundial Sekai Kyusei Kyo en la Argentina c/ Mercado Libre S.A. y otros s/ propiedad intelectual 11.723", 28-III-2022.

[50] CNCiv., Sala D, "Kosten, Esteban c/Mercado Libre S.R.L. s/ ordinario", 22-III-2018.

[51] CNCom., Sala C, "Ferraro Antonio Fabián C. Car Group S.A. y Mercado Libre S.R.L.", 1-X-2019.

marcha por ellos haya sido *conditio sine qua non* del daño] cuando en la cadena causal se interpone la acción de un tercero [usuario] mediante una conducta dolosa o gravemente negligente"[52]. No obstante, este criterio no operaría si dicha conducta se viese significativamente favorecida por la actuación de los sujetos involucrados en el desarrollo del sistema[53], lo cual podría ocurrir si estos no incorporan las "marcas de agua" mencionadas (es decir, por incumplir el deber de transparencia).

IV.- Conclusión

En conclusión, el auge de la IA generativa ha suscitado una serie de desafíos en el ámbito del Derecho de Daños, especialmente en cuanto al alcance de la responsabilidad civil derivada del uso y de la creación de sistemas de IA para generar *deepfakes*. La facilidad con la que se crea este contenido falso demuestra la virtualidad del acaecimiento de daños a la persona, como a la integridad personal, psicológicos y espirituales.

La responsabilidad civil de los usuarios, programadores y desarrolladores que se benefician con su funcionamiento debe abordarse considerando que no todos los usos de la "IA" pueden ser regulados de manera uniforme debido a la diversidad de tecnologías y usos de ellas que este término abarca, cuyo impacto y riesgo es sustancialmente distinto. En efecto, cuando se crean *deepfakes* de contenido artístico, satírico o –en términos generales– creativo, y se cumple estrictamente con el deber de transparencia, el propio contexto de su generación elimina completamente el componente "engaño" y, con este, la gravedad del riesgo creado; al no poder enmarcarse como "actividad riesgosa", el factor de atribución de responsabilidad del usuario es subjetivo. Empero, cuando el contenido no encuadra en la categorización presentada, el contexto de su creación no es suficiente para eliminar el peligro, siendo la "actividad riesgosa" y la responsabilidad, objetiva.

En esta línea, la responsabilidad de los programadores y desarrolladores es –en principio–, en función a la teoría del riesgo creado, objetiva. No obstante, con base en la teoría de la imputación objetiva, se puede aplicar el criterio de "prohibición de regreso" por el que se excluiría la imputación a dichos sujetos ante el accionar doloso o gravemente culposo del usuario (siempre que su conducta no haya sido significativamente favorecida por los primeros).

Por lo expuesto, considero que el sistema jurídico argentino cuenta, en materia de responsabilidad civil, con las herramientas necesarias para abordar los desafíos que el surgimiento de las técnicas de IA generadoras de *deepfakes* suscitan. Sin embargo, en pos de aportar seguridad jurídica, es necesario establecer un marco normativo que regule la IA, no entendida genéricamente, sino que comprenda la especificidad de los usos particulares. Es imperativo que el ordenamiento jurídico argentino evolucione en paralelo con los avances tecnológicos, que se adapte con precisión a estos cambios, especialmente en lo que respecta la nueva tendencia en la era digital: el uso y creación de sistemas de inteligencia artificial capaces de generar *deepfakes*.

V.- Bibliografía

[52] MELCHIORI, Franco Andrés, "La responsabilidad civil en los pronunciamientos del Tribunal Supremo de España: Aproximación al papel de la teoría de la imputación objetiva en la atribución causal", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, Nro. 47, 2016, p. 111.
[53] PRIETO MOLINERO (n. 46), p. 19.

Alferillo, Pascual E., "Capítulo 1: Responsabilidad civil. Sección 4ª: Daño resarcible", en Jorge Horacio Alterini (dir.) e Ignacio Ezequiel Alterini (coord.), *Código Civil y Comercial: Tratado exegético*, 3ª ed., La Ley, Buenos Aires, 2019, Tomo VIII.

Andrada, Alejandro Dalmacio, *Responsabilidad civil de los medios de comunicación: El factor de atribución*, Juris, Rosario, 1998.

Araya Paz, Carlos, "Desafíos legales de la inteligencia artificial en Chile", *Revista chilena de derecho y tecnología*, Vol. 9, 2020.

Argencon, "Argencon propone un marco regulatorio para desarrollar a la Argentina como referente internacional en Inteligencia Artificial", 5 de agosto de 2024, https://www.argencon.org/argencon-propone-un-marco-regulatorio-para-desarrollar-a-la-argentina-como-referente-internacional-en-inteligencia-artificial/ (Disponible el 6-VIII-2024).

Calvo Costa, Carlos A., *La causalidad adecuada en el derecho de daños: ¿causalidad real o criterio de imputación objetiva?*, La Ley 2021-A.

Calvo Costa, Carlos A., *Derecho de las obligaciones*, 3ª Edición, Hammurabi, Buenos Aires, 2020.

Citron, Danielle K., "Sexual Privacy", *The Yale Law Journal*, Vo. 128, 2019.

CNCiv., Sala M, "Iglesia Mesiánica Mundial Sekai Kyusei Kyo en la Argentina c/ Mercado Libre S.A. y otros s/ propiedad intelectual 11.723", 28-III-2022.

