Facultad de Ciencias Jurídicas, Políticas y Relaciones Internacionales

Maestría de Investigación en Derecho mención Derechos Constitucionales, Humanos y Ambientales

Tema:

Riesgos de la inteligencia artificial para el derecho a la imagen en Ecuador

Tesis para la obtención del Título de Magíster en Investigación en Derecho con mención en Derechos Constitucionales, Humanos y Ambientales

Presentada por:

Johnny José Guerra Cedeño

Tutor:

Andrés Castillo

Quito, septiembre 2025

Resumen

La investigación aborda los desafíos que plantea la inteligencia artificial (IA) al derecho a la imagen, entendida como expresión de la identidad y de la dignidad humana. Se analizan los riesgos que surgen con el uso de herramientas como los deepfakes, la clonación facial y de voz, y los generadores de imágenes sintéticas, que permiten manipular la representación personal con un realismo cada vez más difícil de detectar. Estos fenómenos evidencian vacíos legales y procesales en la protección de los derechos personalísimos, lo que expone a las personas a vulneraciones con graves consecuencias sociales y psicológicas. El trabajo concluye que resulta urgente fortalecer la normativa, incorporar responsabilidades claras para quienes desarrollan o difunden estos contenidos y promover la alfabetización digital como medio de prevención y defensa frente a las nuevas formas de violencia simbólica y digital.

Palabras clave: inteligencia artificial, derecho a la imagen, deepfakes, dignidad humana, datos biométricos, protección de datos personales.

Declaración de aceptación de norma ética y derechos

El presente documento se ciñe a las normas éticas y reglamentarias de la Universidad Hemisferios. Así, declaro que lo contenido en este ha sido redactado con entera sujeción al respeto de los derechos de autor, citando adecuadamente las fuentes. Por tal motivo, autorizo a la Biblioteca a que haga pública su disponibilidad para lectura dentro de la institución, a la vez que autorizo el uso comercial de mi obra a la Universidad Hemisferios, siempre y cuando se me reconozca el cuarenta por ciento (40%) de los beneficios económicos resultantes de esta explotación.

Además, me comprometo a hacer constar, por todos los medios de publicación, difusión y distribución, que mi obra fue producida en el ámbito académico de la Universidad Hemisferios.

De comprobarse que no cumplí con las estipulaciones éticas, incurriendo en caso de plagio, me someto a las determinaciones que la propia Universidad plantee.

Nombre: Johnny José Guerra Cedeño

Cédula: 1723468474

Dedicatoria

A Dios, por ser mi refugio en los momentos de duda y mi fuerza en los momentos de debilidad.

A mi familia, por su amor incondicional y por enseñarme que la constancia y la fe son más fuertes que cualquier adversidad.

A aquellos que, sin compartir un lazo consanguíneo directo, se han convertido en familia por su presencia constante, sus palabras de aliento y su sabiduría compartida.

En especial, a Mishell Villa G., cuya fortaleza, ternura e inspiración han sido un faro y sustento en esta travesía, y por recordarme cada día que vale la pena resistir, luchar y soñar.

Y, a Rómulo Tehanga C., quien supo iluminar mis momentos de oscuridad con consejos sinceros y una voz firme que me animó a seguir adelante.

Índice

Riesgos de la inteligencia artificial para el derecho a la imagen en Ecuador

Johnny José Guerra Cedeño
jjohnny_99@hotmail.com

Resumen

La investigación aborda los desafíos que plantea la inteligencia artificial (IA) al derecho a la imagen, entendida como expresión de la identidad y de la dignidad humana. Se analizan los riesgos que surgen con el uso de herramientas como los deepfakes, la clonación facial y de voz, y los generadores de imágenes sintéticas, que permiten manipular la representación personal con un realismo cada vez más difícil de detectar. Estos fenómenos evidencian vacíos legales y procesales en la protección de los derechos personalísimos, lo que expone a las personas a vulneraciones con graves consecuencias sociales y psicológicas. El trabajo concluye que resulta urgente fortalecer la normativa, incorporar responsabilidades claras para quienes desarrollan o difunden estos contenidos y promover la alfabetización digital como medio de prevención y defensa frente a las nuevas formas de violencia simbólica y digital.

Palabras clave: inteligencia artificial, derecho a la imagen, deepfakes, dignidad humana, datos biométricos, protección de datos personales.

Abstract

This research addresses the challenges that artificial intelligence (AI) poses to the right to image, understood as an expression of personal identity and human dignity. It examines the risks associated with tools such as deepfakes, facial and voice cloning, and synthetic image generators, which allow the manipulation of personal representation with increasing realism. These developments reveal legal and procedural gaps in the protection of personality rights, leaving individuals exposed to violations with serious social and psychological consequences. The study concludes that it is urgent to strengthen regulation, establish clear responsibilities for those who develop or disseminate such content, and promote digital literacy as a means of prevention and defense against new forms of symbolic and digital violence.

Keywords: artificial intelligence, right to image, deepfakes, human dignity, biometric data, data protection..

Capítulo I: Riesgos de la Inteligencia Artificial para el Derecho a la imagen en Ecuador

Las revoluciones tecnológicas en la humanidad han permitido el desarrollo de condiciones materiales, culturales, económicas y sociales, que mejoran la calidad de vida de las poblaciones. Sin embargo, dichas innovaciones han significado el despertar de fuerzas que pueden tornarse peligrosas, considerando que en muchas ocasiones se utilizan para generar procesos de dominación, puesto que el ser humano suele inclinarse hacia la guerra. Con la creación de softwares avanzados conocidos como inteligencia artificial, se instaura la cuarta revolución tecnológica, de la cual todavía no se puede visualizar sus alcances.

El acceso y uso de la IA en el Ecuador, ha posibilitado que el incremento de obtener información, producción y acceso de contenido afecte sectores laborales sobre todo en el campo de las ciencias sociales y las artes. Lo que plantea muchas interrogantes y preocupaciones por el desplazamiento de personal que empieza a ser reemplazado por la tecnología, situación que tiene como antecedente la primera revolución industrial, en donde se desplazó la población rural hacia las grandes ciudades para convertirse en mano de obra. En la segunda revolución industrial, se instauro la producción masiva de productos gracias a la introducción de maquinaria especializada que permitía reducir la cantidad de mano de obra y potenciaba la capacidad productiva reduciendo tiempo y amenorando costos.

No obstante, la última revolución tecnológica trae consigo una mayor capacidad de automatización de la que experimentamos en la revolución digital. Además, la capacidad para procesar datos y manipular contenidos se ha incrementado de manera exponencial lo que puede desembocar en el uso arbitrario de información personal, afectando la imagen de las personas. Ya se han visto casos en los que se utiliza la voz y la imagen de personas famosas para realizar

contenido, por lo que se hace imperante considerar desde la ciencia jurídica mecanismo de regulación que proteja a las personas del uso arbitrario de sus datos personales.

Se debe tomar en cuenta que la innovación tecnológica de las IA supone un gran avance para la ciencia, consolidándose como una herramienta versátil para la generación de conocimiento al reducir significativamente procesos de sistematización de datos, experimentación virtual, correlación de datos y análisis en tiempo real. Pero que deja la incógnita de que estos avances pueden suponer la reducción de trabajos lo cual traería serias consecuencias económicas y que produciría contradicciones que pueden trastocar los paradigmas socioeconómicos.

Fundamentos conceptuales: derecho a la imagen e inteligencia artificial

La presente investigación tiene como objetivo identificar los límites y alcances de la Ley ecuatoriana sobre el uso de la IA y en específico sobre el uso de datos personales, en este caso la imagen de las personas. ¿Existe legislación sobre el uso de aplicaciones con IA en el Ecuador, hay reglamentación específica? ¿Está protegido el derecho a la imagen? Para el efecto debemos considerar que previo a la creación e implementación de aplicaciones con IA, se contaba con programas (software) que podían modificar imágenes, sin embargo, los mismos podían ser detectados como alteraciones y su capacidad era limitada. Ahora, las aplicaciones de edición de IA pueden realizar videos, fotografías e imágenes que difícilmente pueden ser diferenciadas de las creaciones originales, por lo que los usuarios pueden generar contenidos que parecen reales sin contar con el consentimiento de las personas, quienes tampoco pueden responsabilizar a las aplicaciones con IA por el uso de sus datos.

Por lo cual, es necesario definir que es la IA y sus capacidades, características y posibles usos que puedan vulnerar derechos como el derecho a la imagen. Debido a que, ¿A quién se le puede atribuir responsabilidad por el uso lesivo de aplicaciones con IA por vulnerar derechos como el derecho a la imagen? Para lo cual, tenemos como primer punto de análisis el problema de reconocer a la IA como sujeto de derecho, de manera que se pueda imputar responsabilidades en el caso de vulneración de derechos. Según el Reglamento Europeo de Inteligencia Artificial en su artículo 3 define a la IA como:

Sistema de IA: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales**.** (Reglamento Europeo de Inteligencia Artificial, p. 166).

Es importante señalar que en el Reglamento Europeo de Inteligencia Artificial no se le reconoce condición de sujeto de derecho a la IA, se establece que las responsabilidades jurídicas que se desprendan de la utilización de las IA se imputaran a los proveedores. No obstante, el debate continúa debido a que con los avances en la ingeniería robótica los entes mecánicos (robots) ya son una realidad. El origen de la palabra 'robot' sería derivación de la palabra checa "robbota", que significa servidumbre o trabajo forzado, creada por el escritor checo Karel Capec (Carranza G, et al, 2022, p. 19). En principio, las maquinas han cumplido, desde su invención, como herramientas que permiten facilitar tareas específicas bajo la conducción u operación del ser humano. El robot, sería una maquina evolucionada capaz de realizar distintas tareas con la

capacidad de desarrollar niveles de autonomía, la interacción con los humanos se reduciría a la asignación de tareas y ya no a la conducción u operación.

Cabe señalar que los sistemas operativos de los robots todavía están restringidos a operaciones específicas que no les permiten mayores niveles de autonomía, como ya sucede con los sistemas de IA. Sin embargo, no estamos lejos de proporcionar sistemas de IA a los robots, lo que genera algunas preocupaciones debido a que otorgar la capacidad de autonomía a maquinas complejas y antropomórficas nos llevaría a considerar un mínimo de derechos a las maquinas gracias a la influencia del posmodernismo que ha derivado en discursos ideológicos que se plantean desde el posthumanismo y el transhumanismo.

La tradición de la ciencia jurídica ha definido como sujeto de derecho al ser humano natural, en algunas tradiciones incluso se reconocía a los nacidos vivos, es decir, la entidad humana se corresponde específicamente a los seres homínidos que son capaces de auto percibirse como humanos (homo sapiens sapiens). Con el avance del posmodernismo y la aparición de los discursos ideológicos que han puesto en duda el concepto de persona y ha dado lugar a varias interpretaciones extensivas que se han considerado por respeto a las libertades fundamentales, en este sentido, el posthumanismo y el transhumanismo desdibujan el concepto de lo humano y de la persona como sujeto, en lo que se puede identificar como un liberalismo tardío que posesiona al concepto de persona como ídolo vaciado, desconociendo la etimología del concepto e incluso, la estructura del lenguaje.

La consideración de “humanizar” a las maquinas, a los programas de computador (software) o, a cualquier otra producción digital, viene tomando fuerza en el discurso posthumanista, que en primera instancia se apoderaba de la defensa de los derechos de los

animales y que en el caso ecuatoriano se llegó más lejos, reconociendo los “derechos de la naturaleza” en la Constitución de 2008. Sin embargo, cabe aquí considerar que como entes naturales somos parte de un medio (ecosistemas) y nos relacionamos con el mismo (procesos culturales). Pero, considerar nuestras creaciones incluyendo el mundo virtual, es una irrupción al orden natural de las cosas, la virtualidad supero los límites de lo abstracto, ya no se puede distinguir solamente entre el mundo de los fenómenos y el de los conceptos, hay que sumar el mundo virtual.

No obstante, reconocer derechos a “personas artificiales” (Morán, 2021) implicaría estirar el concepto de persona, más allá de la entidad biológica que consiste en la base material de la persona, las personas jurídicas que son artificios sociales están compuestas por personas naturales, mientras que las “personas artificiales” podría significar desde avatares personales, IA con niveles de autonomía, hasta robots dotados de la misma, para una mejor comprensión debemos considerar lo siguiente:

En el ámbito de la ficción científica, Isaac Asimov propuso en la década de 1940 un conjunto de principios orientadores para el comportamiento de los robots, que posteriormente influirían en reflexiones éticas y jurídicas sobre la interacción entre seres humanos y sistemas automatizados. Estas normas, concebidas inicialmente con fines literarios, delineaban una jerarquía funcional de deberes: en primer lugar, impedir cualquier daño a los seres humanos, incluso por omisión; en segundo término, obedecer las órdenes impartidas por personas, salvo que contradigan la regla anterior; y, finalmente, procurar la autopreservación, subordinada a las dos normas previas. Años más tarde, el autor incorporó un principio adicional de carácter más amplio, que establece la prohibición de causar perjuicio a la humanidad en su conjunto, incluso

mediante la pasividad. Aunque estas disposiciones no tienen fuerza normativa en el derecho positivo, su estructura lógica ha servido de referencia conceptual en debates contemporáneos sobre la ética algorítmica y el diseño de sistemas autónomos.

A pesar de que las leyes propuestas por Asimov prevén que los robots antepongan su propia seguridad a la seguridad de los humanos, existe la posibilidad de que se generen paradojas como las que se han propuesto en el cine y en las obras de ciencia ficción. Sobre todo, cuando la IA alcance la "singularidad tecnológica", instancia que le permitiría niveles de autonomía superiores a la mente humana puesto que su capacidad de procesamiento de información, análisis, predicción y toma de decisiones se realiza con mayor velocidad y sin la interferencia de las emociones humanas, privilegiando el razonamiento lógico. Lo que podría llevar a la maquina a inferir que el mayor riesgo para la humanidad es la propia humanidad y decida revelarse para salvaguardar el futuro de la especia humana bajo condiciones controladas por la IA. Existen varias propuestas de clasificación de las IA, consideremos la propuesta de Daniel Martínez señalada en el artículo de Alejando Morán Espinosa:

"a) IA Asistida: colabora en las tareas para realizarlas con rapidez. b) IA Automatizada: realiza tareas cotidianas y excepcionales de forma automática, generalmente de apoyo administrativo en el sector empresarial (administración). c) IA Aumentada: facilita la toma de decisiones, aprendiendo de la interacción realizada y los resultados obtenidos (sugerencias no solicitadas de navegadores y redes sociales). d) IA Autónoma: su capacidad es la toma de decisiones sin intervención humana". (Martínez D., como se citó en Morán, 2021, p. 293).

Las 4 características identificadas por Martínez son programas específicos que responden a tareas, predicciones y toma de decisiones basados en análisis de datos y que son capaces de

inferir de la información obtenida para evaluar la eficiencia de las posibles respuestas optimizando la calidad de las respuestas y ahorrando tiempo. Para lo cual, poseen capacidades o técnicas que emulan las inteligencias humanas, dichas capacidades son descritas por Morán como:

> Aprendizaje automático (machine learning analíticas de texto y NLP, siglas en inglés de procesamiento de lenguaje natural, utiliza las analíticas de texto para descifrar la estructura de enunciados, su significado, entonación y hasta la comprensión); Ingeniería del conocimiento (knowledge engineering); Lógica difusa (fuzzy logic); Redes neuronales artificiales (artificial neural networks); Sistemas reactivos (reactive systems); Sistemas multiagente (multi agent systems); Sistemas basados en reglas (rule based systems), Razonamiento basado en casos (case based reasoning); Sistemas expertos (expert systems); Redes bayesianas (bayesian networks); Vida artificial (artificial life); Estrategias y computación evolutiva (evolutionary computation); Algoritmos genéticos (genetic algorithms) y Técnicas de representación de conocimiento y redes semánticas (semantic networks). (Morán, 2021, p. 293).

Las capacidades descritas, nos permiten comprender que las habilidades de aprendizaje, de inferir y deducir, de generar análisis complejos en tiempo real, de procesar datos complejos en tiempo reducido y generar información que permite comprender los fundamentos de la vida por los descubrimientos realizados en el campo de la genética y la decodificación del genoma humano. Lo cual abre nuevas fronteras a nuevos conocimientos y que con la asistencia de la IA se ha podido recopilar y procesar una mayor cantidad de datos, realizar simulaciones y generar predicciones con mayor eficiencia y en menor tiempo. Así mismo, las IA con redes semánticas ya están siendo utilizadas en algunos países como Colombia, en donde colaboran en la

sistematización de archivos digitalizados, que pueden ser pruebas, testimonios, escritos y demás insumos jurídicos, para organizar la información y proporcionar recomendaciones para la toma de decisiones, resoluciones, sentencias y veredictos.

En Colombia nuestra disposición procesal residual, Código General del Proceso, Ley 1564, no emplea en ninguno de sus contenidos la expresión ni los vocablos “inteligencia artificial”, tampoco lo hace nuestra actual disposición procesal especial, Código de Procedimiento Administrativo y de lo Contencioso Administrativo, Ley 1437; sin embargo, este silencio no implica que, para el ejercicio del proceso, medios de control, procedimientos, acciones o recursos, etc., ya se esté probando e incluso se hayan adoptado mecanismos u herramientas que tienen injerencia sobre los actos y etapas de las formas propias de cada juicio, sin importar la especialidad o ámbito de aplicación. (Guerra, D., et al, 2022, p. 9)

Hasta aquí, la generalidad tratada nos sirve para considerar si en un futuro se podrá concebir a la IA y los entes mecánicos conectados o dotados de la misma sean susceptibles de ser considerados sujetos de derecho, considerando que en el Ecuador se ha reconocido a la naturaleza como sujeto de derechos, particularmente porque el desarrollo tecnológico está ya en condiciones de influenciar en lo biológico, lo que alteraría el concepto tradicional de lo humano y ha generado constantes debates sobre la bioética. Aunque no nos compete prever la problemática señala, es importante considerarla, debido a que los avances en la ingeniería genética se han intensificado gracias a las aportaciones de IA en el procesamiento del genoma humano y los fundamentos de la vida orgánica, los avances en la física y otras ciencias como la medicina generan algunas interrogantes en la capacidad de comprender y manejar estas nuevas

habilidades, que nos acercan a lo divino. (...) tal como Yuval Harari lo ha proclamado bajo el concepto de ‘Homo deus’. (Andruet, et al., 2022, p. 27).

No obstante, desde la negatividad se puede apreciar que el acceso a la tecnología es restringido y que la gran masa humana ignora toda la complejidad del fin de la modernidad y el principio de un mundo nuevo, que aún sostiene una delgada frontera entre lo real material y lo virtual. La realidad es que somos infantes con acceso a poderes de los cuales no nos hacemos responsables y que esa accesibilidad está privilegiada a las personas que poseen capital, de momento no se democratiza, ni se redistribuye los conocimientos, equipos y tecnologías con la población mundial en general, considerando que son pocos los países con capacidad de producir y albergar computadoras cuánticas.

El preámbulo que se ha desarrollado es un esfuerzo de enmarcar la temática que nos atañe, la capacidad que tienen los sistemas de la IA para vulnerar derechos y en específico el derecho a la imagen (concepto que trataremos con mayor énfasis en los siguientes capítulos). Los sistemas de IA capacitados para generar contenido visual no poseen restricción alguna en el uso de imágenes y son capaces de encontrar datos en redes sociales puesto que las personas voluntariamente proveen de fotografías y archivos digitales que pueden ser requeridos por los usuarios para generar productos visuales que puedan afectar la honra de las personas. Además, de que al ser capaz de producir productos visuales de alta credibilidad pueden ser utilizados para cometer otra serie de delitos, lo que puede significar adentrarnos en debates interdisciplinarios complejos para ir determinando las tipificaciones legales para proteger a las personas de posibles delitos cometidos con asistencia de la IA o incluso realizados por la misma IA.

El derecho a la imagen como garantía constitucional:

El derecho a la imagen, reconocido por la Constitución ecuatoriana en su artículo 66, numeral 18[1], forma parte del conjunto de derechos personalísimos que garantizan la autodeterminación individual y la protección de la identidad visual en el entorno físico y digital. Este derecho reviste particular importancia dentro del sistema de protección de datos personales, en tanto la imagen constituye un dato biométrico sensible, vinculado de manera unívoca a la identidad del sujeto. En línea con la doctrina desarrollada por Carlos Alberto Ghersi (2019), la imagen debe entenderse como una expresión jurídica de la personalidad, cuya titularidad confiere a cada individuo el control exclusivo sobre su captación, reproducción y difusión, salvo en los casos limitados por razones de interés público.

La relevancia de este derecho se proyecta sobre otras garantías constitucionales, como la protección de datos personales y el derecho al honor y la intimidad (Art. 66.20[2] Constitución)**.** La manipulación o divulgación no consentida de imágenes puede constituir una injerencia ilegítima en la vida privada de la persona, afectando su dignidad y menoscabando su reputación. En consecuencia, el tratamiento de la imagen debe sujetarse a los principios rectores de la protección de datos (legalidad, consentimiento, finalidad y proporcionalidad) a fin de asegurar su uso legítimo y respetuoso de los derechos fundamentales en el contexto de la sociedad digital.

El uso de la imagen está sujeta al consentimiento de las personas, las mismas que voluntariamente suben archivos digitales con sus imágenes a las redes sociales. De ahí, cualquier usuario de internet, puede acceder, descargar, copiar y utilizar imágenes para generar contenido

[1] 18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona.
[2] 20. El derecho a la intimidad personal y familiar.

con aplicaciones de IA. Sin que exista restricciones explícitas sobre el uso de imágenes de personas, por lo que se ha publicado imágenes y videos de gente famosa en situaciones comprometedoras o para generar contenidos direccionados a influenciar a la gente para obtener resultados específicos.