CNCiv., Sala D, "Kosten, Esteban c/Mercado Libre S.R.L. s/ ordinario", 22-III-2018.

CNCom., Sala C, "Ferraro Antonio Fabián C. Car Group S.A. y Mercado Libre S.R.L.", 1-X-2019.

Consejo Europeo y Consejo de la Unión Europea, "Reglamento de Inteligencia Artificial", https://www.consilium.europa.eu/es/policies/artificial-intelligence/ (Disponible el 3-VIII-2024).

Corvalán, Juan G., Requejo, Roberto y Carro, María Victoria, *El impacto de la inteligencia artificial generativa y los deepfakes en los procesos electorales*, La Ley, 2024-B.

de Cucco Alconada, María Carmen, *El derecho a la imagen y las redes sociales*, Sistema Argentino de Información Jurídica (SAIJ), 2018.

Gilbourne, Jade, "Taylor Swift deepfakes: a legal case from the singer could help other victims of AI pornography", *The Conversation*, 31 de enero de 2024, https://theconversation.com/taylor-swift-deepfakes-a-legal-case-from-the-

singer-could-help-other-victims-of-ai-pornography-222113 (Disponible el 2-VIII-2024).

Infobae, "Escándalo en una escuela de Córdoba: un alumno utilizó IA para crear imágenes pornográficas de sus compañeras", 3 de julio de 2024, https://www.infobae.com/sociedad/2024/07/03/escandalo-en-una-escuela-de-cordoba-un-alumno-utilizo-ia-para-crear-imagenes-pornograficas-de-sus-companeras/ (Disponible el 2-VIII-2024).

Jodka, Sara H., "Manipulating reality: the intersection of deepfakes and the law" (2024), *Reuters*, https://www.reuters.com/legal/legalindustry/manipulating-reality-intersection-deepfakes-law-2024-02-01/, (disponible en Internet el 07-VIII-2024).
Llambías, Jorge Joaquín, Raffo Benegas, Patricio, Sassot, Rafael A., *Manual de derecho civil: obligaciones*, 14ª ed., Abeledo Perrot, Buenos Aires, 2005.

Melchiori, Franco Andrés, "La responsabilidad civil en los pronunciamientos del Tribunal Supremo de España: Aproximación al papel de la teoría de la imputación objetiva en la atribución causal", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, Nro. 47, 2016.

Murphy G., Ching D., Twomey J. y Linehan C., "Face/Off: Changing the face of movies with deepfakes", *PLoS ONE*, Vol. 18, 2023.

Ossola, Federico Alejandro, *Responsabilidad civil*, Abeledo Perrot, Ciudad Autónoma de Buenos Aires, 2016.

Pascale, Emily, "Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse", *Syracuse Law Review*, Vol. 73, 2023.

Pechenik Gieseke, Anna, "'The New Weapon of Choice': Law's Current Inability to Properly Address Deepfake Pornography", *Vanderbilt Law Review*, Vol. 73, 2020.

Pizarro, Ramon D., *Responsabilidad civil por actividades riesgosas o peligrosas en el nuevo Código*, La Ley 2015-D.

Prieto Molinero, Ramiro J., "Causalidad e imputación objetiva en la responsabilidad civil", *Revista de Responsabilidad Civil y Seguros*, Nro. 6, 2014.

Ramos Chávez, Alejandro, "Información líquida en la era de la posverdad", *Revista General de Información y Documentación*, Vol. 28, 2018.

Roxin, Claus, *Derecho penal: parte general*, trad. de la 2ª ed. alemana de Diego-Manuel Luzon Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal, Civitas, Madrid, 1997, Tomo I.

Sturges, Julia, "Taylor Swift, Deepfakes, and the First Amendment: Changing the Legal Landscape for Victims of Non-Consensual Artificial Pornography", *The Georgetown Journal of Gender and the Law*, Vol. 25, 2024.

Tobías, José W., "Capítulo 3: Derechos y actos personalísimos", en Jorge Horacio Alterini (dir.) e Ignacio Ezequiel Alterini (coord.), *Código Civil y Comercial: Tratado exegético*, 3ª ed., La Ley, Buenos Aires, 2019, Tomo I.

Ubiría, Fernando Alfredo, *Derecho de daños en el Código Civil y Comercial de la Nación*, Abeledo Perrot, Ciudad Autónoma de Buenos Aires, 2015.

Uddin Mahmud, Bahar y Sharmin, Afsana, "Deep Insights of Deepfake Technology: A Review", *Dhaka University Journal of Applied Science & Engineering*, Vol. 5, 2020.
Zavala de González, Matilde, "La noción de actividades riesgosas en el Proyecto del Código Civil", J.A. 1988-I.

Zornoza Somolinos, Alejandro, "Breves apuntes a la propuesta de reglamento del parlamento europeo sobre responsabilidad civil en materia de inteligencia artificial", *Revista de Derecho, Empresa y Sociedad*, Nro. 17, 2020.

Zou, Mimi [Oxford Martin School], *'China's Deepfake Regulations: navigating security, misinformation and innovation' Prof Mimi Zou* [Archivo de video], 1 de junio de 2023, https://www.youtube.com/watch?v=_bfoq5y6Rsw (Disponible el 8-VIII-2024).

XXVII Jornadas Nacionales de Derecho civil, Conclusiones de la Comisión n.°3, Rosario, 2019, https://drive.google.com/file/d/1FDqjvrsFsB9b_2nwBK61N0peL0vsSToA/view (Disponible el 15-VII-2024).