Ahora bien, las protecciones constitucionales no surten efecto, sino existe un marco jurídico que provea de mecanismos efectivos que protejan el derecho a la imagen. De momento no se ha visualizado un proyecto de ley que haga referencia al uso de las IA y la consideración de las posibles violaciones que se puedan cometer en cuanto al uso deliberado de imágenes de personas sin consentimiento. Considerando que la implementación y acceso a las IA en el Ecuador ya es una realidad, por lo que es necesario contemplar posibles regulaciones para la protección efectiva de los derechos de las personas, además de generar espacios de capacitación continua para que la población tenga un mayor entendimiento sobre el uso y aplicaciones responsables de la IA.

Si bien, existe la Ley Orgánica de Protección de Datos Personales y su Reglamento, no se ha tipificado condiciones de uso adecuado y de usos no adecuados de la IA que además puedan implicar violaciones o delitos. Debido a que la capacidad de las IA diseñadas para generar contenido visual, pueden imitar datos personales o biométricos como la imagen y la voz de las personas para generar contenido audiovisual, en los cuales es muy difícil distinguir entre creaciones de la IA y producciones personales generadas por las personas principalmente para proporcionar contenido en redes sociales.

Inteligencia artificial: definición y alcances

La inteligencia artificial (IA) puede entenderse como el conjunto de sistemas tecnológicos diseñados para replicar procesos cognitivos humanos, tales como el aprendizaje adaptativo, el razonamiento lógico, la resolución de problemas complejos y la generación de contenido creativo (OCDE, 2019). Esta capacidad de emulación convierte a la IA en una herramienta de creciente impacto en diversos ámbitos, incluido el jurídico, donde plantea desafíos novedosos en torno a los derechos de la personalidad, particularmente el derecho a la imagen.

En el contexto de las tecnologías emergentes, ciertas aplicaciones de inteligencia artificial generan desafíos importantes en cuanto a la representación visual y la protección de la identidad individual, lo cual plantea interrogantes sobre la responsabilidad jurídica derivada de su uso. La inteligencia artificial generativa, por ejemplo, ha dado lugar a herramientas capaces de producir imágenes o videos con un nivel de realismo notable. Un caso ilustrativo son los denominados deepfakes, que emplean sofisticadas técnicas de edición audiovisual para insertar rostros o voces humanas en escenarios falsos, pero visualmente creíbles, generando confusión respecto a la autenticidad del material.

Asimismo, plataformas como DALL·E o MidJourney han facilitado la creación de retratos hiperrealistas, tanto de personas reales como ficticias, a partir de simples descripciones textuales, sin requerir imágenes originales como base. Este tipo de herramientas contribuye a ampliar el debate sobre el uso no autorizado de la imagen personal en entornos digitales.

Otra manifestación de preocupación es el uso de algoritmos biométricos en el reconocimiento facial, utilizados para verificar identidades a través de fotos o videos. Aunque estas tecnologías suelen implementarse con fines legítimos, como el control de acceso o la autenticación de usuarios, también pueden derivar en prácticas problemáticas cuando se usan para seguimiento o categorización automatizada de personas sin consentimiento, lo cual puede transgredir principios fundamentales como la legalidad, la proporcionalidad o la confidencialidad de datos sensibles. Además, su integración en sistemas de vigilancia o en plataformas de redes sociales potencia su alcance y el impacto sobre derechos fundamentales.

Por otro lado, la falta de regulación específica sobre el uso de datos biométricos en inteligencia artificial genera vacíos normativos que dificultan el control sobre su aplicación. En muchos casos, estos algoritmos pueden generar material visual sin que exista una autorización expresa por parte del titular de los datos, facilitando así la producción de contenidos falsos —incluidos videos o imágenes que simulan rasgos personales con notable precisión— sin necesidad de intervención humana directa. A medida que estas tecnologías evolucionan hacia mayores niveles de autonomía, aumenta también el riesgo de que generen contenidos sin supervisión, lo que eleva su potencial para representar a personas reales sin su consentimiento.

En el campo específico de la producción audiovisual, las consecuencias jurídicas del uso de inteligencia artificial aún no están claramente definidas. Aunque se ha demostrado que los contenidos creados con estas tecnologías pueden alcanzar un nivel de realismo que dificulta su diferenciación de la realidad, el ordenamiento jurídico actual no ha desarrollado parámetros concretos que regulen su aplicación. Esta carencia normativa deja a las personas expuestas a posibles vulneraciones del derecho a la imagen, ya que tales herramientas pueden ser empleadas

con fines lesivos, como la difamación, el fraude de identidad o el chantaje. A esto se suma la falta de procedimientos eficaces que permitan prevenir, sancionar o reparar este tipo de afectaciones de manera oportuna.

Las herramientas y técnicas antes señaladas pueden ser clasificadas según su potencial lesivo. En efecto, tecnologías como los deepfakes y los generadores de imágenes sintéticas permiten la creación de contenido hiperrealista sin el consentimiento de las personas. Este tipo de representaciones puede ser utilizada en contextos de difamación, extorsión, suplantación de identidad o violencia simbólica, generando daños psicológicos y a la reputación generando estigma social. Al no existir jurisprudencia previa, los riesgos que se pueden vislumbrar del uso de la IA son alarmantes y conforme se potencialice su uso, se debe considerar mecanismos jurídicos que permitan la protección efectiva de los datos personales en el entorno digital. (Zuboff, 2019; Corte IDH, OC-24/17; ONU Mujeres, 2023).

Es importante señalar que los riesgos y beneficios que la IA pueda proveer aún son difusos y solo vemos la punta del iceberg. De momento las aplicaciones con IA son independientes, pero se pueden combinar para la generación de servicios específicos, actividad que ya se está implementando en áreas de administración en el sector privado, los resultados en cuanto al procesamiento, análisis y sistematización de datos permiten reducción de tiempo en los procesos y ayudan a organizar la información de manera más eficiente. Sin embargo, de aumentar los niveles de autonomía y la capacidad de auto relacionarse los riesgos aumentarían debido a que la IA ya no necesitaría del control humano para realizar tareas, pudiendo asignarse una agenda propia e independizarse para la toma de decisiones.

Semiótica de la imagen: bases teóricas para su protección jurídica

La semiótica, como disciplina es una rama de la lingüística dedicada al estudio de los signos y los procesos de significación (simbolismos), aporta un marco teórico valioso para comprender la naturaleza y el valor jurídico de la imagen, así como del derecho a la imagen. El ejercicio académico obliga a los investigadores a considerar la interdisciplinariedad para mejorar la objetividad a la hora de desarrollar un trabajo investigativo, comprender los conceptos como el concepto de imagen desde la lingüística y la etimología nos permitirá comprender su relación con el derecho para poder facilitar la identificación de vulneraciones. Así, la lingüística se convierte en una disciplina base para el análisis de textos y la comprensión hermenéutica del derecho y la ciencia jurídica.

Para el presente estudio tomaremos como referencia la categoría de Charles Sanders Peirce el "signo icónico" que se refiere a la relación de semejanza de la imagen o concepto con el objeto que representa configurando un código específico. En este contexto las imágenes de personas en fotografías y videos se corresponden como signos icónicos, lo que podría verse vulnerado con contenidos que afecten la honra, la intimidad y los datos personales. Para Humberto Eco, connotado lingüista, las falsificaciones de imágenes irrumpen el vínculo de iconicidad entre la imagen real y la natural semejanza con lo que se representa (Eco, 2000). Con la proliferación de los deepfakes la capacidad de generar insumos de audio, visuales y audiovisuales que pueden ser indistinguibles de la realidad es ya un hecho, por mucho que sean falsificaciones las imágenes tomadas con consentimiento o no, pueden ser manipuladas al nivel de que la salida proporcionada por la IA imite la producción en tiempo real.

Para una mejor comprensión del importante papel de la lingüística debemos considerar el concepto de significante y significado propuestos por Ferdinand de Saussure. A manera de ejemplo vamos a considerar la letra A, el signo A, tiene varios significados dependiendo de su contexto significante, es decir, desde la fonética se corresponde con el sonido ah, que a su vez es la primera letra del abecedario y la primera vocal, en matemática es una variable, etc. En el caso de las imágenes la representación de una persona sea por medio de un retrato artesanal (dibujo o pintura) o sea por medio de una fotografía, se corresponde a su semblante y se significa como representación de la persona. Ahora bien, el significante dependerá de la situación captada en el contexto de la imagen, un dibujo o retrato puede ser lesivo o inofensivo dependiendo del significante en el que está inmersa la imagen, al igual que una fotografía o video. No obstante, imágenes generadas por la IA con contextos totalmente diseñados pueden causar muchos perjuicios sino se considera a tiempo los potenciales riesgos en el uso deliberado de imágenes personales sin consentimiento, lo que puede afectar en gran medida los derechos de las personas afectando su honra y privacidad.

Para Paul Ricoeur la identidad personal constituye una construcción narrativa que se desarrolla con el paso del tiempo. Lo que se ha incrementado con la internet y la aparición de las redes sociales, que son espacios virtuales en donde las personas comparten historias de sus actividades mediante fotografías, videos y publicaciones de texto, hacen contacto con otras personas normalmente de sus círculos sociales quienes pueden interactuar mediante mensajes y reaccionar a las historias de sus contactos. Gracias a estos espacios virtuales, muchas personas alrededor del mundo se hicieron famosas o “virales” lo que ha generado nuevas “celebridades” que se conocen como “influencers”.

Ahora, con la implementación de la IA la producción de contenidos se ha incrementado y sin regulaciones pertinentes, las IA tienen acceso a la Internet de la cual pueden extraer datos de todos los lugares posibles, imágenes de personas, contenido audiovisual de toda clase y generar salidas con simulaciones de alta credibilidad. Lo que pone en riesgo la identidad personal y el derecho a la honra, mucho más si no existen márgenes jurídicos que protejan los datos personales en el uso de herramientas con IA, por lo que el contenido creado podría afectar la imagen personal al colocarla en situaciones comprometedoras o usar la misma para cometer delitos como chantaje, extorción y estafa.

Como hemos señalado con anterioridad, la imagen constituye un dato biométrico, un signo icónico y una construcción narrativa. Por lo que, al distorsionar la imagen personal a través de manipulaciones o creaciones sintéticas, puede fracturar esta construcción identitaria, generando confusión y daño a la autopercepción y la imagen social del individuo. Las afectaciones psicosociales pueden ser graves y de no haber regulaciones pertinentes que contemplen mecanismos reales de protección y reparación en el caso de violación de derechos mediante el uso de la IA o por creación autónoma de la misma, estaríamos ignorando el riesgo potencial y el cambio paradigmático que implica la cuarta revolución tecnológica.

Riesgos de la IA para el derecho a la imagen en Ecuador

El uso de la IA en el Ecuador está en su etapa de implementación, por lo que, de momento, no se ha realizado la migración tecnológica en todas las áreas posibles, aunque en algunas industrias ya se viene utilizando herramientas con IA sobre todo en el sector privado en las áreas administrativas y se propende implementar en el sector público, lo cual ha generado ciertas resistencias debido a que con la automatización de procesos se evitaría actividades al

margen de la Ley, como tramitadores, conflicto de intereses y filtración de información privilegiada, entre otras.

Desde este punto de vista la implementación de herramientas con IA proporcionaría una mejora en el servicio público, dotando de racionalidad y mejorando el procesamiento, análisis y organización de los datos y de la información, posibilitando el fortalecimiento de la transparencia y el acceso a información por parte de la ciudadanía, lo que significaría un riesgo positivo. Sin embargo, es necesario considerar que existe el peligro de que se empiece a depender de la tecnología y que eso se vea reflejado negativamente en la poca participación ciudadana en el control del Estado reduciendo aún más el interés de la ciudadanía en lo público.

Por otro lado, el uso privado y personal de las IA puede ocasionar usos lesivos, el uso indiscriminado de imágenes personales puede realizarse con el objetivo de afectar a las personas y sus círculos cercanos. El afectar la imagen personal ya consiste en un perjuicio grave que puede interferir en el medio social y en la autopercepción ocasionando problemas psicológicos y estigmatización social, lo que pueden derivar en traumas. Los riesgos psicológicos y sociales pueden ser drásticos si no se cuenta con mecanismos jurídicos seguros, eficaces y eficientes, además, cabe considerar que en el uso de datos personales no se ha contemplado los riesgos del uso deliberado de estos dentro de las leyes ecuatorianas.

El hecho de que se filtre una imagen alterada que contenga un escenario comprometedor para una persona, le puede significar problemas personales, familiares e incluso laborales. Se ha visto la publicación de videos cortos de personas famosas, como políticos, tanto nacionales como internacionales en los que los opositores se daban un beso apasionado, del cual se puede inferir con inmediata claridad que es un producto visual falso. No obstante, un infante o una persona no

muy informada en el ámbito político, pudiera inferir que el contenido es real, lo que plantea varias problemáticas sobre las libertades que se puede tomar para la creación de contenido sin consentimiento de las personas, donde sus imágenes pueden ser manipuladas y utilizadas para crear contenido lesivo.

Impacto psicosocial y jurídico

Para poder identificar los usos lesivos que pueden ocasionarse por el uso de herramientas con IA capaces de manipular, usar y modificar imágenes generando contenido hiperrealista. Se debe considerar las afectaciones psicológicas, sociológicas y psicosociales que pueden ser devastadoras y su impacto en la ciencia jurídica también puede ser perjudicial para la sociedad, en tanto los debates para normar el uso y aplicación de herramientas con IA se van tornando lentos y complejos mientras que las capacidades de la IA se continúan entrenando, refinando y avanza a pasos agigantados.

La vulneración del derecho a la imagen mediante la IA trasciende la esfera puramente legal, pues la ciencia jurídica nace, se nutre, se refuerza, se adapta y modifica de acuerdo con los eventos sociales, políticos y culturales, en su afán de comprender y normar el comportamiento humano por lo que está estrechamente ligada al resto de las ciencias sociales y a la filosofía. Ya habíamos establecido la estrecha relación entre la lingüística y la ciencia jurídica para poder identificar los conceptos que nos sirven para enmarcar la problemática de la vulneración del derecho a la imagen mediante el uso de herramientas de generación de contenido audiovisual con IA, así mismo, es importante determinar los campos compartidos entre la sociología, la psicología y el derecho, para vislumbrar los efectos negativos y positivos del uso de la IA, en este sentido, partiremos por los siguientes conceptos: **1) Daño moral**: En el cual, las víctimas de

montajes, como los deepfakes de contenido sexual o difamatorio, cargan con un sufrimiento tan invisible como real, en el que la ansiedad y la depresión se instalan como huéspedes no deseados; y, **2) Erosión de la verdad:** La capacidad de la inteligencia artificial para producir falsificaciones casi perfectas convierte a la verdad en un espejismo; lo falso se presenta como real y lo verdadero comienza a ser cuestionado.

El daño moral que puede surgir de la manipulación de la imagen puede ser clasificado desde varias aristas. En primera instancia desde su valor simbólico, se debe considerar el sentido significante del uso de la imagen, es decir, en el contexto que esté inmersa la imagen de una personal y el mensaje que se desprenda del contenido completo del producto de salida generado por las herramientas de IA siendo el resultado final una fotografía y/o una imagen alterada. Desde las herramientas de generadores de imágenes, los contenidos pueden ser usados para amedrentar, estafar, chantajear, extorsionar, etc. Desde la creación de contenido (noticias falsas, solicitud de ayudas económicas, propuestas de negocios ficticios, etc.) que puede afectar las relaciones personales de las personas involucrados en el contenido, afectando su credibilidad y su honra lo cual esta intrínsecamente ligado a la autopercepción moral.

Es importante considerar, que la identidad personal está construida por el medio social y el temperamento. Esto, desde la tradición de la psicología sobre todo desde el estructuralismo y el funcional estructuralismo, siendo un elemento fundamental la percepción que tengan los miembros de una sociedad sobre los individuos que componen la misma. Dicha percepción construye la reputación y fortalece las relaciones interpersonales, que se pueden ver afectadas por la divulgación de una imagen manipulada que sea ampliamente difundida, la cual puede inferir en la autopercepción y en la percepción social causando daño moral y crisis existencial, lo

que conlleva, a una desconexión del sentido propio de la imagen, de una alteración en la narrativa propia de la forma en la que se concibe la persona, quien se puede llegar a alienarse de su propia auto determinación y su bienestar emocional.

En ese mismo sentido, el uso de deepfakes pueden ser mucho más lesivos debido a que los productos generados son hiperrealistas y en el caso de contenido audiovisual puede simular gestos y la voz, lo que puede ser usado para configurar delitos como los previamente señalados con la diferencia que desde este tipo de herramientas se puede generar videos con contenido realista. Las imágenes fotográficas o las generadas constituyen un riesgo considerable por la calidad que sostienen, mientras que en la producción de videos la credibilidad de estos puede ocasionar daños a la autopercepción. Lo cual, se incrementan, puesto que, incluso pueden causar problemas psicológicos profundos que podrían alterar la percepción de la realidad y tener consecuencias incluso en la salud de la memoria impactando la narrativa de la autopercepción de las personas afectadas y provocar trastornos de la personalidad.

No obstante, la exposición de contenidos manipulados por IA puede desembocar en trastornos psicológicos más profundos de los previamente señalados. Los deepfakes y las imágenes creadas por IA pueden generar trastornos como cuadros de ansiedad, depresión, estrés postraumático (TEPT) e incluso disociación de la personalidad. Dichos trastornos psicológicos pueden generar cuadros de ansiedad social, aislamiento, desconfianza, paranoia, psicosis y comportamientos autodestructivos que pueden llevar a las personas al suicidio. En principio, la ansiedad y la depresión se presentan generalmente ante la exposición a contenidos falsificados que contengan situaciones comprometedoras, ridiculizantes o sexualmente explícitas, como síntoma común en cualquier persona víctima de exposición pública con difamaciones, más, si

están reforzadas por imágenes, lo que atenta directamente a la reputación e integridad de las personas. La pérdida de control sobre la propia imagen y la incertidumbre sobre quienes hayan tenido acceso al contenido publicado puedo provocar la sensación de angustia y un estado de alerta constante que puede derivar en paranoia y psicosis. Lo que se puede ahondar dependiendo de los casos, considerando que cada individuo procesa los eventos del medio social de manera subjetiva, por lo que hay personas que pueden desarrollar TEPT lo que haría que sean propensos a revivir el trauma causado por la exposición de contenido falsificado que afectaron su integridad o al encontrar personas cercanas que hayan sufrido la misma situación o ser expuesto a situaciones similares, lo que puede causar cambios negativos en la forma de pensar y en el estado de ánimo.

Se debe considerar que la exposición prolongada a este tipo de violencia digital puede provocar trastorno paranoide, que desarrolla una desconfianza generalizada hacia los demás miembros de la sociedad en la que interactúa y se desenvuelve; trastorno esquizoide, que se caracteriza por el distanciamiento de las relaciones sociales y que puede llegar a generar un cuadro de esquizofrenia, lo que puede tornarse peligroso para la persona y sus círculos cercanos. Estos trastornos afectan profundamente la calidad de vida de las víctimas, al interferir con su capacidad para establecer relaciones saludables y tener acceso a una vida social activa.

Con la finalidad de enmarcar el presente estudio, consideraremos el interaccionismo simbólico propuesto en la teoría de Erving Goffman y su metáfora con la teatralidad de la vida cotidiana, usado para analizar las instituciones sociales, políticas y económicas. Para lo cual, es importante señalar que para Goffman la puesta en escena de un individuo está marcada por el escenario en el que interactúa, así, su comportamiento estará orientado a proyectar la mejor

imagen posible con la finalidad de obtener respuestas determinadas de los otros actores dentro de la interacción social. En palabras del autor:

Cuando un individuo llega a la presencia de otros, estos tratan por lo común de adquirir información acerca de él o de poner en juego la que ya poseen. Les interesará su status socioeconómico general**,** su concepto de sí mismo, la actitud que tiene hacia ellos, su competencia, su integridad, etc. Aunque parte de esta información parece ser buscada casi como un fin en sí, hay por lo general razones muy prácticas para adquirirla. La información acerca del individuo ayuda a definir la situación, permitiendo a los otros saber de antemano lo que él espera de ellos y lo que ellos pueden esperar de él. Así informados, los otros sabrán cómo actuar a fin de obtener de él una respuesta determinada. (Goffman, 1981, p. 13)

Sin embargo, si esta información es falseada y promovida sin consentimiento, ni control por parte de un individuo, puede generar estigmas sociales. Como se ha venido señalando, las afectaciones a la reputación pueden generar conflictos sociales afectando la interacción de los individuos con la víctima. Puesto que, el estigma social es una marca simbólica de que esa persona ha atentado contra los fundamentos morales de la sociedad y que por ende merece ser relegado y estigmatizado. Según Goffman:

Los griegos, que aparentemente sabían mucho de medios visuales, crearon el término estigma para referirse a signos corporales con los cuales se intentaba exhibir algo malo y poco habitual en el status moral de quienes lo presentaba. (...) En la actualidad, la palabra es ampliamente utilizada con un sentido bastante parecido al original, pero con ella se designa preferentemente al mal en sí mismo y no a sus manifestaciones corporales. (Goffman, 2006, p. 11).

En este nuevo escenario global, que además es virtual y que puede llegar a manifestarse en el plano de lo real material, las interacciones sociales se ven interpeladas por un nuevo espectro que como característica fundamental acorta tiempo y distancia. Es decir, que los individuos pueden expandir sus círculos sociales y generar espacios virtuales para interactuar en ellos y en donde el uso de máscaras o la adopción de personajes es versátil lo que dificulta la consolidación de interacciones sociales con propósito, más allá de la distracción y el entretenimiento. Consecuentemente, se hace necesario considerar el contexto social e histórico del Ecuador y su papel en las nuevas fronteras de la globalización en la era digital.

En segunda instancia, vamos a considerar el contexto social del Ecuador, desde lo cual hay que considerar algunos puntos como la administración de justicia, la historia jurídica y política, las costumbres y mitos con el factor constitucional de lo plurinacional para comprender el tejido social del País. El Ecuador está compuesto por 14 nacionalidades indígenas, pueblos montubios y mestizos blancos, los cuales han sido reconocidos en la Constitución de 2008 en la que se reconoce derechos de autonomía, lo mismo que no se ha materializado debido a que el Estado plurinacional suponía la generación de confederaciones con territorios delimitados por nación con competencia jurídica autónoma basada en las costumbres y cultura propia.

No obstante, la delimitación territorial se realizó manteniendo la estructura tradicional del Estado liberal que se suponía se dejaba atrás. Pues no se realizó el trabajo de identificar la demografía que se autoidentifica como parte de una nación determinada y su ubicación de forma que se estableciera fronteras determinadas, debido a que la división política del territorio sigue conservando el sistema de parroquias, cantones y provincias. El problema es que existen poblaciones de distintas naciones conviviendo en una jurisdicción territorial sin que se delimite

las capacidades autónomas de los pueblos, contradicción que se asienta en las ciudades y que de momento no se observa capacidades de autonomía territorial a pesar de que existe el reconocimiento de comunas y comunidades dentro de la jurisdicción de los GADs (Gobiernos Autónomos Descentralizados) municipales las cuales no ejercen sus derechos debido a que se consideran GADs parroquiales, sin embargo responden a las políticas públicas de los GADs Municipales, los mismos que evitan la promoción de la autonomía territorial de las comunas y comunidades, puesto que sus políticas y tradiciones pueden entrar en conflicto con las políticas públicas impulsadas por los gobiernos municipales.

Ahora bien, a pesar de las falencias y contradicciones que se han generado desde la posesión de la nueva constitución, lo que cabe señalar del contexto multicultural es que cada nación tiene sus propias formas culturales, costumbres e imaginario colectivo que no se corresponde con la tradición occidental (incluyendo a los blancos mestizos). Y que se debe contemplar para poder generar normativa general que proteja los derechos de los pueblos desde su propia autodeterminación, debido a que el concepto de imagen varia desde cada nación y cada individuo proyecta la pertenecía a dicha nación desde su propia imagen personal, sea por fenotipo racial, vestimenta y/o autoidentificación y correspondencia cultural con la nación a la que se pertenece.

En cuanto a la cultura jurídica del Ecuador, como hemos señalado con anterioridad desde 1830 hasta la actualidad ha habido 20 constituciones, es decir, la República se ha fundado en 20 ocasiones y en cada una de estas refundaciones existió un determinado proyecto político que incluida la última constitución no logró generar una coalición identitaria de lo ecuatoriano, mucho menos desde la idea de lo plural como componente unificador. Puesto que, después de 17

años no se ha reformulado el Estado para que se convierta en un Estado plurinacional competente, el solo hecho de que la Asamblea Nacional no esté compuesta por la presencia proporcional de las naciones que componen el Estado y que se mantenga las elecciones con la división política territorial tradicional, es muestra de que no se ha dado pasos significantes en la consolidación del Estado plurinacional.

Además, cabe considerar las problemáticas tanto académicas como prácticas del derecho y del derecho ecuatoriano. A saber, desde la época de Constantino se produce el evento de transición de la Ley divina a la Ley del hombre, que no pasó de ser una retórica, puesto que, traspasar la dimensión sacra de la Ley divina a la Ley del hombre que se basaba en la racionalidad y que posteriormente se intensifica en el renacimiento, se configuró la positividad de las ciencias y sobre todo de la ciencia jurídica. En donde se embiste a la figura del Juez como elemento social apto para juzgar las controversias legales entre los ciudadanos y el Estado. Previamente en el caso europeo, quienes ejercían estas capacidades eran los Señores y los Reyes con total soberanía, pues la misma era atribuida a una posición divina, es decir, eran autoridades puestas por los dioses y que contaban con tradición de nobleza, la misma que se adquiría por el desempeño en batalla o por acciones que beneficiaban a la comunidad.

El establecimiento de audiencias se realizaba en la corte de los señores y si el caso era más prominente se atendía en la corte del rey, zar o quien ejercía la soberanía, en el cual se escuchaba los testimonios de las partes para poder establecer una determinada solución o juicio para la resolución de controversias o de delitos cometidos. Por supuesto, el evento sostenía en las ordalías, el juramento de los presentes ante los dioses, consistiendo en un ritual sagrado para reestablecer el orden irrumpido, la justificación de la capacidad de juicio de quien ejercía la

soberanía o se pronunciaba en nombre de ella, estaban avalados por la tradición y posición social. Que ya en la modernidad se otorga la categoría de honorabilidad al Juez, basado en sus méritos académicos y en su calidad profesional, lo cual se ha ido desgastando en el estado-nación y que en Hispanoamérica no se cuenta con una tradición racional de independencia de poderes, lo que ha convertido a la justicia en una práctica de mercado impulsada por las élites y que ha desbordado en corrupción, por lo que los ciudadanos y usuarios han ido perdiendo la confianza en los sistemas judiciales. En palabras de Jordi Neiva Fenoll:

(...) confiamos simplemente en un ser humano: el juez. Le creemos con capacidad para determinar si el reo miente, si la víctima miente o si los testigos mienten. Le suponemos especialmente dotado para interpretar dictámenes periciales, e incluso para acceder al fondo de los mensajes que se escondan tras la muy numerosa prueba documental que hoy adorna al proceso penal, gracias fundamentalmente a la tecnología. Los procesos se han llenado de conversaciones de chat, audios, fotografías y todo tipo de grabaciones, que son los documentos de nuestra época, antes más excepcionales, y hoy al alcance de cualquiera a través de algo todavía más suave que un click. (Neiva, J., et al, 2022, p. 20-21).

Con el avance de la tecnología, hoy se considera pruebas a medios que antes no se los podía considerar debido a que no existían como grabaciones de audio, de video y de audio/video. En el pasado reciente, no había confianza en estos insumos debido a que son susceptibles de alteraciones, sin embargo, con el avance de las ciencias, la capacidad pericial ha ido mejorando por lo que la contribución técnica de las ciencias arroja evidencia cada vez más confiable para esclarecer los hechos controvertidos. A pesar de esto, aún se confía en los interrogatorios como en el pasado, en donde el testimonio era la prueba más confiable por la falta de procesos de

investigación y elementos de peritaje, y porque la producción de documentos no era fiable, como bien parafrasea Neiva a Lara Peinado. (...) los interrogatorios en absoluto tienen la utilidad que se les atribuyó en el pasado. La razón es eminentemente científica y en parte histórica. En un mundo no tan lejano en que la pericia no existía y el documento era tantas veces una quimera, lo único que quedaba para demostrar algo era traer a alguien que dijera lo que había visto. (Lara Peinado, 1997 como se citó en Neiva, J., et al, 2022, p. 22).

El testimonio como prueba ha sido objeto de análisis durante todo el desarrollo de la ciencia jurídica, lo que ha devenido en el desarrollo teórico desde la doctrina para fortalecer los elementos fundantes del derecho, como la deontología, la jurisprudencia y la historia general y particular del derecho (historia del derecho en un país determinado). Neiva identifica tres momentos históricos que aportaron a la cientificidad del debido proceso:

La primera, nacida en la Europa continental (Norr, 2012, pág. 630), consistió a partir del siglo XIII en la creación del régimen de valoración legal de la prueba. El sistema partió de una cierta consciencia de que el juez no podía valorar la prueba en realidad, tal y como se ha explicado, aunque el trasfondo de dicho sistema se situaba sobre todo en el intento de evitar una valoración que, precisamente por la falta de elementos fiables de juicio y realizada por jueces delegados de la nobleza –por tanto, dependientes–, podía ser increíblemente arbitraria. (Norr, 2012 como se citó en Neiva, J., et al, 2022, p. 22-23).

El reconocimiento de la condición humana del juez y las limitaciones que esto implica, permitieron identificar el riesgo de la arbitrariedad lo que permitió para el futuro, abrir el debate sobre la independencia de poderes y el debido proceso, que aún en estas épocas sigue mostrando claros oscuros que no permiten identificar un tratamiento de la justicia desde el paradigma de la

racionalidad moderna, debido a que se continúa ejerciendo justicia desde el arreglo a intereses políticos y económicos.

La segunda solución surgió en el mundo anglosajón. En 1215 la baja nobleza inglesa consiguió librarse directamente de los jueces de designación real a través de la Carta Magna Libertatum, recurriendo en sus incisos 20 y 39 a un curioso mecanismo de origen romano que parece que pervivió en aquellas tierras en los pleitos civiles durante la Alta Edad Media: el jurado. (Neiva, J., et al, 2022, p. 23).

Para el análisis general, el jurado se ha mantenido dentro de la tradición anglosajona la cual fue traspasada al derecho estadounidense y proveía un veredicto para ayudar al juez a determinar su juicio. En la tradición del derecho ecuatoriano, no se ha contado con un dispositivo igual o parecido, siendo que la tradición oral fue incorporada en la Constitución de 2008, dejando atrás la tradición documental que todavía se sostiene pero que era limitada y vulnerable a arbitrariedades, con la inclusión de la oralidad, los testimonios volvieron a ser importantes y se concuerda con la tradicionalidad precolonial, sobre todo en la nación kichwa.

La última derivación de todo ello ha sido ya en nuestra época la mezcla de modelos, de manera que en la Europa continental se incorporó en parte el estilo de interrogatorio anglosajón, aunque dirigido a jueces y no a jurados, y en el Reino Unido se fue renunciando al jurado, pero no a esos interrogatorios tradicionales de su sistema, aunque intentando no llegar jamás al momento del juicio, tratando de pactar antes con el reo una culpabilidad con pena rebajada. (Neiva, J., et al, 2022, p. 24).

En la modernidad se estableció mecanismos aprendidos de la experiencia y se propendió a dar especial relevancia a los testimonios oportunos, en donde la parte implicada a la cual le recaía la responsabilidad podía aceptar la culpabilidad para acceder al beneficio de una pena rebajada. La valoración de la legalidad de las pruebas, incluyendo los testimonios, han encontrado problemas técnicos debido al incremento de conocimientos y al avance de las ciencias, por lo que la interdisciplinariedad ha tomado mayor relevancia sobre todo en el siglo actual, lo que limita la capacidad de los jueces y juristas debido a que no poseen el conocimiento adecuado para valorar peritajes técnicos generados desde otras ciencias, sobre todo desde las ciencias exactas, biológicas y la química.

A pesar de que la relación entre las ciencias sociales es mucho más estrecha e indefinida en tanto a las fronteras de conocimiento. Y que se ha implementado la interdisciplinariedad para determinar una objetividad en cuanto al levantamiento de evidencias y la verificación pericial de las mismas, como es el caso de la medicina y la antropología forense, también se incluye la psicología para la evaluación de testimonios y declaraciones. Además, de que se utiliza peritos especializados dependiendo de los casos y de la necesidad para determinar mediante el juicio de expertos, elementos que permitan esclarecer los hechos y fortalecer el debido proceso. Sin embargo, existe la limitante de que los jueces, expertos en derecho, puedan no estar dotados de los conocimientos científicos necesarios para valorar de forma objetiva los insumos aportados por científicos. (...) ese es el problema de la prueba pericial. Se le hace valorar a un lego lo que dictaminó un científico (Neiva, J., et al, 2022, p. 25). Para Neiva:

La alternativa de formar a los jueces en psicología del testimonio debiera ser valorada, aunque difícilmente podrían ser auténticos expertos al faltarles el fondo de armario de

conocimientos de un psicólogo. Por consiguiente, si algún día llega lo anterior y vemos muchos menos interrogatorios y más entrevistas cognitivas de psicólogos cuando sean realmente necesarias, el cambio en nuestro modelo procesal tradicional será reseñable, porque habremos abandonado definitivamente la tradición. (Neiva, J., et al, 2022, p. 24).

La ciencia, incluyendo a las sociales y en este caso a la ciencia jurídica, no puede dogmatizar la conjetura de conocimientos y experiencias por mantener "la tradición". Todas las ciencias avanzan o se reformulan en cuanto se presentan evidencias que desestiman los conocimientos adquiridos. Pues, la ciencia no es un sistema de creencias, sino una práctica académica que está en constante contrastación, ya que la ciencia parte de la duda y la experimentación para poder generar teorías y leyes científicas en la búsqueda de la verdad objetiva. Según Neiva:

Todo debería haber cambiado con el auge de la ciencia en el siglo XIX. Los médicos empezaron a poder hacer autopsias y examinar lesiones con un rigor creciente (Karl Virchow, 1854). Los químicos analizaban sustancias con cada vez más precisión. Luego vinieron los biólogos, los ingenieros, los psicólogos, los topógrafos y un sinfín de científicos que paulatinamente empezaron a aportar su asistencia en el proceso. (Virchow, 1854 como se citó en Neiva, J., et al, 2022, p. 24-25).

El problema es que (...) el juez no es competente para analizar esos criterios científicos, precisamente porque el juez no es un especialista en esas materias científicas. Es sólo un jurista. (Neiva, J., et al, 2022, p. 25). Dicha condición limita la capacidad del juez para realizar un veredicto objetivo al carecer de los conocimientos técnicos científicos para determinar la veracidad de los peritajes, así como el juicio de expertos. Lo que conlleva a cuestionar la

capacidad objetiva de los jurisconsultos sobre otras ciencias y esferas del conocimiento, según Neiva:

> La constatación de todo ello acaba haciendo que los jueces acepten ciegamente el parecer del perito (lo que ya ocurre ahora en no pocas ocasiones), o bien lo descarten sin razones de peso o, aún peor, ante dos dictámenes contradictorios sobre un mismo tema, decidan en favor de uno u otro según la mejor calidad de la redacción, lo que puede ser muy injusto porque esa claridad expositiva puede no ser más que retórica muy bien empleada. Pero el juez no tiene manera de saberlo con certeza. (Neiva, J., et al, 2022, p. 26).

Esta situación, evidencia los problemas de objetividad en la ciencia jurídica y en las ciencias sociales. Debido a que en muchas ocasiones se valora más la consistencia lógica y la congruencia que la intención del mensaje lo que limita el acceso a la justicia para personas que no estén familiarizadas con el ámbito académico, siendo indispensable la dependencia a la contratación de abogados. En el contexto ecuatoriano, dicha problemática se acrecienta debido a que no existe celeridad jurídica y que la mayoría de los jueces no son académicamente aptos y no hay procesos de selección objetivos, más bien, se favorece a juristas que están involucrados con élites o personajes políticos influyentes, quienes manipulan el sistema para poder obtener niveles de impunidad, lo que constituye una aberración a la racionalidad y fortalece la corrupción.

El acceso a la justicia se ha ido perdiendo con el paso de los gobiernos y la poca presencia de competencia académica y de valores éticos, que a pesar de que el espíritu de la Constitución es garantista y reconoce una gran gama de derechos, en la práctica es complicado acceder a un ejercicio pleno por parte de la ciudadanía, lo que pone en duda la racionalidad en el funcionamiento del aparato judicial. Si consideramos que no han existido debates pertinentes

sobre la protección de derechos en el caso de que exista vulneración por el uso de herramientas con IA y sobre todo en este caso, el derecho a la imagen, se puede identificar que el interés político se sobrepone al trabajo legislativo y que, de las leyes emanadas por dicho poder, a que se actúe con celeridad en el poder judicial, depende mucho de las relaciones sociales y políticas, las mismas que se corresponden más a privilegiar la astucia (viveza criolla) que el conocimiento y que beneficia a la descomposición social al trasladar valores del mercado al campo constitutivo legal que sostiene al Estado-nación o en este caso "Estado-plurinacional", lo que desgasta el sentido de pertenencia y hace de las leyes letra muerta.

La ausencia de mecanismos claros y efectivos en el acceso a la justicia, y en el ejercicio pleno de los derechos dificulta el análisis teórico, debido a que por más que se tipifique los usos de la IA para determinar los correctos de los incorrectos y la determinación de cuando estos últimos puedan implicar delitos o vulneración de derechos, pues existen vicios culturales como las interpretaciones extensivas que se realizan para inadmitir causas, alargar procesos o realizar abuso de poder con respuestas evasivas, hasta incluso ignorando sentencias en franco irrespeto a las leyes y a la Patria, sin caer aquí en nacionalismos o patriotismos, más bien, se trata de la defensa del racionalismo.

La intención de este contexto sociopolítico es enmarcar la realidad del ejercicio jurídico del Ecuador para poder adentrarnos en la problemática que nos atañe, la protección del derecho a la imagen, que como hemos señalado previamente existen riesgos potenciales en el uso de imágenes con herramientas de IA, los cuales se potencian cuando las instituciones estatales no son sólidas y no proveen de mecanismos eficientes para la protección, reparación y defensa de los derechos de la ciudadanía. Lo que podría instaurar un entorno adecuado para afectaciones

personales, daño moral e indefensión frente a compañías extranjeras quienes son proveedores de los servicios con IA.

En tercera instancia, el espectro psicológico y el entorno social son elementos que debemos considerar en cuanto a las salidas que proporcionen las herramientas con IA causen daño moral, como se ha manifestado con anterioridad las implicaciones psicológicas pueden causar problemas en la autopercepción que están ligados a la construcción de los valores morales de las personas. Una imagen que comunique algo comprometedor o bochornoso puede causar alteraciones en la personalidad, puede afectar la capacidad de distinguir la realidad y generar problemas relacionados con la ansiedad, la paranoia e incluso la esquizofrenia.

Además, desde la esfera social podría haber afectaciones a la reputación, a la credibilidad, podría afectar las relaciones personales, laborales, culturales y políticas, gracias a que el contenido generado es hiperrealista y por lo tanto de alta credibilidad, los riesgos de que contenido mal intencionado sea usado para intimidar, extorsionar, chantajear, estafar, etc.; afectarán los círculos sociales de las personas, a manera de ejemplo, una imagen que comprometa a una persona casada en una situación de infidelidad, podría llegar a el divorcio y la ruptura de una familia. Las repercusiones sociales tienen influencia en las concepciones psicológicas, religiosas e ideológicas de los individuos por lo que cambios negativos que alteren el entorno social de una persona podría generar traumas e incluso desembocar en situaciones de desequilibrio y tornarse violentos con los demás e incluso con ellos mismos.

En el caso de la erosión de la verdad propuesto por Delarbre, es plausible considerar que el uso deliberado de la IA ahonda un problema que parte desde la comunicación. Considerando que como se dice en el viejo adagio popular “una imagen vale más que mil palabras”, la

manipulación de imágenes personales dentro de creaciones malintencionadas va a tener un fuerte impacto en la narrativa personal y en la autopercepción, mucho más si la víctima adolece de problemas de memoria o alguna condición médica. A quienes convendría considerarlos como casos especiales, con delimitaciones precisas que provean mecanismos para tratar a los afectados considerando que las repercusiones psicológicas pueden ser más graves y que puede generar estigmatización social.

El desarrollo de tecnologías como los deepfakes ha debilitado notoriamente la confianza social en la autenticidad de los contenidos audiovisuales. Esta situación ha alterado la forma en que se percibe la realidad compartida, generando un entorno en el que se vuelve cada vez más difícil distinguir entre lo verdadero y lo manipulado. A medida que se difunde el conocimiento de que las imágenes y videos pueden ser intervenidos mediante inteligencia artificial, se acentúa el escepticismo frente a los medios digitales y a la información que circula en ellos. Esta pérdida de credibilidad no solo obstaculiza la validación de hechos, sino que también contribuye a generar un ambiente de desinformación que propicia la polarización de opiniones, debilita el consenso público y fragmenta la cohesión social.

Esta creciente desconfianza impacta de forma directa en los vínculos sociales, al erosionar los marcos de referencia simbólicos que orientan la interacción entre las personas. En escenarios donde la línea entre lo real y lo ficticio se desdibuja, los individuos pueden experimentar dificultades para ubicarse en su entorno, lo cual afecta tanto su percepción del espacio social como sus relaciones interpersonales. Cuando esta situación se prolonga, puede derivar en efectos psicológicos adversos, como ansiedad, retraimiento o desorientación,

especialmente en personas con mayor exposición a contenidos manipulados o en situación de vulnerabilidad.

Quienes han sido blanco de deepfakes pueden enfrentar una alteración profunda en su percepción de sí mismos, al ver distorsionados sus recuerdos o expuesta su imagen en contextos falsos. Este fenómeno, denominado gaslighting digital, puede menoscabar la autoestima, erosionar la confianza personal y generar estigmas sociales de difícil superación. En muchos casos, estas secuelas se traducen en un daño profundo a la identidad y a la reputación de las víctimas.

Dada la gravedad de las consecuencias psicológicas de los deepfakes, es fundamental que las víctimas tengan acceso a apoyo psicológico adecuado. La terapia puede ayudar a las personas a procesar el trauma, reconstruir su autoestima y desarrollar estrategias para enfrentar el acoso y la estigmatización. Siendo crucial que existan espacios públicos para el tratamiento de estos problemas y que estén al alcance de todos los ciudadanos, considerando que la vulnerabilidad del uso de imágenes personales afecta a todas las personas indistintamente de su condición socioeconómica, de salud, estado civil, edad, autoidentificación o preferencia sexual.

Además, es crucial establecer redes de contención que incluyan a familiares, amigos y comunidades de apoyo. Estas redes pueden proporcionar un espacio seguro para que las víctimas compartan sus experiencias y se sientan comprendidas y respaldadas. Favoreciendo la inclusión en sus propios círculos cercanos para evitar los estigmas y prejuicios sociales, permitiendo a la víctima reconstruir su narrativa identitaria y de ser necesario reinventar sus personajes para poder mantener y mejorar su interacción social. Para enfrentar las consecuencias psicológicas derivadas del uso de deepfakes, es necesario adoptar una perspectiva integral que combine

acciones preventivas, institucionales, educativas y normativas. Una estrategia eficaz debería partir de campañas de información pública que alerten sobre los riesgos de la manipulación audiovisual, así como de la importancia de verificar la autenticidad del contenido que se consume o se comparte. Esta sensibilización debe ir acompañada de mecanismos ágiles para responder ante la difusión de imágenes falsas, de forma que se actúe con prontitud tanto en la remoción del contenido como en la atención y acompañamiento a las personas afectadas.

Desde el ámbito educativo, se vuelve crucial incorporar el pensamiento crítico y la alfabetización digital como parte de la formación desde etapas escolares tempranas. Esta herramienta pedagógica permitiría preparar a niñas, niños y adolescentes para interactuar de manera responsable en entornos digitales, reconociendo riesgos y previniendo daños. Paralelamente, en el plano jurídico, urge avanzar hacia marcos normativos claros que tipifiquen y sancionen la producción y divulgación de contenidos manipulados sin consentimiento, particularmente aquellos que afectan la imagen, la voz o cualquier atributo personal vinculado a la identidad.

La manipulación de representaciones personales a través de inteligencia artificial representa una amenaza grave no solo para la privacidad, sino también para la salud mental de quienes resultan expuestos a estas prácticas. Las afectaciones psicológicas que pueden derivarse —ansiedad, pérdida de autoestima, estigmatización social— tienden a intensificarse en contextos donde no existen protocolos claros de protección institucional. Por lo tanto, se impone como una necesidad urgente el diseño de políticas públicas integrales que, sin limitar el desarrollo tecnológico, aseguren estándares mínimos de protección emocional y jurídica frente a estos nuevos riesgos digitales.

En definitiva, la manipulación de imágenes mediante inteligencia artificial constituye una amenaza compleja que compromete no solo la privacidad y la dignidad de las personas, sino también su estabilidad emocional y bienestar psicológico. Los efectos de estas prácticas, cuando no se controlan, pueden ser severos y persistentes, especialmente en contextos sociales donde aún no existen garantías institucionales eficaces para contenerlas. Por ello, resulta urgente implementar medidas de carácter preventivo, educativo y normativo que permitan responder a los desafíos que plantea el uso irrestricto de herramientas de IA, asegurando condiciones mínimas de protección jurídica y emocional para las personas y preservando la integridad del espacio digital como ámbito de interacción social legítima.

Capítulo II: Clasificación y riesgos de las herramientas de IA en relación con el derecho a la imagen

Introducción

El acelerado desarrollo tecnológico ha puesto en tensión los fundamentos tradicionales del derecho, obligándolo a responder ante fenómenos disruptivos que no se ajustan con facilidad a sus categorías clásicas. Entre los múltiples retos que surgen en este escenario digital, el derecho a la imagen ocupa un lugar especialmente delicado, debido al auge de herramientas basadas en inteligencia artificial capaces de generar, modificar o reproducir representaciones visuales y sonoras de personas reales, muchas veces sin su autorización o conocimiento.

En el caso ecuatoriano, esta problemática reviste una gravedad particular debido a la confluencia de tres factores estructurales: en primer lugar, la debilidad institucional para asegurar una protección eficaz de los derechos fundamentales en el entorno digital; en segundo lugar, la inexistencia de un marco normativo específico que regule la generación sintética de imágenes personales; y, finalmente, la acelerada expansión de tecnologías basadas en IA (como los deepfakes o los modelos de clonación facial y vocal), que pueden ser utilizadas para propósitos lesivos, sin que existan mecanismos jurídicos adecuados para prevenir o reparar las afectaciones que generan. La coexistencia de lagunas normativas, el crecimiento acelerado de tecnologías avanzadas y las debilidades institucionales en el ámbito nacional conforman un contexto especialmente vulnerable para la protección efectiva del derecho a la imagen en el Ecuador actual.

Este capítulo tiene como propósito examinar, desde una óptica técnico-jurídica, las principales tipologías de herramientas de inteligencia artificial que inciden en el tratamiento de

datos biométricos —especialmente imágenes— y los riesgos que estas tecnologías suponen para la protección del derecho a la imagen en el entorno digital ecuatoriano. Para ello, se plantea una clasificación funcional basada en el nivel de autonomía y en la capacidad de simulación de dichas herramientas, y se analizan los usos lesivos más comunes identificados en el país, así como las deficiencias normativas que obstaculizan una tutela efectiva de este derecho fundamental.

A su vez, se dedicarán secciones específicas al estudio de los fundamentos dogmáticos y constitucionales que vinculan el derecho a la imagen con la dignidad humana, abordando su naturaleza como dato biométrico sensible y su reconocimiento como bien jurídico dentro del entorno digital. Se tomará en cuenta lo establecido por la Ley Orgánica de Protección de Datos Personales (2021), así como las discusiones éticas y jurídicas en torno al uso de tecnologías de vigilancia algorítmica. En todos estos apartados, se hará énfasis en el contexto ecuatoriano, integrando referencias normativas nacionales, decisiones relevantes de la jurisprudencia constitucional e interamericana, y ejemplos concretos que evidencian la necesidad de reformar el marco normativo vigente de manera estructural.

En suma, este capítulo busca demostrar que la inteligencia artificial, en su dimensión generativa y automatizada, no constituye solo una herramienta neutra de innovación, sino también un campo emergente de conflicto jurídico, donde la protección de la imagen como expresión de la personalidad se juega frente a lógicas tecnológicas que, si no son reguladas adecuadamente, pueden desembocar en nuevas formas de violencia simbólica, discriminación algorítmica y afectación estructural de derechos.

Clasificación, evolución y riesgos de las herramientas de IA: desarrolladores, contexto histórico, impacto ambiental y amenazas al derecho a la imagen

La literatura especializada distingue cuatro categorías funcionales de inteligencia artificial, según el grado de autonomía y el tipo de tarea que ejecutan (Russell & Norvig, 2021):

Tabla 1

IA Asistida:	**Apoya tareas humanas mediante algoritmos predictivos o generativos (p. ej., redacción automática, asistentes conversacionales).**
IA Automatizada:	Sustituye actividades humanas repetitivas (p. ej., clasificación de imágenes, vigilancia digital).
IA Aumentada:	Potencia la toma de decisiones humanas a través del análisis de grandes volúmenes de datos (big data).
IA Autónoma:	Actúa sin supervisión humana directa, con capacidad de aprendizaje adaptativo (p. ej., sistemas de vigilancia con reconocimiento facial y toma de decisiones automáticas).

Fuente: elaboración propia

Cada una de las categorías funcionales de la IA previamente señaladas (asistida, automatizada, aumentada y autónoma) pueden representar riesgos potenciales, diferenciados para el derecho a la imagen, que se magnifican cuando las tecnologías implicadas incorporan o procesan datos biométricos, o bien simulan visual o sonoramente la imagen signo de identidad de una persona. Esta amenaza se vuelve particularmente sensible en entornos jurídicos donde el reconocimiento del derecho a la imagen no ha sido acompañado por una infraestructura legal y técnica adecuada para enfrentar los desafíos de la era digital.

El derecho a la imagen, entendido como una manifestación del principio de dignidad y de la autodeterminación informativa, protege tanto la captación como la reproducción y difusión de la representación personal (ya sea fotográfica, audiovisual o incluso simulada) sin el consentimiento del titular. Cuando las herramientas de IA generan imágenes sintéticas o deepfakes que simulan identidades reales, lo que está en juego no es solo la privacidad, sino el control sobre la propia representación en el espacio público. Esta forma de simulación constituye una afectación directa al núcleo esencial del derecho a la imagen, particularmente cuando las tecnologías utilizadas escapan del control de la persona afectada (Carrillo, 2007, p. 55–56).

En esta línea de ideas es importante señalar que, si bien herramientas como DALL·E fueron diseñadas para generar imágenes a partir de descripciones textuales, su uso no está exento de potenciales riesgos jurídicos. Aunque OpenAI (desarrollador de DALL·E) ha implementado filtros para evitar la creación directa de imágenes de personas, estos sistemas pueden ser vulnerados. Es decir, es posible generar imágenes lo suficientemente reales que imiten a una persona específica, facilitando así escenarios de suplantación de identidad visual, especialmente cuando se utilizan en conjunto con otras herramientas de edición o clonación facial. En conclusión, el uso de DALL·E y modelos similares puede derivar en la vulneración de varios derechos fundamentales, pese a que su diseño no lo permita de manera directa.

En el contexto normativo ecuatoriano, la imagen facial de una persona, al constituir un dato biométrico que permite su identificación individual, está protegida como dato personal sensible de acuerdo con lo previsto en el artículo 4 y el artículo 25 de la Ley Orgánica de Protección de Datos Personales. Por esta razón, el tratamiento de dicha imagen —ya sea a través de su captura directa o mediante herramientas de generación sintética basadas en inteligencia

artificial— debe someterse a un régimen jurídico riguroso, fundamentado en los principios de licitud, consentimiento informado, proporcionalidad y finalidad.

El empleo de sistemas de IA que permitan crear o manipular rostros humanos sin la autorización del titular contraviene directamente estos principios, sobre todo cuando el contenido generado afecta su honor, su reputación o su capacidad de ejercer el control sobre sus propios datos personales. Esta problemática se agrava en Ecuador ante la ausencia de un marco legal específico que regule la generación artificial de imágenes de carácter personal, lo cual contribuye a un escenario de creciente inseguridad jurídica. A ello se suma la complejidad técnica que implica verificar la autenticidad del contenido, la limitada capacitación institucional sobre el uso de estas tecnologías emergentes, y la escasa jurisprudencia que aborde de manera integral esta forma de afectación a los derechos personalísimos.

La jurisprudencia internacional ha comenzado a abordar este problema. En el caso Lozano Aragón vs. Colombia (Corte IDH, 2021), la Corte Interamericana subrayó que la identidad visual es un elemento constitutivo de la dignidad y que su manipulación puede generar "daños a la honra y reputación aun en ausencia de exposición corporal explícita". Este criterio puede aplicarse, mutatis mutandis, a la alteración de la imagen mediante IA.

En consecuencia, el riesgo jurídico no se limita únicamente al uso no autorizado de una imagen previamente captada, sino que se extiende también a la generación de representaciones visuales o auditivas falsas que se atribuyen a personas reales. Estas simulaciones producidas mediante inteligencia artificial (aunque técnicamente construidas desde cero) no son neutrales desde la perspectiva jurídica, pues constituyen una forma emergente de afectación a los derechos de la personalidad. Su impacto trasciende la esfera patrimonial, ya que el daño que generan suele

revestir una dimensión simbólica y reputacional, comprometiendo de manera directa la dignidad, la identidad y la autonomía informativa del sujeto representado. En este contexto, se vuelve imperativo que el ordenamiento jurídico reconozca la gravedad de estas nuevas formas de vulneración y adopte respuestas normativas específicas orientadas a su prevención, sanción y reparación efectiva en entornos digitales (véase Chesney y Citron, 2019, pp. 1766–1767).

Tecnologías de IA generativas y productos derivados que afectan el derecho a la imagen

En el contexto ecuatoriano, si bien no se han reportado casos emblemáticos como en Estados Unidos o Europa, sí existen antecedentes de manipulación de contenido, extorsión y difusión de material falso con tecnologías de edición digital que hoy podrían potenciarse con IA. A continuación, se resumen las principales tecnologías con mayor riesgo:

Tabla 2

Tecnología con IA	Descripción técnica	Riesgos jurídicos concretos en Ecuador
Generadores de imágenes sintéticas	Modelos como DALL·E y Stable Diffusion que crean rostros o cuerpos hiperrealistas	Suplantación de identidad, difamación, difusión de contenido íntimo sin consentimiento
Generadores de video hiperrealista	Ej. Veo 3 (Google); integra texto, imagen y movimiento en videos falsos	Manipulación de discursos, afectación a honra, chantaje digital

Deepfakes	Integración de imagen, voz y gestualidad para simular escenas inexistentes	Extorsión, fraude, pornografía no consentida (COIP, arts. 178, 179, 180)
Reconocimiento facial y voice cloning	Identificación y clonación sin consentimiento mediante patrones biométricos	Vigilancia masiva, usurpación de identidad (Ley Orgánica de Protección de Datos, arts. 26, 27)
Avatares y chatbots con identidad humana	Simulan conversaciones humanas usando perfiles falsos	Engaño digital, manipulación emocional, fraude en contratación o relaciones sociales

Fuente: elaboración propia

La revisión técnica y jurídica de las herramientas de inteligencia artificial evidencia un fenómeno complejo: su desarrollo ha superado la capacidad de respuesta normativa del sistema jurídico ecuatoriano, especialmente en lo penal, donde **rige el principio de legalidad estricta y la prohibición de analogía in malam partem**. En este marco, aunque la Constitución garantiza de forma expresa el derecho a la imagen (art. 66, num. 18) y a la información veraz, verificada y contextualizada (art. 18), el uso de IA para generar contenidos falsos, manipulados o engañosos **no se encuentra específicamente tipificado ni en el Código Orgánico Integral Penal ni en normas complementarias**, lo que impide accionar mecanismos de protección o sanción directa en estos casos.

Este vacío normativo genera una situación jurídica crítica: **el derecho a la imagen se encuentra formalmente reconocido, pero en una situación de indefensión estructural** frente

al avance tecnológico. Ello no solo vulnera la dignidad individual, sino que afecta también el derecho colectivo a la información veraz y no manipulada, tal como lo establece el artículo 18 de la Constitución, el cual impone la exigencia de veracidad, verificación y contextualización de los contenidos difundidos, así como la responsabilidad ulterior por los daños que esta información pueda generar.

En suma, el sistema legal ecuatoriano se enfrenta a un dilema: o permanece atado a una interpretación formalista y reactiva, que impide actuar ante nuevas formas de afectación, o asume la necesidad de una reforma legal clara y expresa, particularmente en el ámbito penal y de protección de datos, que tipifique con precisión los usos lesivos de herramientas de IA que simulan identidades, vulneran la honra o propagan desinformación. Hasta entonces, el derecho a la imagen permanece jurídicamente vulnerable, sin un régimen efectivo de garantías que responda a los riesgos actuales.

En Ecuador, el marco normativo vigente no ofrece una respuesta del todo adecuada frente a los riesgos emergentes derivados del uso de inteligencia artificial generativa en relación con la imagen personal. Si bien la Ley Orgánica de Protección de Datos Personales (LOPDP), en su artículo 5, reconoce la imagen facial como un dato biométrico (y, por tanto, como un dato personal sensible cuando permite la identificación unívoca del titular), este reconocimiento no viene acompañado de una regulación específica sobre la generación sintética, la manipulación automatizada o la difusión no consentida de imágenes a través de herramientas de IA. Es decir, la ley se enfoca principalmente en el tratamiento tradicional de datos personales ya existentes, sin embargo, no aborda expresamente lo que podría ocurrir cuando esos datos se crean artificialmente mediante algoritmos generativos.

A pesar de ello, es importante considerar que usar imágenes generadas por IA representando a una persona real sin su consentimiento podría considerarse, en sí mismo, un tratamiento de datos sin base legitimadora. En ese sentido, ya existen disposiciones dentro de la LOPDP (como los artículos 7 y 10) que exigen una justificación legal y el consentimiento expreso del titular para cualquier tratamiento de datos personales, incluidos los biométricos. Por tanto, incluso sin una regulación específica sobre IA, estos actos podrían, o no, ser sancionados en la vía administrativa, lo que abre una posible vía de protección. Sin embargo, subsiste una importante inseguridad jurídica, ya que la ausencia de una norma clara y expresa que regule este tipo de tratamientos genera incertidumbre tanto para las víctimas como para los operadores jurídicos a la hora de determinar responsabilidades y activar mecanismos de tutela eficaces.

La inexistencia de una regulación específica sobre el uso de inteligencia artificial para generar imágenes o videos representa un serio vacío legal, especialmente en materia penal. El principio de legalidad exige que las conductas sancionables estén tipificadas, lo que dificulta actuar frente a hechos no previstos, como los contenidos sintéticos. Esta rigidez, aunque necesaria, se convierte en un obstáculo frente a los daños que pueden causar estas tecnologías.

Las imágenes creadas con IA pueden generar afectaciones graves a derechos personalísimos: desde daños morales y afectaciones a la reputación, hasta chantaje o suplantación de identidad. Al no encajar del todo en figuras penales existentes, estas situaciones quedan en una zona gris. Por ejemplo, un video íntimo falso atribuido a una persona real no tiene una tipificación penal clara, por lo que podría intentarse encuadrar en delitos como la difusión no consentida de contenido íntimo (COIP, art. 178), lo que plantea serias dudas jurídicas.

Desde el punto de vista penal, esto es particularmente preocupante porque rige el principio de legalidad estricta (nullum crimen, nulla poena sine lege), consagrado en el artículo 76, numeral 3 de la Constitución ecuatoriana. Esto significa que ningún acto puede considerarse delito ni sancionarse si no está previamente tipificado en una norma clara y expresa. Por tanto, incluso cuando una conducta vulnera gravemente derechos fundamentales, si no hay una norma penal expresa que la sancione, el Estado no puede perseguirla sin vulnerar los derechos del procesado, como el derecho al debido proceso, al juez natural y a la defensa técnica.

En el contexto actual, el derecho a la imagen (como expresión concreta del principio de dignidad humana consagrado en el artículo 66, numeral 18 de la Constitución de la República del Ecuador) se encuentra en una situación de alta vulnerabilidad jurídica. La producción y difusión de contenidos manipulados mediante inteligencia artificial no solo constituyen una afectación directa al derecho a la imagen, sino que también comprometen otros derechos conexos, como la honra, la intimidad, el libre desarrollo de la personalidad y el acceso a información veraz y contextualizada, todos ellos protegidos por el artículo 18 de la Constitución. En ausencia de una regulación específica que aborde estas nuevas formas de vulneración, el ordenamiento jurídico ecuatoriano ha quedado rezagado frente al ritmo acelerado de las transformaciones tecnológicas actuales, lo que favorece la reiteración de daños sin que existan mecanismos adecuados de prevención, sanción o reparación.

Este fenómeno no debe interpretarse únicamente como una carencia normativa o técnica aislada, sino como expresión de una falla estructural más profunda: la falta de capacidad estatal para garantizar el ejercicio efectivo de los derechos fundamentales en entornos digitales. La inexistencia de normas claras que regulen los usos lesivos de la IA generativa, junto con la ausencia de criterios probatorios definidos y de protocolos institucionales de respuesta rápida

frente a la circulación masiva de contenidos falsificados, coloca a las personas en una situación de indefensión tanto jurídica como fáctica. Así, el derecho a la imagen, aunque formalmente reconocido, se encuentra debilitado en su eficacia real.

En este contexto, el riesgo jurídico no se limita al uso no autorizado de imágenes previamente captadas, sino que se amplía a la creación artificial de contenidos visuales o sonoros atribuidos a personas sin base real, pero que resultan creíbles. Estas prácticas no solo amplían el espectro de afectación, sino que configuran un nuevo tipo de conflicto entre el avance acelerado de la tecnología y la vigencia efectiva de los derechos constitucionales. Este desequilibrio exige una reforma normativa urgente, orientada a restablecer la centralidad de la persona frente a la lógica autónoma de los algoritmos. Desde una perspectiva de política pública y de constitucionalismo transformador, este escenario exige una reforma normativa integral que aborde los usos lesivos de la inteligencia artificial con enfoque de derechos, técnica jurídica y sensibilidad social. En consonancia con Boaventura de Sousa Santos, el constitucionalismo en contextos periféricos no puede limitarse a reproducir estructuras formales: debe responder activamente a las injusticias estructurales y adaptarse a desafíos emergentes como los planteados por las tecnologías de IA generativa (Santos, 2009, p. 23).

En concreto, se requiere:

1. **Tipificación penal específica del uso doloso de IA para generar o difundir imágenes falsas** que vulneren la honra, intimidad, reputación o integridad moral de las personas. Esta medida es coherente con el principio de legalidad penal (art. 76.3 CRE) y con el mandato de protección reforzada frente a nuevas formas de violencia simbólica, digital y mediática (Rodríguez-Piñero, 2021). La incorporación de estos delitos debe considerar estándares de

proporcionalidad, dolo específico y mecanismos probatorios digitales adaptadas a entornos de IA.

2. **Diseño de una vía rápida de protección judicial o administrativa,** que permita accionar de manera ágil ante la difusión de imágenes falsas creadas por IA. Esto puede materializarse mediante una acción de protección constitucional especializada en entornos digitales, inspirada en figuras como la tutela efectiva o un habeas data ampliado, con enfoque de reparación integral, retiro de contenido y garantía de no repetición.

En este contexto, resulta indispensable definir con claridad a quién debe imputarse la responsabilidad por la afectación de derechos, considerando que muchas de las plataformas que permiten la generación o difusión de estos contenidos tienen domicilio en el extranjero. Si bien lo ideal sería accionar contra el autor directo de la simulación o contra la plataforma que aloja el contenido, no siempre será posible identificarlo o tener acceso jurisdiccional sobre él. Por ello, el Estado debe evaluar mecanismos de respuesta excepcionales, como el bloqueo temporal de acceso a ciertos servicios digitales dentro del territorio nacional, no como una medida autoritaria o de censura, sino como una forma de defensa legítima de la soberanía digital y de los derechos de sus ciudadanos, siguiendo precedentes adoptados por otras jurisdicciones. Este tipo de decisiones deben implementarse bajo criterios de proporcionalidad, necesidad y temporalidad, asegurando que no se afecte injustificadamente la libertad de información, pero sí se garantice una protección efectiva de derechos fundamentales vulnerados mediante tecnologías emergentes.

3. **Incorporación de un enfoque preventivo y educativo**, dirigido a promover la alfabetización digital crítica, el conocimiento sobre los derechos digitales, la ética tecnológica y el funcionamiento de las herramientas de IA. Esta estrategia debe tener un enfoque interseccional, dado que jóvenes, mujeres, personas racializadas o de diversidad sexo genérica

suelen ser los grupos más afectados por la manipulación de imágenes y contenidos digitales (ONU Mujeres, 2023). La educación jurídica, tecnológica y mediática constituye, en este sentido, una herramienta de emancipación y contención frente a la violencia simbólica automatizada.

Esta triple respuesta no solo es necesaria desde una perspectiva técnico normativa, sino también desde la garantía del principio de progresividad en materia de derechos, consagrado en el artículo 11 numeral 8 de la Constitución ecuatoriana. No adaptar el orden jurídico a los nuevos mecanismos de daño es, en sí mismo, una forma de regresividad institucional frente a la expansión de los riesgos digitales.

Generadores de imágenes sintéticas

En los últimos años, el desarrollo de herramientas generativas basadas en inteligencia artificial ha transformado radicalmente la producción de contenido visual. Los generadores de imágenes sintéticas permiten crear representaciones fotográficas hiperrealistas de personas, objetos o escenarios a partir de descripciones textuales, sin requerir material visual de partida. Esta capacidad, potenciada por modelos como DALL·E (OpenAI), Stable Diffusion (Stability AI) o el sistema de video Veo 3 (Google DeepMind), ha democratizado el acceso a herramientas creativas, pero también ha desencadenado una ola de preocupaciones jurídicas, éticas y sociales a nivel global (Qu, Y., et al., 2023; DeepMind, 2025).

Una característica central de estos modelos es su capacidad para producir identidades visuales completamente nuevas, como rostros inexistentes o en su forma más problemática, simulaciones de rostros de personas reales sin consentimiento. En muchos casos, las imágenes generadas por inteligencia artificial alcanzan tal grado de realismo que se vuelven casi

indistinguibles de fotografías auténticas. Esta característica plantea desafíos normativos inéditos en materia de regulación del contenido visual digital. A diferencia de las imágenes obtenidas por medios físicos tradicionales —captadas por dispositivos que registran la realidad—, las representaciones creadas mediante algoritmos no siempre se ajustan a las categorías jurídicas convencionales. Esta dificultad es aún mayor cuando dichas imágenes no provienen de una fotografía base, sino que son el resultado de procesos computacionales autónomos (Koch & Padovani, 2023). La carencia de una clasificación jurídica clara para estas nuevas formas de representación visual debilita la eficacia de las normas vigentes y evidencia la necesidad de revisar críticamente el marco legal aplicable, a fin de responder a los desafíos específicos que plantea la creación de contenido visual sintético.

Desde una perspectiva ética y filosófica del derecho, el problema radica en el estatus ambiguo de lo que se presenta como real sin serlo. Estas imágenes pueden insertarse en contextos lesivos (chismes, extorsiones, campañas de odio, sátiras malintencionadas o contenido sexual) y en muchos casos los daños ocurren antes de que la víctima pueda reaccionar o demostrar que el contenido es falso. A diferencia de la sátira o la parodia tradicional, que operan dentro de convenciones culturales claramente reconocibles, el uso de IA puede borrar toda señal de artificio, convirtiéndose en una forma tecnológicamente asistida de engaño reputacional (Zuboff, 2019).

En el caso ecuatoriano, la complejidad de esta problemática se ve acentuada por la falta de criterios jurisprudenciales y doctrinales consolidados que permitan distinguir con claridad entre una imagen auténtica, una alterada y una generada íntegramente por medios digitales. Esta indefinición normativa obstaculiza tanto la identificación de los supuestos jurídicos aplicables como la configuración de mecanismos efectivos de tutela. Aunque hasta la fecha no se han

documentado públicamente casos emblemáticos que hayan escalado al debate judicial o mediático, debe considerarse que las tecnologías de generación de contenido visual mediante inteligencia artificial son ampliamente accesibles desde cualquier dispositivo conectado a internet. Esta disponibilidad masiva incrementa de forma sostenida el riesgo de que dichas herramientas sean empleadas en contextos sensibles (como redes sociales, procesos electorales o disputas interpersonales) generando afectaciones a la imagen personal, la honra o la reputación, sin un marco claro de contención jurídica. Situación que puede desembocar en vulneraciones sobre todo al derecho a la imagen y la honra de las personas.

Para ilustrar esta vulnerabilidad, se puede imaginar un escenario verosímil a manera de ejemplo: un actor político local es víctima de un montaje visual en el que aparece en un contexto íntimo o comprometedor y el contenido es difundido viralmente en redes. Aunque no existe una grabación original, ni se trata de una fotografía manipulada, la imagen generada mediante IA resulta es tan realista que produce efectos concretos en su carrera, honra y vida familiar. En este escenario, la víctima no tiene certeza de si está protegida por el derecho a la imagen o si debe recurrir a acciones por difamación, daño moral o protección de datos personales, con resultados inciertos dada la inexistencia de normas o precedentes aplicables al caso y a la percepción subjetiva de las autoridades judiciales.

Este tipo de afectaciones no necesariamente se limitan a figuras públicas. Mujeres jóvenes, estudiantes, docentes, activistas, personas LGBTI+ o incluso funcionarios de bajo perfil pueden ser objeto de falsificaciones visuales difundidas por terceros, muchas veces con fines de intimidación, acoso o burla. El riesgo está ligado no solo a la sofisticación de la tecnología, sino a su banalización, es decir, al hecho de que herramientas altamente poderosas estén hoy disponibles en interfaces amigables, gratuitas y sin control ético (Zhang, et al, 2022).

Por ello, más que una respuesta puramente normativa, se necesita una reconfiguración del sistema jurídico para identificar y sancionar la instrumentalización de lo ficticio como herramienta de daño reputacional. Esta discusión, apenas incipiente en el Ecuador, debe nutrirse de los debates internacionales sobre derechos digitales, manipulación algorítmica y daño simbólico, integrando una perspectiva crítica sobre los límites de la creatividad, la libertad de expresión y la responsabilidad tecnológica.

La influencia de la inteligencia artificial en la generación de contenido falso, su impacto en los derechos de imagen y su uso en conflictos geopolíticos y propaganda política

La capacidad de la inteligencia artificial (IA) para generar contenido visual y de audio hiperrealista representa uno de los principales desafíos actuales para la protección de los derechos de imagen y para el ejercicio democrático del derecho a la información. El empleo de herramientas generativas como DALL·E, Stable Diffusion o Veo 3 ha permitido crear imágenes y videos con un alto grado de verosimilitud, dando lugar a un entorno inédito de riesgo jurídico y comunicacional. Estas tecnologías, que inicialmente fueron desarrolladas con fines creativos, han sido utilizadas para producir contenidos conocidos como deepfakes: simulaciones audiovisuales que reproducen rostros y voces de personas reales en contextos falsos, sin contar con su autorización y con un elevado potencial lesivo. En este escenario, se observa un desdibujo de la frontera entre realidad y realidad virtual, que amenaza el derecho a la imagen (entendido como el control individual sobre la representación visual de la propia persona) y afecta, por extensión, al derecho colectivo a la información veraz, contextualizada y verificada, garantizado en el artículo 18 de la Constitución de la República del Ecuador (CRE, 2008).

Un ejemplo ilustrativo de los riesgos que plantea la circulación de contenido sintético es el caso del video viral que mostraba, de forma aparentemente inofensiva, a un canguro abordando un avión en calidad de animal de soporte emocional. Este material, completamente generado mediante inteligencia artificial y difundido inicialmente a través de la cuenta @infiniteunreality, logró engañar a miles de usuarios, incluidos periodistas y medios digitales, antes de que su falsedad fuera confirmada públicamente (Univision, 2025). Aunque no implicaba la representación de personas reales ni ocasionó un daño directo, el caso revela con claridad el enorme potencial de estos contenidos para activar reacciones emocionales, generar narrativas virales y consolidarse como "hechos" en la esfera pública, pese a carecer de toda veracidad. El caso evidencia que la inteligencia artificial generativa puede tener un impacto significativo en la opinión pública, incluso cuando no se utiliza con intención maliciosa. Esta capacidad de influir en la percepción colectiva se vuelve especialmente grave cuando se vincula con la imagen o identidad de personas reales. Si las mismas tecnologías se emplean para simular el rostro o la voz de figuras públicas, las consecuencias podrían ser graves, tanto a nivel reputacional como institucional.

En conflictos internacionales recientes, esta tecnología ha sido utilizada con fines estratégicos. En marzo de 2022, durante la guerra en Ucrania, se difundió un video que mostraba al presidente Volodímir Zelenski pidiendo a sus tropas que depusieran las armas. Aunque rápidamente fue desmentido por las autoridades ucranianas y medios internacionales, su efecto inicial generó desinformación e incertidumbre (EU Parliament, 2023). La Organización del Tratado del Atlántico Norte (OTAN) ha identificado esta modalidad como parte de las tácticas de guerra híbrida, en la que las operaciones informativas se integran con tecnologías de IA para debilitar la cohesión social de los Estados democráticos (NATO, 2022). De igual manera, en

Taiwán y Hong Kong se han documentado campañas de manipulación mediante IA que simulan líderes políticos locales, contribuyendo a desestabilizar procesos electorales, generar pánico y manipular la opinión pública (Bradshaw y Howard, 2023).

Este tipo de prácticas no se limita al escenario internacional. En América Latina, si bien los casos documentados aún son escasos, los riesgos son tangibles. La creciente disponibilidad de herramientas generativas, la falta de regulación específica y la polarización política crean condiciones propicias para que los deepfakes se utilicen como armas de desinformación en campañas electorales, conflictos judiciales o disputas mediáticas. En Ecuador, donde las redes sociales juegan un papel creciente en la construcción de opinión pública y donde las instituciones aún carecen de pericia técnica para identificar contenido sintético, el uso de IA con fines lesivos representa una amenaza real al derecho a la imagen y al funcionamiento de la esfera pública democrática.

Desde el punto de vista normativo, la situación es alarmante, aunque la Constitución garantiza el derecho a la imagen (art. 66, num. 18) y a la información veraz (art. 18), y a pesar de que la Ley Orgánica de Protección de Datos Personales reconoce la imagen como dato biométrico (art. 5.11), ninguna disposición legal regula de forma expresa la creación o difusión de contenido falso generado por inteligencia artificial. La omisión normativa resulta incompatible con el principio de progresividad de los derechos y deja a las personas expuestas a afectaciones no reparables. En el ámbito penal, la situación es aún más crítica: el principio de legalidad estricta (art. 76.3 CRE) impide sancionar estas conductas si no han sido tipificadas previamente, lo que significa que incluso la creación de un deepfake íntimo o difamatorio (por más lesivo que sea) no podría ser objeto de persecución penal directa sin violar los derechos del procesado.

Además, esta tecnología plantea una amenaza estructural al derecho colectivo a la información. Tal como ha advertido el congreso de la Unión Europea, la capacidad de los deepfakes para generar dudas sobre cualquier registro audiovisual (incluso los verdaderos) produce una erosión del principio de prueba visual y alimenta el cinismo informativo (EU Parliament, 2023). Este fenómeno, conocido como "efecto liar's dividend", implica que la existencia de contenido falso hace que incluso los contenidos auténticos sean puestos en duda, debilitando la confianza ciudadana en la información (Chesney y Citron, 2019). Si no se establece una regulación adecuada, el uso de contenidos sintéticos generados por inteligencia artificial podría poner en riesgo pilares fundamentales del orden democrático, en especial aquellos vinculados con la administración de justicia y la deliberación pública basada en hechos comprobables. La posibilidad de construir narrativas ficticias que aparentan veracidad contribuye a borrar la línea entre verdad y falsedad, con consecuencias que afectan tanto a los derechos individuales como a la estabilidad del sistema democrático en su conjunto.

Frente a este escenario, el Estado ecuatoriano enfrenta un reto normativo ineludible. Es necesario avanzar hacia una legislación especializada que tipifique expresamente la producción dolosa de contenidos sintéticos con fines lesivos, en particular aquellos que afecten la imagen, el honor o la reputación de las personas. Además, se requiere desarrollar mecanismos probatorios digitales y herramientas forenses que permitan verificar la autenticidad de los archivos audiovisuales generados por IA. Esta respuesta normativa debe complementarse con la habilitación de vías judiciales expeditas (como acciones de protección adaptadas al entorno digital) que permitan reaccionar con celeridad frente a la circulación de contenidos perjudiciales, garantizando así una tutela efectiva del derecho a la imagen frente a los riesgos emergentes de la era algorítmica. Al mismo tiempo, deben implementarse políticas públicas de alfabetización

digital con sentido crítico, con enfoque interseccional, para que las personas puedan reconocer, cuestionar y actuar frente al uso engañoso de contenidos generados por IA.

En síntesis, la inteligencia artificial no solo ha transformado la forma en que se produce contenido, sino que ha modificado el terreno en el que se disputan el poder simbólico, la identidad pública y la verdad política. En este nuevo campo de batalla, el derecho a la imagen (como manifestación de la dignidad, la autonomía informativa y la reputación personal) debe ser resguardado con herramientas jurídicas que estén a la altura de los riesgos que plantea el presente. Además, considerar la efectividad de respuesta en el aparato estatal con políticas públicas y mecanismos institucionales que permitan el pleno goce de derechos y de reparación de estos.

Usos lesivos de las herramientas de IA en el contexto ecuatoriano

La rápida expansión de las tecnologías basadas en inteligencia artificial ha desafiado de forma directa la capacidad de los marcos normativos tradicionales para garantizar la protección efectiva de los derechos fundamentales. Uno de los más expuestos en este nuevo escenario es el derecho a la imagen, concebido como una manifestación de la autodeterminación personal en relación con la representación visual y audiovisual del cuerpo propio. Las herramientas de IA hoy disponibles permiten generar imágenes hiperrealistas, alterar rasgos faciales, replicar gestos o voces, y construir montajes que simulan ser registros auténticos, desdibujando la frontera entre lo real y lo fabricado. Este nuevo tipo de amenaza (de carácter estructural, algorítmico e invisible) adquiere una dimensión especialmente crítica en contextos como el ecuatoriano, donde la vigencia de los derechos se ve limitada por factores estructurales como la fragmentación institucional, la precariedad tecnológica del aparato estatal y la escasa articulación entre el

sistema judicial y las transformaciones propias del entorno digital. En consecuencia, la discusión sobre los usos lesivos de la inteligencia artificial no puede abordarse como un problema exclusivamente teórico o comparado, sino como una expresión concreta de nuevas formas de violencia simbólica que ya están operando en la práctica, muchas veces con absoluta impunidad.

Una de las manifestaciones más preocupantes de este fenómeno en el contexto ecuatoriano es el uso creciente de deepfakes con fines fraudulentos. Estas falsificaciones audiovisuales, generadas mediante redes neuronales, permiten suplantar la voz o el rostro de una persona con tal nivel de realismo que resulta difícil distinguirlas del contenido auténtico. En el ámbito nacional, se han documentado casos en los que figuras públicas —como comunicadores, profesionales de la salud o personas con visibilidad en redes— han sido reproducidas digitalmente para promocionar falsas oportunidades laborales, modelos de inversión inexistentes o esquemas fraudulentos que se presentan como propuestas tecnológicas.

En estos escenarios, la manipulación de la imagen de personas con credibilidad social funciona como herramienta de captación de víctimas, explotando su reputación con fines engañosos. Este tipo de prácticas no solo atentan contra derechos personalísimos, sino que también agravan desigualdades estructurales, pues suelen dirigirse a poblaciones económicamente vulnerables. La falta de regulación específica sobre estas conductas, sumada a la lentitud del sistema judicial para atender delitos tecnológicos, ha propiciado un entorno de impunidad (Fontaine, et al, 2016).

Más allá del fraude económico, uno de los impactos más alarmantes de estas tecnologías es su uso en la producción y difusión de material sexual falso. La aplicación de inteligencia artificial para crear imágenes íntimas de personas sin su consentimiento configura una nueva

forma de violencia digital. En particular, mujeres, adolescentes y personas de identidades sexo-genéricas disidentes han sido blanco frecuente de este tipo de agresiones, que suelen utilizar imágenes extraídas de redes sociales o fotografías personales y las transforman en contenido sexual explícito sin autorización alguna.

Estas simulaciones, que pueden incluir escenas gráficas con apariencia realista, circulan con facilidad en canales digitales y plataformas pornográficas, generando daños profundos a la integridad, la privacidad y la dignidad de las víctimas. En la mayoría de los casos, las personas afectadas enfrentan obstáculos para acceder a mecanismos eficaces de protección y reparación. En una sociedad todavía estructurada en torno a lógicas patriarcales (donde la honra, el cuerpo y la imagen de las mujeres y disidencias continúan siendo objeto de vigilancia social), la publicación de este tipo de contenido puede provocar consecuencias devastadoras: ruptura de vínculos familiares, pérdida del empleo, estigmatización, aislamiento social o incluso pensamientos suicidas. Este fenómeno constituye una forma contemporánea de violencia sexual simbólica, mediada por tecnologías digitales, frente a la cual el ordenamiento jurídico ecuatoriano aún ofrece una respuesta limitada. Aunque el artículo 176.3 del Código Orgánico Integral Penal sanciona la difusión no consentida de contenido íntimo, la norma vigente no contempla de forma expresa la creación artificial de imágenes ni la suplantación algorítmica como agravantes específicas de esta conducta, lo que evidencia una respuesta normativa aún insuficiente por parte del ordenamiento jurídico ecuatoriano.

Por otra parte, preocupa especialmente el uso político de estas tecnologías de manipulación visual. En los últimos años, el Ecuador ha presenciado un aumento en las campañas de desinformación, sobre todo en contextos electorales o de alta tensión social. En estos casos se han utilizado imágenes falsificadas, audios alterados y videos manipulados con el

fin de afectar la reputación de candidatos, difundir rumores o influir de manera ilegítima en la formación de opinión pública. En un entorno institucional débil, con escasos mecanismos de verificación, la circulación de estos contenidos compromete directamente la calidad del debate democrático y la confianza ciudadana en el proceso electoral. Como ha advertido la Corte Interamericana de Derechos Humanos en su Opinión Consultiva OC-24/17, la difusión masiva de noticias falsas y contenidos manipulados puede vulnerar el derecho a la información veraz y constituir una forma de violencia simbólica con impactos colectivos, especialmente cuando va dirigida a grupos históricamente marginados como los pueblos indígenas, las mujeres o los sectores rurales.

Este panorama se agrava por la ineficacia estructural del sistema judicial ecuatoriano para brindar protección, reparación y garantías de no repetición. La Corte Constitucional ha reconocido en múltiples fallos la existencia de un "déficit estructural de cumplimiento de derechos", señalando que la sola consagración normativa de garantías no es suficiente si no se articulan mecanismos accesibles, eficaces y adecuados para su exigibilidad (Sentencia No. 198-17-SEP-CC). Esto se refleja, por ejemplo, en la escasa capacitación del personal judicial sobre delitos digitales, la inexistencia de peritos especializados en análisis de imágenes generadas por IA, y la lentitud en la emisión de medidas cautelares. En este escenario, los daños ocasionados por montajes digitales, suplantaciones de identidad y formas de chantaje mediante inteligencia artificial no cuentan con una respuesta institucional efectiva, lo que favorece la reproducción de la impunidad y perpetúa dinámicas de exclusión estructural. Las consecuencias de esta inacción afectan de manera especialmente aguda a grupos históricamente marginados, como mujeres, jóvenes, pueblos indígenas y personas en situación de pobreza, quienes enfrentan mayores barreras para acceder a mecanismos de protección y reparación.

Ante esta problemática, se vuelve imperativo diseñar un marco normativo específico sobre inteligencia artificial que incorpore un enfoque transversal de derechos humanos, perspectiva de género e interseccionalidad. Esta legislación no solo debería prohibir de manera explícita los usos lesivos de tecnologías algorítmicas, sino también imponer obligaciones concretas de diligencia a los desarrolladores, plataformas tecnológicas y entidades públicas. Además, debe contemplar mecanismos de trazabilidad algorítmica que permitan atribuir responsabilidades en caso de afectaciones, y establecer procedimientos de reparación que sean eficaces, ágiles y proporcionales al daño sufrido. Tal como lo ha planteado Luigi Ferrajoli, la vigencia sustantiva de los derechos fundamentales no se garantiza únicamente con su reconocimiento formal, sino con la existencia de garantías secundarias que aseguren su cumplimiento mediante normas operativas, procedimientos efectivos y estructuras institucionales capacitadas para responder frente a su vulneración. En contextos como el ecuatoriano, donde los derechos suelen proclamarse más de lo que se hacen cumplir, el diseño de estas garantías debe ser radicalmente democratizante, orientado a revertir las históricas relaciones de exclusión y violencia estructural (Pisarello, 2001).

Ahora bien, para que esta legislación sea realmente efectiva frente a actores transnacionales (como los desarrolladores de plataformas de IA con sede fuera del país) el Estado debe contemplar mecanismos complementarios de carácter administrativo, judicial o incluso tecnológico que garanticen la protección real de los derechos de las personas en el territorio. Entre estos mecanismos podrían incluirse desde procesos de notificación y retiro de contenidos hasta sanciones proporcionales, incluyendo restricciones de acceso o responsabilidades subsidiarias frente a proveedores locales. Si bien estas medidas pueden encontrar límites en el derecho internacional y en la arquitectura descentralizada de internet, su sola previsión

normativa refuerza la soberanía jurídica del país y sienta las bases para exigir mayor corresponsabilidad global en la protección de derechos fundamentales.

La imagen como dato biométrico y su tratamiento en la legislación ecuatoriana

La imagen de una persona, más allá de su función representativa o estética, constituye un dato biométrico sensible en la medida en que permite la identificación unívoca del individuo. En el marco del derecho ecuatoriano, esta consideración se encuentra recogida expresamente en la Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021, que establece que los datos biométricos (como la imagen facial, la voz o las huellas dactilares) deben ser objeto de un tratamiento diferenciado, dotado de mayores salvaguardas, por cuanto su uso indebido puede afectar directamente la intimidad, la seguridad y la autonomía de los titulares.

El artículo 24 de la Ley Orgánica de Protección de Datos Personales establece que la imagen de una persona constituye un dato personal sensible, lo que implica un régimen reforzado de protección en su tratamiento. En consecuencia, cualquier uso de la imagen requiere el consentimiento expreso del titular, el cual debe ser libre, informado, específico e inequívoco. Asimismo, se exige la adopción de medidas técnicas y organizativas que garanticen la seguridad de dicho dato.

Esta clasificación no tiene un carácter meramente formal, sino que conlleva efectos jurídicos relevantes: la imagen no puede ser captada, almacenada ni utilizada con fines publicitarios, comerciales o estadísticos sin autorización expresa. El uso no autorizado puede generar sanciones administrativas, así como responsabilidad civil o penal, en función de la gravedad del perjuicio causado. Este marco legal ecuatoriano se encuentra alineado con estándares internacionales, como el Reglamento General de Protección de Datos (RGPD) de la

Unión Europea, que también reconoce la imagen como dato sensible sujeto a los principios de minimización, proporcionalidad y finalidad legítima.

No obstante, el marco normativo ecuatoriano presenta una importante limitación: no contempla explícitamente los desafíos asociados al tratamiento automatizado, manipulación algorítmica o generación sintética de imágenes mediante herramientas de inteligencia artificial. El desarrollo acelerado de herramientas como los deepfakes ha alcanzado tal nivel de sofisticación que permite generar representaciones visuales falsas con alto grado de realismo, desafiando los estándares tradicionales de identificación, reconocimiento y verificación facial. Esta capacidad representa una amenaza creciente para el derecho a la imagen, especialmente en contextos como el ecuatoriano, donde aún persisten vacíos legales, limitaciones técnicas y una institucionalidad débil en esta materia.

Frente a esta situación, se vuelve indispensable plantear una reforma específica a la Ley Orgánica de Protección de Datos Personales (LOPDP) que regule el tratamiento de contenidos generados mediante inteligencia artificial. Esta reforma debería contemplar al menos los siguientes aspectos esenciales: (i) La incorporación de una definición jurídica de imagen sintética o generada algorítmicamente, entendiéndola como toda representación visual manipulada que simule la apariencia de una persona real. (ii) La prohibición expresa del tratamiento de datos personales mediante IA sin el consentimiento previo, libre, informado y expreso del titular, cuando dicho tratamiento tenga por objeto recrear, manipular o simular la imagen de la persona, salvo en los casos establecidos por la ley, como investigaciones científicas o fines periodísticos justificados. (iii) El establecimiento de una presunción legal de vulneración a la honra o dignidad cuando se difundan representaciones sintéticas que impliquen escenas íntimas o comprometedoras sin autorización, invirtiendo en tales casos la carga probatoria a favor de la

víctima. (iv) La imposición de un deber de trazabilidad algorítmica a proveedores y usuarios de herramientas de IA en el Ecuador, que obligue a documentar los procesos técnicos empleados en la generación de contenido visual vinculado a personas reales, permitiendo su posterior auditoría y control. Esta propuesta normativa no solo permitiría cubrir un vacío legal existente, sino que también reforzaría la seguridad jurídica y el respeto al derecho a una vida libre de violencia digital, en particular frente a nuevas formas de agresión simbólica como la manipulación visual no consentida.

Actualizar el marco normativo en esta dirección no solo resulta oportuno, sino urgente, dado que permitiría alinear el régimen de protección de datos personales con los desafíos que plantea la inteligencia artificial. Asimismo, dotaría a las autoridades de mejores herramientas legales para prevenir y sancionar prácticas abusivas, fortaleciendo las vías de reparación frente a las afectaciones derivadas del uso indebido de tecnologías algorítmicas. Con ello, se garantizaría un mayor control público y se consolidaría el rol del Estado como garante de los derechos fundamentales en entornos digitales.

La imagen como extensión de la dignidad humana

La dignidad humana constituye el fundamento ontológico y normativo de todo el sistema de derechos fundamentales. En el marco del constitucionalismo contemporáneo, este principio no se reduce a una simple afirmación simbólica, sino que actúa como eje estructural que orienta la interpretación jurídica, el diseño de políticas públicas y los límites del poder estatal.

En el caso ecuatoriano, la Constitución de 2008 consagra en su artículo 10 que todas las personas son titulares de derechos “por el hecho de existir”, destacando así su carácter inherente, inalienable e irrenunciable. Esta disposición obliga al Estado a garantizar el respeto, la

protección y la realización efectiva de la dignidad en todos los ámbitos de la vida social, incluidos aquellos mediados por tecnologías digitales emergentes.

Desde esta visión, la imagen personal no debe entenderse únicamente como un dato biométrico o una representación del cuerpo físico, sino como una expresión simbólica de la dignidad del individuo. Cada persona tiene derecho a decidir cómo se representa públicamente su imagen, ya que ello incide directamente en su identidad social, su valoración por parte del entorno y su equilibrio emocional. El uso no autorizado o el manejo inadecuado de imágenes personales —en particular cuando intervienen herramientas de manipulación digital como la inteligencia artificial— puede generar procesos de despersonalización que afectan aspectos esenciales del reconocimiento social y subjetivo del individuo. Cuando este tipo de exposición tiene como finalidad humillar, estigmatizar o ridiculizar sin consentimiento, se configura una forma de violencia simbólica con impactos reales: desde el aislamiento social o la pérdida de relaciones familiares, hasta consecuencias psicológicas de severa gravedad.

La violencia digital ejercida a través de herramientas de IA que manipulan imágenes no representa una simple extensión de la difamación tradicional. Más bien, configura una modalidad contemporánea de agresión sistémica, que impacta de forma directa en la autonomía corporal, la capacidad de autodeterminación simbólica y la integridad psíquica de las personas. Esta forma de violencia adquiere particular gravedad cuando se dirige contra mujeres, niñas o personas con identidades sexo-genéricas diversas, ya que reproduce estructuras de opresión históricas mediante nuevas tecnologías que potencian la exposición, la cosificación y la humillación pública de los cuerpos sin consentimiento. Este tipo de afectaciones requiere una respuesta jurídica que no solo reconozca su gravedad, sino que también comprenda su naturaleza estructural y simbólica. La violencia derivada del uso indebido de tecnologías digitales, como la

inteligencia artificial, demanda la implementación de medidas integrales orientadas a la prevención, la reparación efectiva del daño y la garantía de no repetición. No basta con mecanismos reparatorios individuales, sino que es indispensable que las respuestas jurídicas estén alineadas con los patrones socioculturales que permiten y perpetúan estas nuevas formas de agresión simbólica y digital.

Un ejemplo paradigmático de esta problemática es el caso de la influencer mexicana Alana Flores, ocurrido en mayo de 2025. En ese contexto, se difundió masivamente una imagen de carácter íntimo, fabricada mediante inteligencia artificial, en la que se la representaba en una situación sexual simulada, atribuida falsamente a material real. La víctima negó categóricamente la autenticidad del contenido y anunció el inicio de acciones legales contra el presunto autor, a quien logró identificar. Asimismo, denunció la manipulación de una entrevista previa, en la que se le asignaron declaraciones tergiversadas con fines sensacionalistas. Según reportes de medios como El Imparcial y MVS Noticias, estos hechos le generaron una afectación emocional de alta severidad, que requirió atención médica psiquiátrica debido a episodios de ansiedad, insomnio, angustia persistente y pensamientos intrusivos vinculados al acoso digital y a la exposición pública no consentida.

Este tipo de agresiones digitales revela la insuficiencia de los marcos normativos tradicionales para abordar nuevas formas de violencia simbólica y mediática. Aunque algunos países han comenzado a tipificar el uso de tecnologías de IA con fines difamatorios o sexuales no consensuados (como ocurre con las propuestas legislativas sobre "pornografía sintética" en Estados Unidos o los proyectos sobre “deepfake revenge porn” en Europa) en América Latina, y particularmente en Ecuador, el derecho aún opera con categorías dogmáticas desfasadas frente a las complejidades de la manipulación algorítmica. Aunque algunos países han comenzado a

tipificar el uso de tecnologías de IA con fines difamatorios o sexuales no consentidos —como ocurre con las propuestas sobre "pornografía sintética" en Estados Unidos o "deepfake revenge porn" en Europa—, en América Latina, y particularmente en Ecuador, el derecho aún opera con categorías tradicionales que resultan insuficientes frente a los retos que plantea la manipulación algorítmica de la imagen.

En este contexto, es urgente reconocer que la vulneración de la imagen personal mediante tecnologías de IA puede constituir una forma directa de atentado contra la dignidad humana. Por su propia naturaleza, esta afectación no solo requiere medidas de protección inmediata, sino también mecanismos para garantizar una reparación integral que contemple el daño simbólico, emocional y reputacional causado. Asimismo, en presencia de agravantes —como el dolo, la discriminación o la reiteración de la conducta—, debería aplicarse un régimen sancionatorio más severo, proporcional a la gravedad del hecho.

Desde una visión garantista, influenciada por el pensamiento de Luigi Ferrajoli, la dignidad humana no debe entenderse como una idea abstracta, sino como un límite normativo que impide toda forma de instrumentalización o cosificación del sujeto. En este marco, el derecho debe funcionar como una barrera frente a cualquier intervención que, mediante tecnologías como la inteligencia artificial, convierta a la persona en un objeto manipulable, desconociendo su calidad de sujeto titular de derechos.

Cuando una imagen es manipulada para ridiculizar, exponer o caricaturizar a una persona —como ocurre en los casos de deepfakes sexuales o montajes ideológicos—, se lesiona simbólicamente su condición de sujeto, lo que justifica la intervención prioritaria del derecho.

Por tanto, el derecho a la protección de datos o a la integridad emocional no puede analizarse de forma aislada: deben comprenderse como expresiones concretas del respeto a la dignidad relacional del individuo, que no debe ser transformado en una figura burlada o despojada de su propia imagen.

En conclusión, el reconocimiento normativo de la imagen como extensión de la dignidad humana impone al Estado ecuatoriano una serie de obligaciones reforzadas: actualizar su legislación penal, civil y administrativa para incorporar la dimensión digital del daño simbólico; establecer protocolos de atención psicosocial a víctimas de violencia digital; y fomentar una cultura de respeto a la representación ajena, especialmente en contextos de redes sociales y plataformas algorítmicas. Solo así será posible garantizar, de forma coherente y eficaz, que la dignidad humana (piedra angular del Estado constitucional de derechos y justicia) no quede al arbitrio de la desinformación automatizada ni del escarnio viral.

La imagen como bien jurídico protegido en el entorno digital

La imagen personal constituye no solo una proyección del yo individual, sino un bien jurídico autónomo cuya protección debe ser reforzada frente a los riesgos propios del entorno digital. En este ámbito, la facilidad con la que pueden generarse y difundirse representaciones hiperrealistas (mediante inteligencia artificial generativa como los deepfakes) ha inaugurado una nueva categoría de amenazas para el derecho a la imagen, la privacidad y la honra. En Ecuador, si bien la imagen ha sido reconocida como un dato personal sensible conforme al artículo 24 de la Ley Orgánica de Protección de Datos Personales y registrada oficialmente en el Suplemento del Registro Oficial No. 459 del 26 de mayo de 2021, el marco jurídico vigente no ha desarrollado aún una regulación penal específica sobre la creación o el uso de contenido sintético

generado mediante inteligencia artificial con fines difamatorios o lesivos. Esta omisión normativa resulta especialmente preocupante en el contexto actual, caracterizado por el uso cada vez más frecuente y sofisticado de técnicas algorítmicas para manipular contenidos audiovisuales.

La ausencia de una figura penal expresa que sancione conductas como la suplantación o difusión de material falso generado por IA debilita el principio de legalidad penal y deja a las víctimas en una situación de desprotección. Además, coloca en evidencia la falta de mecanismos normativos que garanticen el acceso a una tutela judicial eficaz. En este sentido, el Comité Jurídico Interamericano ha señalado la urgencia de actualizar los marcos legales nacionales para incluir principios como la trazabilidad algorítmica, la responsabilidad de las plataformas digitales y la garantía del derecho a no ser desinformado.

Un caso emblemático que ilustra esta problemática en el contexto ecuatoriano es el de Leidy Álvarez, conocida como “La Chonera Bonita”, quien en 2025 fue presuntamente víctima de la difusión de un video íntimo falso, generado mediante técnicas de deepfake. A pesar de las denuncias presentadas ante la Fiscalía y de la existencia de indicios técnicos, el caso no registró avances procesales significativos ni se logró identificar a los responsables. Este caso evidencia un doble vacío por parte del Estado: por un lado, la ausencia de normas penales que tipifiquen con claridad este tipo de agresiones; por otro, la ineficacia institucional para investigarlas y sancionarlas. Ante este escenario, resulta prioritario impulsar una reforma legislativa que contemple, al menos, tres elementos fundamentales: (i) La tipificación penal expresa de la creación y difusión de contenidos falsos mediante IA cuando afecten derechos personalísimos; (ii) La adopción de medidas cautelares urgentes para impedir la reproducción de este tipo de

contenidos; y (iii) La implementación de acciones administrativas y judiciales que obliguen a plataformas tecnológicas a colaborar con las autoridades en la identificación de responsables.

La imagen, como bien jurídico, debe ser protegida no solo en su dimensión patrimonial, sino principalmente en su función simbólica, relacional y comunicativa, íntimamente vinculada con la dignidad humana, la honra y la autonomía personal. En el entorno digital contemporáneo, donde las tecnologías de generación sintética permiten alterar con alta fidelidad la apariencia de una persona, el derecho a la imagen adquiere una complejidad inédita. Su vulneración no solo puede ocasionar daños reputacionales, sino también provocar formas de violencia simbólica, discriminación estructural y afectaciones psicoemocionales graves que requieren una respuesta jurídica integral y efectiva. Este contexto exige una respuesta normativa que reconozca el carácter vulnerable de la identidad visual digital y garantice su tutela efectiva ante agresiones algorítmicas invisibles y transnacionales.

Debates éticos y de derechos humanos

El uso de tecnologías de reconocimiento facial y de vigilancia automatizada plantea importantes desafíos éticos y jurídicos que no deben evaluarse únicamente desde la perspectiva de la eficiencia o la seguridad pública. Estas herramientas, al implicar la captura, procesamiento y análisis de datos biométricos, pueden operar sin el consentimiento libre e informado de las personas, ni control independiente sobre su uso, lo que entra en tensión con los principios de legalidad, necesidad, proporcionalidad y respeto a la privacidad.

Aunque en Ecuador la Ley Orgánica de Protección de Datos Personales reconoce la imagen facial como dato biométrico sensible, actualmente no existe una norma específica que regule la aplicación de sistemas de reconocimiento facial en espacios públicos, ni que establezca

límites claros sobre su uso con fines de vigilancia. Esta omisión resulta especialmente preocupante si se considera que algunas instituciones públicas y privadas ya han empezado a utilizar tecnologías biométricas sin contar con mecanismos de control adecuados, exponiendo a la ciudadanía a escenarios de vigilancia masiva y riesgo de discriminación algorítmica (Fundamedios, 2021).

Organizaciones de la sociedad civil como Fundamedios han advertido sobre los riesgos de estas prácticas, señalando la posibilidad de que se utilicen para criminalizar la protesta social, estigmatizar a poblaciones marginadas o facilitar prácticas abusivas por parte de cuerpos policiales. La ausencia de estudios de impacto, evaluaciones éticas o garantías de transparencia en la adquisición de estas tecnologías genera una situación de vulnerabilidad estructural frente al poder estatal o corporativo que controla los sistemas de videovigilancia.

A nivel internacional, las preocupaciones en torno al uso de inteligencia artificial y su impacto sobre los derechos humanos han sido ampliamente reconocidas. La UNESCO, en su Recomendación sobre la Ética de la Inteligencia Artificial (2021), ha subrayado que toda implementación de tecnologías algorítmicas debe respetar de manera irrestricta los derechos humanos, prohibir el uso discriminatorio de sistemas de reconocimiento facial y evitar prácticas de vigilancia masiva que configuren escenarios panópticos incompatibles con la dignidad humana. De igual forma, organizaciones como Human Rights Watch (2023) han exhortado a los Estados a prohibir el uso de tecnologías de reconocimiento facial en espacios públicos, advirtiendo que estas herramientas pueden socavar gravemente la libertad de reunión, el derecho a la privacidad y la libertad de expresión.

Casos emblemáticos ilustran los riesgos concretos de delegar decisiones sensibles en sistemas algorítmicos técnicamente sesgados. El Tribunal de Apelaciones del Reino Unido, por ejemplo, declaró ilegal el uso de tecnología de reconocimiento facial por parte de la policía de Gales del Sur, al considerar que vulneraba garantías fundamentales. En Estados Unidos, el caso de Robert Williams (detenido erróneamente a raíz de una coincidencia algorítmica) evidenció las consecuencias materiales que pueden derivarse de errores en el procesamiento de datos biométricos (Dejusticia, 2022).

En el caso ecuatoriano, la incorporación de estas tecnologías sin un marco legal sólido plantea riesgos importantes. La falta de regulación puede agravar desigualdades estructurales, reproducir sesgos raciales o clasistas, y debilitar aún más la confianza ciudadana en las instituciones públicas. Ante este escenario, es urgente que el Estado ecuatoriano no solo adecúe su normativa a estándares internacionales, sino que lo haga desde una perspectiva crítica, situada y contextualizada, que considere las condiciones sociales, étnicas y territoriales propias del país. En consecuencia, resulta necesario promover un debate democrático, interdisciplinario y participativo sobre el uso legítimo de la inteligencia artificial en contextos de seguridad pública. Además, se deben establecer reglas claras, fortalecer los mecanismos de control institucional y auditoría, y garantizar vías efectivas de reparación ante posibles abusos.

Capítulo III: Límites del Derecho Ecuatoriano frente al uso de IA con imágenes: alcances y responsabilidades

Introducción

El acelerado desarrollo de tecnologías basadas en inteligencia artificial (IA), en particular aquellas orientadas a la generación y manipulación de imágenes (como los deepfakes, algoritmos de clonación facial o generadores de contenido visual hiperrealista), ha inaugurado una nueva dimensión de riesgos jurídicos que desafía los marcos normativos tradicionales. Estas herramientas permiten crear imágenes falsas con apariencia de autenticidad, que pueden afectar derechos fundamentales como la imagen, la intimidad, la honra, la privacidad y la autodeterminación informativa, reconocidos en el ordenamiento constitucional ecuatoriano (Constitución de la República del Ecuador, 2008, arts. 10, 10.9, 66.18 y 66.19).

En el contexto ecuatoriano, la arquitectura normativa vigente presenta una protección fragmentada, generalista y mayormente reactiva, que resulta insuficiente frente a los desafíos que plantea la IA generativa aplicada a datos visuales. Si bien existen disposiciones en la Constitución, el Código Orgánico Integral Penal, la Ley Orgánica de Protección de Datos Personales, y mecanismos jurisdiccionales como la acción de protección o la acción civil por daños y perjuicios, dichos instrumentos no han sido diseñados para responder a fenómenos algorítmicos autónomos, transnacionales y de rápida propagación digital. Considerando la debilidad institucional, la poca deontología y los limitantes académicos presentes en gran parte de los profesionales del derecho, de lo cual, se evidencia en el irrespeto constante al debido proceso, el limitado acceso al pleno goce de derechos y las polémicas sentencias que han permitido la impunidad de personas relacionadas con crimen organizado.

El principal problema no radica únicamente en la ausencia de tipificaciones o cláusulas explícitas sobre IA, sino en la inadecuación dogmática de los conceptos jurídicos tradicionales (autoría, dolo, captura de imagen, consentimiento) para abordar nuevas formas de afectación como la síntesis de rostros sin contacto físico previo, la manipulación audiovisual sin intervención humana directa o la suplantación de identidad mediante modelos entrenados con datos disponibles en redes sociales. Esta distancia conceptual ha sido señalada por la doctrina como un indicio de obsolescencia normativa frente a las lógicas emergentes de la sociedad digital (De Gregorio, 2021; Calo, 2020).

Este capítulo examina, desde una perspectiva jurídica crítica, los límites estructurales del derecho ecuatoriano frente al uso de IA con imágenes personales, con énfasis en la falta de tipificación específica, los desafíos probatorios, los vacíos de imputación normativa y las restricciones del régimen actual de responsabilidad. A su vez, se analizan posibles reformas normativas que permitan fortalecer la tutela efectiva de los derechos personalísimos en entornos digitales, garantizando estándares de reparación integral, trazabilidad tecnológica y supervisión institucional de las herramientas de IA.

Partiendo de una lectura constitucional garantista y con respaldo en la jurisprudencia nacional e interamericana, el análisis propuesto en este capítulo busca desplegar un marco propositivo de actualización normativa que permita compatibilizar los avances tecnológicos con el contenido esencial de los derechos fundamentales, y prevenir escenarios de impunidad jurídica ante nuevas formas de violencia simbólica y afectación algorítmica.

Análisis de la normativa vigente

El ordenamiento jurídico ecuatoriano reconoce, de manera dispersa, distintos instrumentos destinados a la protección del derecho a la imagen, la intimidad, y los datos personales. No obstante, al enfrentarse al fenómeno de la inteligencia artificial (IA) (particularmente en lo que concierne a la generación y manipulación de imágenes mediante herramientas como deepfakes), este marco normativo revela graves vacíos de regulación y escasa operatividad práctica. La aceleración tecnológica y la complejidad algorítmica de las nuevas herramientas utilizadas para manipular imágenes superan, en muchos casos, los estándares tradicionales de imputación penal, reparación civil o garantías constitucionales, generando escenarios de indefensión jurídica para las víctimas.

La Constitución de la República del Ecuador consagra en su artículo 66, numeral 18, el derecho a la imagen como parte del conjunto de derechos personalísimos vinculados a la dignidad humana. Asimismo, reconoce el principio de progresividad y no regresividad en el desarrollo normativo de los derechos (art. 11.8). Estas disposiciones tienen un carácter programático, y su eficacia depende de su concreción a través de leyes específicas y garantías procesales efectivas (Constitución de la República del Ecuador, 2008).

En el ámbito penal, el Código Orgánico Integral Penal (COIP) sanciona conductas como la violación a la intimidad (art. 178), la difusión no consentida de contenido íntimo (art. 179) y la suplantación de identidad (art. 212). Estas figuras responden a modelos tradicionales de delito, tipos penales que parten de la existencia de contenido real, grabación directa o manipulación convencional de datos personales. Sin embargo, la proliferación de imágenes generadas artificialmente, sin una fuente original ni intervención física del rostro de la víctima, proporciona

un comportamiento de tipo penal restringido que impide aplicar de forma extensiva o analógica disposiciones lo que produce un limbo normativo. En virtud del principio de legalidad penal, no resulta admisible extender o aplicar por analogía tipos penales que no regulan de manera expresa el uso de tecnologías basadas en inteligencia artificial. Esta omisión normativa evidencia la necesidad de impulsar reformas legislativas específicas que permitan cerrar ese vacío doctrinal.

La Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Suplemento del Registro Oficial No. 459 de 26 de mayo de 2021, constituye un avance normativo relevante en materia de protección de datos en el Ecuador. Dentro de su articulado, reconoce expresamente la imagen facial como un dato biométrico sensible (art. 4), lo que implica un tratamiento reforzado en términos de protección jurídica y establece principios como el consentimiento, la finalidad específica y la proporcionalidad (arts. 8 y 10). Sin embargo, la ley no incorpora disposiciones expresas sobre el tratamiento automatizado de datos con fines de manipulación o síntesis mediante IA, dejando sin cobertura normativa a prácticas emergentes como la creación de deepfakes con fines de difamación, acoso o suplantación (LOPDP, 2021).

Desde la perspectiva constitucional, la acción de protección (consagrada en el artículo 88 de la Constitución de la República del Ecuador y desarrollada en los artículos 39 a 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional) constituye una garantía jurisdiccional orientada a tutelar derechos fundamentales frente a actos u omisiones de autoridades públicas o de particulares. En principio, esta acción puede ejercerse contra cualquier persona natural o jurídica que pueda ser identificada como autora, difusora o responsable de permitir la permanencia de un contenido lesivo, incluyendo —en ciertos casos— a plataformas digitales que, pese a haber sido notificadas, no proceden con su remoción. No obstante, su eficacia frente a afectaciones generadas mediante inteligencia artificial se ve limitada por

diversos factores, entre ellos: la complejidad para demostrar una relación de causalidad directa, la exigencia de acreditar un daño concreto y la dificultad para identificar de forma precisa al responsable.

Frente a este escenario, se hace necesario que el juez constitucional adopte un enfoque interpretativo más flexible al momento de valorar el nexo causal y la legitimación pasiva, de modo que se privilegie la tutela efectiva del derecho afectado sobre las rigideces probatorias que caracterizan a los entornos analógicos. Como advierten Basabe-Serrano y Cobo (2022, pp. 21–23), el contexto digital exige repensar las categorías clásicas del derecho constitucional, a fin de asegurar la operatividad real de los mecanismos de protección frente a nuevas formas de afectación.

En el plano del derecho privado, el ordenamiento jurídico ecuatoriano reconoce la acción de indemnización por perjuicios, prevista en los artículos 2214 y siguientes del Código Civil, como una vía general para exigir la reparación de los daños derivados de hechos ilícitos, incluyendo aquellos que comprometan la imagen personal. Sin embargo, su aplicación efectiva en controversias relacionadas con el uso de inteligencia artificial presenta obstáculos importantes. Entre las principales dificultades se encuentran la limitada disponibilidad de peritos con formación especializada en tecnologías digitales, las elevadas cargas probatorias que recaen sobre quien promueve la acción, y una práctica judicial —todavía presente en ciertos órganos jurisdiccionales— que supedita la admisión de la vía civil a la existencia previa de una sentencia penal condenatoria. Esta práctica, aunque doctrinalmente discutible, restringe el acceso oportuno a mecanismos de reparación integral, en contradicción con los principios de celeridad y efectividad que deben regir los procesos de tutela de derechos.

En suma, el marco normativo vigente en Ecuador ofrece una protección fragmentada, general e insuficiente frente a las amenazas emergentes que plantea la inteligencia artificial respecto al derecho a la imagen. La falta de tipificación penal específica, la ausencia de una política pública de gobernanza algorítmica y la carencia de instituciones con capacidad técnica para investigar estas vulneraciones constituyen una amenaza estructural a los derechos personalísimos en el entorno digital. El avance tecnológico es una amenaza para los derechos, en tanto no existan mecanismos jurídicos e instituciones sólidas y capacitadas para enfrentar los desafíos de la era digital.

Constitución de la República del Ecuador

La Constitución de la República del Ecuador, vigente desde 2008, reconoce en su artículo 66, numeral 18, el derecho de toda persona a la protección de su imagen y voz, así como de otros elementos constitutivos de su identidad personal. Esta disposición se inscribe dentro del catálogo de derechos personalísimos, cuya tutela deriva del principio de dignidad humana, eje estructurante del sistema constitucional. En este marco, la imagen no se concibe únicamente como una representación física, sino como una proyección simbólica y social de la personalidad jurídica que emana de la persona natural, y que por tanto merece una protección reforzada frente a cualquier forma de manipulación, suplantación o utilización no autorizada.

Este reconocimiento se articula con los principios establecidos en el bloque de constitucionalidad, especialmente con los tratados internacionales de derechos humanos ratificados por el Estado ecuatoriano. El artículo 11, numeral 3, dispone que todos los derechos son de aplicación directa e inmediata, y que, en caso de ambigüedad o duda sobre su alcance, deberá prevalecer la interpretación más favorable a la persona. A su vez, el numeral 8 del mismo

artículo consagra el principio de progresividad, que prohíbe la adopción de normas regresivas y exige al Estado desarrollar activamente su normativa para garantizar el ejercicio pleno y actualizado de los derechos, particularmente frente a nuevos contextos como el entorno digital y las tecnologías emergentes.

No obstante, el reconocimiento constitucional del derecho a la imagen, la Carta Magna no aborda de forma expresa los desafíos emergentes asociados al uso de inteligencia artificial para generar, alterar o difundir imágenes. Su formulación se enmarca en un contexto normativo previo al desarrollo de tecnologías como los deepfakes, las redes generativas adversariales (GANs) o los sistemas de clonación facial por algoritmos. Esta distancia entre la consagración abstracta del derecho y las nuevas formas de afectación mediante herramientas automatizadas reduce su operatividad jurídica y dificulta su exigibilidad efectiva ante las instancias jurisdiccionales. La necesidad de reinterpretar y actualizar el contenido del derecho a la imagen se vuelve entonces imperativa para asegurar su vigencia frente a los desafíos del ecosistema digital contemporáneo.

Desde la perspectiva dogmática, esta laguna puede generar conflictos en la interpretación del contenido esencial del derecho a la imagen. La Corte Constitucional ha señalado que el contenido protegido de un derecho debe analizarse a la luz del contexto social y tecnológico en el que se desarrolla su ejercicio y que las nuevas formas de afectación deben ser incorporadas a su alcance mediante interpretación evolutiva (Corte Constitucional del Ecuador, Sentencia No. 11-18-CN/19, FJ. 34). En este sentido, la jurisprudencia comparada ha ampliado el contenido del derecho a la imagen para incluir situaciones en las que la persona es afectada sin que haya existido una captación directa de su imagen, como ocurre con la síntesis digital o la recreación artificial de su rostro mediante IA (De Gregorio, 2021).

La Constitución ecuatoriana reconoce el acceso a la justicia (art. 75), la tutela judicial efectiva (art. 76) y el principio de responsabilidad objetiva del Estado por violaciones de derechos fundamentales (art. 11.9). No obstante, estos principios enfrentan serias dificultades cuando las afectaciones al derecho a la imagen provienen de tecnologías autónomas o de agentes anónimos que actúan desde entornos digitales con baja trazabilidad. Esta situación genera una tensión estructural entre las garantías establecidas en el orden constitucional y las lógicas de funcionamiento propias de los sistemas algorítmicos.

En conclusión, aunque el texto constitucional ofrece un andamiaje normativo sólido para la protección de la imagen como derecho fundamental, su capacidad de respuesta frente a las amenazas emergentes asociadas al uso de inteligencia artificial sigue siendo limitada y requiere actualización. La omisión de una referencia explícita a las tecnologías digitales y algorítmicas en el tratamiento del derecho a la imagen exige una labor urgente de interpretación jurisprudencial y reforma legislativa que permita actualizar la noción de este derecho en consonancia con la realidad tecnológica contemporánea.

Código Orgánico Integral Penal (COIP)

Uno de los tipos penales que podría considerarse aplicable en casos de afectación a la imagen mediante inteligencia artificial es el delito de violación a la intimidad, previsto en el artículo 178 del Código Orgánico Integral Penal (COIP). Esta norma establece una sanción privativa de libertad de uno a tres años para quien, sin el consentimiento del titular, capte, reproduzca, difunda o publique datos personales, audios, imágenes o videos obtenidos en contextos de intimidad o privacidad, incluso si el contenido divulgado resulta veraz. Aunque ofrece una forma de protección directa frente a intromisiones en la vida privada, su eficacia se ve

limitada cuando se enfrenta a nuevas conductas vinculadas con el uso de inteligencia artificial, que no siempre se ajustan a los supuestos tradicionales contemplados en el tipo penal.

En primer lugar, los tipos penales vinculados a la violación de la intimidad, la difusión no consentida de material íntimo o la suplantación de identidad presuponen la existencia previa de un contenido real captado o intervenido por terceros. En contraste, las imágenes generadas artificialmente mediante IA (por ejemplo, mediante técnicas de deepfake) no se originan a partir de un hecho auténtico, sino que son fabricadas ex novo por algoritmos, lo cual las coloca fuera del alcance de los supuestos tradicionales. Esta incompatibilidad genera una laguna de tipicidad que no puede ser superada por vía analógica, en virtud del principio de legalidad penal. Como ha señalado Martínez Hernández (2021), este vacío normativo evidencia la urgencia de adaptar el derecho penal a las nuevas formas de agresión simbólica y reputacional habilitadas por tecnologías emergentes.

En segundo lugar, en aquellos casos en los que el contenido sintético no se deriva de una grabación original ni de datos previamente recopilados, el consentimiento de la víctima deviene jurídicamente irrelevante bajo el esquema actual. Esta circunstancia genera una tensión interpretativa respecto de si los montajes digitales pueden subsumirse dentro del tipo penal vigente. En la práctica, esta ambigüedad contradice la finalidad preventiva de la norma, al no ofrecer una respuesta clara frente a nuevas formas de exposición no consentida que afectan gravemente la imagen y la intimidad de las personas.

Adicionalmente, el artículo 179 del COIP penaliza la difusión no consentida de contenido íntimo con una pena de uno a tres años, aún cuando la persona haya entregado el contenido de forma voluntaria. Esta norma se enmarca en la lucha contra la violencia digital y el “revenge

porn". Sin embargo, su aplicación se limita a contenidos existentes que han sido captados o compartidos por la víctima en algún momento, y no cubre los casos en los que el contenido íntimo es totalmente fabricado mediante IA, como ocurre en los deepfakes pornográficos.

Por otro lado, el artículo 212 sanciona la suplantación de identidad, entendida como la acción de utilizar datos ajenos para realizar actos jurídicos o técnicos en nombre de otra persona. Aunque esta figura podría utilizarse en casos donde la imagen de una persona es falsificada mediante IA con el fin de engañar a terceros (por ejemplo, en fraudes digitales o estafas virtuales que involucran videos manipulados), también presenta limitaciones:

- El tipo penal requiere que se utilicen datos identificativos como nombres, firmas o números de documento, y no necesariamente imágenes o rasgos biométricos.
- La escensia automatizada y descentralizada de la IA no ofrece luces para la identificación de un autor penalmente identificable. Debido a que, entra en tensión directa con el principio de imputación subjetiva que dispone exista dolo o culpa humana como base para poder atribuir responsabilidad penal. Puesto que, los sistemas algorítmicos autónomos no pueden ser sujetos a atributos de intencionalidad o conocimiento típico, lo que refleja un vacío en las estructuras dogmáticas tradicionales del derecho penal y evidencia la urgencia de generar normas específicas para aborardar la brecha generada por el entorno digital.

En este contexto, se produce una paradoja normativa: las herramientas digitales que más afectan a la imagen y reputación de las personas (como los deepfakes o las aplicaciones de clonación facial) escapan de la cobertura del COIP, al no haber sido diseñadas como medios típicos de comisión del delito. Además, la arquitectura jurídica del COIP parte de la noción de autoría

individual, lo cual complica la imputación cuando las conductas han sido automatizadas o ejecutadas en plataformas que no operan desde territorio ecuatoriano.

La doctrina penal comparada ha comenzado a discutir la necesidad de tipificar figuras específicas como la "falsificación digital de identidad visual" o la "difusión de contenidos sintéticos no consentidos", que reconozcan la existencia de un daño real aún sin contenido original, y que incluyan agravantes cuando el material involucre connotaciones sexuales, racistas o discriminatorias (De Gregorio, 2021).

En suma, el COIP no ofrece un marco penal adecuado para enfrentar los usos lesivos de la IA aplicados a imágenes personales, y su aplicación requiere forzadas interpretaciones extensivas que pueden vulnerar el principio de legalidad estricta (art. 76.3 CRE). Frente a este vacío, el legislador tiene el deber de incorporar tipos penales específicos, claros y proporcionados, que protejan a las personas frente a la violencia simbólica y la afectación reputacional que estas tecnologías pueden producir.

Ley Orgánica de Protección de Datos Personales

La promulgación de la *Ley Orgánica de Protección de Datos Personales* (LOPDP), publicada en el Registro Oficial Suplemento No. 459 el 26 de mayo de 2021, constituye un hito normativo en el desarrollo del derecho a la autodeterminación informativa en el Ecuador. Esta ley establece un marco general de garantías orientado a regular el tratamiento de datos personales, consagrando principios como la legalidad, finalidad, proporcionalidad, minimización, consentimiento, confidencialidad y seguridad, los cuales deben ser respetados por los responsables y encargados del tratamiento de dichos datos (arts. 7–12, LOPDP, 2021).

Entre los aspectos más relevantes de la Ley Orgánica de Protección de Datos Personales en el contexto de este estudio se encuentra el reconocimiento expreso de los datos biométricos como datos personales sensibles. El artículo 4 de la ley define los datos biométricos como aquellos “relativos a características físicas, fisiológicas o de comportamiento, que permiten o confirman la identificación única de una persona natural, tales como huellas dactilares, imágenes faciales, patrones de iris, reconocimiento de voz, entre otros”. A partir de esta definición, la imagen facial queda comprendida dentro del ámbito de especial protección, y su tratamiento indebido puede dar lugar a sanciones administrativas o incluso responsabilidades civiles o penales.

El artículo 8 de la Ley Orgánica de Protección de Datos Personales establece que el tratamiento de datos personales sensibles solo será lícito cuando el titular haya otorgado su consentimiento expreso y por escrito, salvo contadas excepciones previstas por la Ley. A su vez, el artículo 10 prohíbe la utilización de estos datos para fines distintos de aquellos que motivaron su recolección, y obliga al responsable del tratamiento a implementar medidas de seguridad técnicas y organizativas adecuadas al nivel de riesgo, principalmente a la filtración de información.

Sin embargo, a pesar de la inclusión de estas garantías, la Ley Orgánica de Protección de Datos Personales (LOPDP) no aborda de manera específica el tratamiento automatizado de imágenes mediante herramientas de inteligencia artificial, ni contempla disposiciones relativas a la generación sintética de contenido audiovisual mediante IA (como los deepfakes, la clonación facial o los generadores de contenido visual hiperrealista). La ausencia de una regulación específica sobre estas tecnologías genera un vacío normativo importante, ya que es posible producir imágenes falsas que simulan rostros humanos sin necesidad de haber captado

directamente datos biométricos. Esta característica dificulta la aplicación estricta de las disposiciones legales vigentes, que suelen presuponer una obtención directa del dato.

Sin embargo, cuando el contenido generado permite identificar a una persona natural, su creación y difusión podrían constituir un tratamiento de datos personales sin base jurídica válida, de acuerdo con lo establecido en los artículos 7 y 10 de la Ley Orgánica de Protección de Datos Personales. En consecuencia, tales prácticas podrían ser sancionadas administrativamente, al constituir un tratamiento ilícito de datos personales sensibles, incluso en ausencia de una norma que regule específicamente las herramientas de IA. Esta interpretación refuerza la necesidad de una reforma normativa que, sin perjuicio de la aplicación del régimen vigente, adapte el marco legal a los nuevos desafíos técnicos y garantice la seguridad jurídica de los titulares de derechos, en concordancia con el artículo 82 de la Constitución, que establece que "el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicables."

Un problema adicional radica en que la Ley Orgánica de Protección de Datos Personales (LOPDP) fue concebida bajo un enfoque centrado en el tratamiento de datos personales desde esquemas tradicionales, es decir, orientado a la recolección, almacenamiento y circulación de información preexistente contenida en bases de datos. Sin embargo, los retos contemporáneos requieren replantear dicho enfoque frente a nuevas formas de generación algorítmica de contenido visual —como los deepfakes— que reproducen características personales sin necesidad de una captación directa de datos reales.

En estos casos, aunque la imagen haya sido generada desde cero, si permite identificar o vincular a una persona natural específica, sigue siendo un dato personal en los términos del

artículo 4 de la LOPDP, por lo que su tratamiento sin base legitimadora podría constituir una infracción. El problema radica en que el estándar técnico-jurídico vigente no siempre contempla con claridad esta modalidad indirecta de tratamiento, lo que puede dificultar el ejercicio de derechos o la sanción de conductas lesivas. Aun así, persiste una clara afectación a la imagen, la honra o la integridad emocional de la persona, que exige una respuesta normativa más precisa y adaptada a estos entornos.

Asimismo, si bien la Ley Orgánica de Protección de Datos Personales del Ecuador recoge en gran parte los principios y obligaciones previstos en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, como la rendición de cuentas (accountability), la evaluación de impacto y el derecho a la explicación frente a decisiones automatizadas (arts. 22–23 RGPD), su desarrollo normativo aún no ha sido adaptado de forma concreta a los desafíos específicos que plantea la inteligencia artificial generativa. En particular, no se prevén obligaciones claras y operativas para los desarrolladores de software basado en IA ni para las plataformas que permiten la generación, circulación o monetización de contenido visual falso, lo que limita la capacidad del régimen actual para enfrentar la opacidad algorítmica y los efectos sistémicos de las tecnologías de manipulación de imagen. La ausencia de regulación específica no se debe únicamente a una omisión formal en el cuerpo normativo, sino que refleja, en gran medida, la falta de una adecuada implementación práctica de los principios ya previstos en la legislación vigente. Esta falencia en la operatividad del marco legal dificulta la aplicación real y oportuna de los derechos reconocidos, especialmente frente a contextos complejos, dinámicos y tecnológicamente avanzados como los que plantea el uso de inteligencia artificial generativa.

En consecuencia, la Ley Orgánica de Protección de Datos Personales resulta insuficiente para dar respuesta a los desafíos jurídicos que plantea la IA aplicada a la imagen personal. Su

enfoque se encuentra limitado por una concepción tradicional del tratamiento de datos, centrada en la captura, almacenamiento y uso de información existente, sin contemplar de forma explícita los fenómenos relacionados con la generación sintética de contenido. Además, la ley carece de disposiciones específicas sobre transparencia algorítmica, trazabilidad de procesos automatizados y deberes de diligencia reforzada para los desarrolladores, proveedores y plataformas tecnológicas que operan en el ecosistema digital. Esta omisión normativa impide establecer mecanismos de control adecuados, debilita la protección de los derechos personalísimos y deja a las víctimas en situación de indefensión ante nuevas formas de afectación generadas por tecnologías emergentes. Tampoco contempla normativa que resuelva conflictos con proveedores internacionales, lo que limita la capacidad de acceso a una tutela efectiva de los derechos.

Como han señalado especialistas en derecho digital, las leyes de protección de datos deben evolucionar desde un paradigma estático y formalista hacia un modelo dinámico, centrado en riesgos, contextos y efectos reales sobre los derechos fundamentales (Tzanou, 2017). En este sentido, Ecuador se enfrenta al desafío urgente de reformar la Ley Orgánica de Protección de Datos Personales para incluir disposiciones explícitas sobre inteligencia artificial, creación de contenido sintético y obligaciones específicas para actores tecnológicos, siguiendo el modelo propuesto por el “Artificial Intelligence Act” de la Unión Europea.

Garantía jurisdiccional de protección constitucional: la Acción de Protección

La acción de protección constituye uno de los mecanismos jurisdiccionales fundamentales dentro del modelo de Estado constitucional de derechos y justicia, destinado a garantizar la vigencia efectiva de los derechos fundamentales. Su base normativa se encuentra en

el artículo 88 de la Constitución de la República del Ecuador y en los artículos 39 a 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, reformada en el año 2024. Esta acción tiene por finalidad tutelar, de forma directa e inmediata, los derechos reconocidos en la Constitución y en los tratados internacionales de derechos humanos, frente a actos u omisiones cometidos por autoridades públicas o por particulares que ejerzan funciones públicas.

En el contexto de la manipulación de imágenes mediante inteligencia artificial (IA), la acción de protección puede configurarse como una vía idónea para hacer cesar una amenaza o vulneración al derecho a la imagen, la honra, la intimidad o la integridad personal, derechos que gozan de protección reforzada y forman parte del núcleo intangible del catálogo constitucional (art. 11 CRE).

a) Configuración dogmática y operativa

La Corte Constitucional ha señalado que este tipo de acciones deben garantizar una protección eficaz frente a amenazas o vulneraciones de derechos, especialmente cuando no existan mecanismos ordinarios adecuados. En particular, ha afirmado que la acción de protección es procedente cuando concurren tres elementos básicos: (i) existencia de un derecho constitucionalmente protegido; (ii) una amenaza o vulneración atribuible a una entidad obligada; y (iii) la inexistencia de mecanismos ordinarios eficaces para atender la afectación (Corte Constitucional del Ecuador, Sentencia No. 002-13-SAN-CC, 2013, FJ. pp. 6–9). Esto refuerza la necesidad de contar con instrumentos ágiles que se adapten a las nuevas formas de afectación de derechos en entornos digitales y tecnológicos complejos.

En los casos en los que se difunden deepfakes u otro tipo de contenido visual generado mediante IA que afecte la imagen de una persona, es posible acudir directamente a la acción de protección para solicitar el cese de la difusión del contenido, su remoción de plataformas digitales, y una reparación integral, entendida conforme a estándares interamericanos como la restitutio in integrum, la indemnización, la rehabilitación y las garantías de no repetición (Corte IDH, Caso Vélez Restrepo y Familiares vs. Colombia, 2012).

b) Jurisprudencia relevante de la Corte Constitucional del Ecuador

En la Sentencia No. 198-17-SEP-CC (caso Alejandro Ribadeneira), la Corte Constitucional del Ecuador estableció que el derecho a la imagen implica el control individual sobre el uso y la difusión de los rasgos visuales de una persona, y que cualquier tratamiento no consentido puede constituir una vulneración directa a la dignidad y a la autodeterminación informativa. En esa misma línea, la Sentencia No. 2032-20-JP/25 reconoció que las plataformas digitales son espacios fundamentales para el ejercicio de derechos fundamentales, y que cualquier restricción o afectación en estos entornos debe someterse a los principios de legitimidad, necesidad, proporcionalidad y revisión judicial efectiva. Estos estándares pueden ser extendidos por analogía a los entornos digitales donde circulan contenidos sintéticos (como imágenes, audios o videos generados mediante inteligencia artificial) que afectan la honra, la reputación o la imagen personal de las personas representadas sin su consentimiento.

En escenarios de violencia digital y manipulación algorítmica de datos personales, derechos personalísimos como la imagen, la honra y la intimidad pueden ser protegidos mediante la acción de protección, incluso cuando los actos lesivos se originan en entornos privados o involucran tecnologías complejas. Si bien la identificación del autor material puede resultar

especialmente complicada —por ejemplo, en casos en que el contenido ha sido generado por sistemas automatizados o alojado en servidores ubicados fuera del país—, el juez constitucional mantiene su facultad de intervención siempre que se constate una amenaza o vulneración suficientemente clara a derechos fundamentales.

Esta postura ha sido sostenida por la Corte Constitucional en sentencias como la No. 2032-20-JP/25, donde se reafirma la obligación de garantizar la protección efectiva de derechos fundamentales en entornos digitales, a través de mecanismos judiciales que sean proporcionales, eficaces y sometidos a control jurisdiccional oportuno.

c) Limitaciones estructurales y retos procesales

Aunque la acción de protección representa, en principio, una herramienta constitucional idónea para salvaguardar el derecho a la imagen, su aplicación práctica enfrenta diversos obstáculos de orden estructural. Uno de los principales desafíos es que, en muchos casos, las imágenes manipuladas provienen de algoritmos anónimos, plataformas extranjeras o redes digitales cuya trazabilidad es limitada. En estos contextos, la persona afectada enfrenta una dificultad probatoria concreta: no siempre puede identificar al responsable directo ni tiene claridad sobre contra quién dirigir la acción. Ante esta situación, una vía alternativa sería permitir que la acción se dirija contra quienes difunden o mantienen el contenido sabiendo que es falso (como una plataforma, medio digital o red social) o incluso contra el Estado cuando este omite adoptar medidas adecuadas para prevenir o remediar la afectación.

Adicionalmente, persiste una marcada disparidad en la forma en que los jueces interpretan y aplican los criterios de admisibilidad y procedencia de la acción de protección, lo

que afecta especialmente a personas en situación de vulnerabilidad. La falta de formación técnica especializada en tecnologías digitales entre operadores judiciales, junto con la desigual distribución de recursos institucionales, configura un escenario poco favorable para el ejercicio pleno del derecho a una justicia efectiva y equitativa. En la práctica, ello se traduce en el rechazo prematuro de acciones constitucionales por supuesta insuficiencia probatoria inicial, revictimizando a quienes ya han visto comprometidos sus derechos fundamentales.

Tal como advierten Quito-Guerrero y Zamora Vázquez (2025), si no se refuerza la institucionalidad judicial mediante un enfoque inclusivo y tecnológicamente actualizado, el acelerado desarrollo de herramientas como la inteligencia artificial no solo perpetuará las desigualdades ya existentes, sino que podría intensificarlas, profundizando las barreras estructurales de acceso a la justicia en entornos digitales.

d) Necesidad de interpretación evolutiva

Ante el desafío que plantea la expansión de tecnologías como la inteligencia artificial en la generación de contenidos visuales sintéticos, se vuelve imprescindible que la Corte Constitucional adopte una interpretación evolutiva y sistemática de los derechos a la imagen, la intimidad y la honra. La creación de imágenes mediante procesos algorítmicos, sin consentimiento del titular, puede ocasionar afectaciones serias a la dignidad personal, incluso si dichas representaciones no se corresponden con hechos reales. Esto es particularmente relevante cuando los efectos simbólicos del contenido comprometen la reputación o la percepción social de la persona implicada.

Desde la perspectiva garantista, se ha sostenido que la valoración de una posible vulneración a derechos fundamentales no puede limitarse a la veracidad del contenido, sino que debe considerar su capacidad de causar daño, generar estigmatización o propiciar formas de control social. La persistencia de enfoques judiciales rígidos, basados en esquemas dogmáticos tradicionales, junto con la falta de marcos normativos adecuados al entorno digital, incrementa el riesgo de que estas afectaciones queden impunes o sin una reparación efectiva. En este contexto, el desarrollo normativo y jurisprudencial en clave de derechos se vuelve indispensable para evitar vacíos de protección ante fenómenos que trascienden los esquemas tradicionales de imputación y daño.

Alternativa en la vía ordinaria civil: la acción de daños y perjuicios

En el sistema jurídico ecuatoriano, la acción de indemnización de perjuicios constituye un mecanismo tradicional de reparación integral frente a los daños causados por hechos ilícitos o por incumplimiento de obligaciones. Esta acción se encuentra regulada en los artículos 2214 y siguientes del Código Civil, y su finalidad es restituir a la persona afectada a la situación anterior al daño o al menos compensar material y moralmente las consecuencias negativas sufridas.

Según la doctrina general del derecho civil, esta acción puede ser ejercida de forma autónoma, siempre que se demuestre la concurrencia de tres elementos esenciales: (i) la existencia de un daño cierto; (ii) la relación de causalidad entre el hecho y el daño; y (iii) la conducta antijurídica de quien lo causa sea dolosa o culposa (Mosquera Benalcázar, 2019). La acción civil resulta procedente tanto en el ámbito contractual como extracontractual y ha sido empleada en múltiples casos relacionados con la afectación de derechos de la personalidad, tales como la honra, la intimidad, el nombre y la imagen. En particular, frente a daños ocasionados por

el uso no autorizado de imágenes manipuladas o generadas mediante inteligencia artificial, esta vía adquiere especial importancia cuando la persona afectada busca obtener una reparación económica por los perjuicios patrimoniales y extrapatrimoniales derivados de la difusión de dichos contenidos. El artículo 1572 del Código Civil ecuatoriano establece expresamente que: La indemnización de perjuicios comprende el daño emergente y el lucro cesante, ya provengan de no haberse cumplido la obligación, o de haberse cumplido imperfectamente, o de haberse retardado el cumplimiento (*Código Civil*, 2025, art. 1572).

Bajo esta premisa, el daño emergente puede entenderse como la pérdida patrimonial directa sufrida por la víctima, derivada de los gastos necesarios para contener la difusión del contenido falso o para acceder a atención médica, psicológica o psiquiátrica ante los efectos de la exposición no consentida. El lucro cesante se refiere a las ganancias o beneficios que la persona afectada razonablemente habría obtenido de no haberse producido el hecho lesivo. En el contexto del uso indebido de imágenes, este daño puede manifestarse en la pérdida de oportunidades laborales, la terminación anticipada de contratos, la disminución del alcance en plataformas digitales o la exclusión de proyectos profesionales. Esta forma de perjuicio adquiere particular relevancia en el caso de figuras públicas o profesionales cuya imagen constituye un activo reputacional clave para el desarrollo de su actividad económica.

Obstáculos en la práctica judicial

Aunque la jurisdicción civil constituye, en principio, una vía adecuada para reclamar la reparación de daños ocasionados por el uso indebido de tecnologías como la inteligencia artificial, su aplicación práctica en el contexto ecuatoriano enfrenta una serie de limitaciones estructurales que afectan su eficacia:

1. Exigencia de prueba directa del daño: Algunos jueces civiles exigen la presentación de prueba objetiva y directa que acredite plenamente la existencia del daño al momento de admitir o resolver la demanda. Esta exigencia resulta especialmente problemática cuando se trata de perjuicios intangibles —como los de carácter emocional, psicológico o reputacional— que, por su naturaleza, no siempre pueden ser cuantificados con criterios tradicionales. La ausencia de lineamientos claros para valorar este tipo de afectaciones y la falta de uniformidad en los criterios judiciales representan barreras relevantes para la admisión y el éxito de las acciones civiles.

2. Subordinación a sentencia penal previa: En ciertos tribunales persiste la práctica de condicionar la procedencia de la demanda civil a la existencia de una sentencia penal condenatoria que acredite la ilicitud del acto causante del daño. Esta postura resulta incompatible con el principio de autonomía de la responsabilidad civil y desconoce la jurisprudencia que permite el ejercicio de acciones indemnizatorias en materia extracontractual sin necesidad de una resolución penal previa.

3. Déficit de especialización judicial y apoyo pericial: La falta de formación técnica en temas de derecho digital y tecnologías emergentes entre operadores judiciales limita la comprensión adecuada de los mecanismos utilizados para manipular imágenes o generar contenido sintético. Además, la escasez de peritos especializados en evidencia digital complica la valoración probatoria y debilita la capacidad del sistema judicial para emitir decisiones informadas y justas.

4. Dificultad para imputar responsabilidad civil: La lógica distribuida, automatizada y transnacional que caracteriza a muchos sistemas de generación de contenido por IA plantea serios desafíos en la determinación de la responsabilidad civil. En casos donde los programas han sido operados por múltiples usuarios anónimos o desarrollados por empresas extranjeras sin representación legal en el país, se vuelve complejo identificar a los sujetos pasivos legitimados, lo que a su vez dificulta la ejecución de eventuales sentencias de reparación.

Necesidad de reformas procesales y normativas

Ante este escenario, es indispensable avanzar hacia una reforma del régimen de responsabilidad civil y de las reglas probatorias aplicables a daños causados por IA, que incorpore los siguientes elementos:

- Reversión de la carga de la prueba en favor de las víctimas en contextos de vulnerabilidad tecnológica, inspirada en principios aplicados en el derecho ambiental, donde se exige al presunto causante del daño demostrar su inocuidad. Esta lógica podría trasladarse a casos de afectación a derechos personalísimos mediante inteligencia artificial, donde la víctima no cuenta con los medios técnicos para demostrar la autoría o el funcionamiento del algoritmo y es el desarrollador o la plataforma quien tiene el control del proceso. En este sentido, se invierte la carga probatoria cuando existe una asimetría estructural entre quien sufre el daño y quien tiene los medios para evitarlo o esclarecerlo.
- Establecimiento de un régimen de responsabilidad objetiva o por riesgo tecnológico, inspirado en la noción de productos defectuosos.
- Creación de cuerpos especializados de peritaje forense digital en el sistema judicial para acreditar la existencia y el origen de contenidos manipulados.

- Reconocimiento normativo del daño moral, reputacional y digital como categorías autónomas y compensables.

La acción civil por daños y perjuicios, en su configuración actual, no ofrece una respuesta adecuada frente a los desafíos que plantea el uso de inteligencia artificial en la manipulación de imágenes. Por esta razón, su reforma no solo es recomendable, sino imprescindible para garantizar una reparación integral, conforme a lo dispuesto en el artículo 11.9 de la Constitución de la República del Ecuador, que impone al Estado la obligación de asegurar mecanismos eficaces de restitución, indemnización y garantías de no repetición.

Desafíos procesales y probatorios

Uno de los principales obstáculos para la tutela efectiva del derecho a la imagen en casos de manipulación mediante inteligencia artificial reside en las barreras procesales y probatorias que enfrentan las personas afectadas al recurrir a la jurisdicción ordinaria o constitucional. Estas dificultades no solo limitan el acceso a la justicia, sino que también afectan la posibilidad de obtener una reparación justa, proporcional y oportuna frente a daños causados por tecnologías avanzadas y de compleja trazabilidad. Si bien existen garantías reconocidas en el plano sustantivo (como el derecho a la imagen, la intimidad, la honra o la autodeterminación informativa), su tutela real depende de la posibilidad de activar mecanismos jurisdiccionales que permitan demostrar la existencia del daño, su autoría y la relación causal con una conducta jurídicamente imputable.

En el contexto ecuatoriano, estos procesos enfrentan múltiples barreras estructurales:

a) Carga probatoria desproporcionada para la víctima

El principio general del derecho procesal civil establece que quien alega un hecho debe probarlo (onus probandi incumbit ei qui dicit). En la práctica, esto significa que las víctimas de manipulación digital deben demostrar no solo que la imagen fue alterada, sino también que esa alteración le causó un daño, quién fue el autor, cómo circuló el contenido y cuál fue su afectación real o potencial. Esta exigencia resulta desproporcionada en el entorno digital, donde los algoritmos que generan imágenes sintéticas suelen ser opacos, anónimos y operan desde plataformas transnacionales que no cooperan con los sistemas judiciales locales (De Gregorio, 2021).

Frente a esta realidad, se propone que, en casos donde exista una notoria asimetría tecnológica y la persona afectada no tenga acceso a los medios probatorios relevantes, se permita la reversión de la carga de la prueba, trasladándola a quien haya difundido el contenido o cuente con control sobre la herramienta generadora. Este enfoque ya ha sido reconocido en ámbitos como el derecho ambiental, donde el presunto causante del daño debe probar que su conducta no generó afectación. Aplicado al entorno digital, este principio permitiría equilibrar el acceso a la justicia y asegurar una protección más efectiva de derechos fundamentales como la imagen, la honra o la intimidad.

b) Ausencia de peritos técnicos especializados en IA y contenido sintético

Los órganos judiciales ecuatorianos carecen, en general, de peritos forenses especializados en tecnologías de IA, análisis de metadatos, verificación de deepfakes o trazabilidad digital, lo cual afecta gravemente la producción y valoración de prueba técnica. Esta

carencia no solo limita la posibilidad de probar la existencia del daño, sino también impide que el juzgador comprenda la naturaleza del fenómeno, dificultando la calificación jurídica correcta de los hechos y la atribución de responsabilidad.

c) Problemas de identificación del autor del daño

En casos de manipulación de imágenes mediante IA, el autor material puede ser anónimo, emplear cuentas falsas o utilizar software alojado en servidores en el extranjero. Esta situación complejiza la posibilidad de identificar a un sujeto pasible de responsabilidad civil, penal o constitucional, y vulnera el principio de eficacia de la tutela judicial. A diferencia de los delitos convencionales, la manipulación con IA se caracteriza por una dispersión de actores (creador, difusor, programador, usuario, plataforma), lo que plantea dudas sobre quién debe responder jurídicamente por el daño.

d) Resistencia judicial a aplicar estándares evolutivos de prueba

En el tratamiento judicial de casos vinculados con violencia digital, persiste una tendencia preocupante por parte de ciertos operadores de justicia a mantener criterios probatorios tradicionales, como la exigencia de prueba documental directa o la condición de que exista previamente una sentencia penal condenatoria. Este enfoque resulta inadecuado para abordar situaciones complejas derivadas del uso de tecnologías emergentes, donde la forma en que se configura el daño no siempre se ajusta a las categorías clásicas del derecho probatorio.

La negativa a incorporar medios alternativos de convicción —como la prueba indiciaria, el análisis de contexto o la aplicación de presunciones razonables— limita de forma considerable la eficacia de la tutela judicial. Esta rigidez no solo obstaculiza el acceso efectivo a la justicia,

especialmente para las víctimas, sino que puede perpetuar prácticas institucionales de revictimización. Una interpretación excesivamente formalista del principio de verdad procesal, desconectada de las particularidades propias del entorno digital, contribuye finalmente a consolidar escenarios de impunidad frente a nuevas formas de afectación. En estos contextos, las pruebas materiales pueden ser escasas, volátiles o incluso inmateriales (como ocurre con contenidos digitales eliminados o alojados en servidores extranjeros), pero los efectos jurídicos y psicosociales de la afectación son plenamente verificables. Como advierten Basabe-Serrano y Cobo (2022), resulta urgente que la judicatura ecuatoriana incorpore una lógica probatoria más adaptativa, orientada a la garantía efectiva de derechos fundamentales frente a las nuevas formas de agresión que emergen del uso indiscriminado de tecnologías algorítmicas.

e) Inexistencia de medidas cautelares eficaces para frenar la difusión del contenido

En numerosos casos, las personas afectadas por la difusión de imágenes manipuladas intentan detener su circulación mediante la solicitud de medidas cautelares urgentes, tales como la eliminación de enlaces o la suspensión temporal de cuentas que propagan el contenido. No obstante, tanto en el proceso civil como en la acción de protección, se evidencia una falta de mecanismos tecnológicos eficaces para ejecutar de forma inmediata estas disposiciones, particularmente cuando el material se ha replicado en múltiples plataformas o en redes sociales descentralizadas. Esto contraviene el principio de eficacia del derecho y afecta el contenido esencial del derecho a la imagen.

Nuevos desafíos jurídicos ante contenidos sintéticos y la incertidumbre del régimen de responsabilidad

La irrupción de la inteligencia artificial generativa ha modificado profundamente los procesos de creación, reproducción y manipulación de contenido audiovisual, posibilitando la elaboración de imágenes hiperrealistas que representan a personas reales en contextos completamente fabricados, sin que exista un registro previo ni el consentimiento de los titulares de los datos visuales. Este fenómeno —vinculado principalmente al uso de modelos algorítmicos avanzados como las redes generativas antagónicas (GANs)— plantea desafíos jurídicos inéditos, tanto por la complejidad tecnológica de las herramientas utilizadas como por la multiplicidad de dimensiones en las que puede producir daño: emocional, patrimonial, simbólica y reputacional (Floridi et al., 2018).

Las imágenes generadas sintéticamente, aunque no representen hechos reales, pueden tener un impacto significativo en la vida de las personas. Su difusión masiva es capaz de generar desinformación, erosionar la credibilidad de figuras públicas, provocar conflictos familiares, desencadenar problemas en el ámbito laboral o influir de manera indebida en procesos contractuales o políticos. Cuando estos contenidos incluyen elementos de carácter íntimo, sexual o difamatorio, las consecuencias sobre la dignidad humana y la estabilidad emocional de la persona afectada se intensifican de forma considerable, dando lugar a afectaciones profundas en su esfera personal y social. La evidencia empírica y doctrinal demuestra que estas representaciones, aunque sean técnicamente ficticias, producen efectos tangibles en la esfera personal de quienes son falsamente retratados, generando estigmatización, pérdida de reputación, ansiedad crónica y afectaciones psicológicas severas (Chesney & Citron, 2019, pp. 177–178).

Desde el punto de vista jurídico, estos casos deberían poder encuadrarse en figuras de responsabilidad civil, constitucional o penal. Sin embargo, el ordenamiento jurídico ecuatoriano no contempla normas específicas sobre la creación y difusión de contenidos sintéticos mediante IA. Como ha advertido De Gregorio (2021), en la mayoría de los países latinoamericanos no existe aún una arquitectura regulatoria capaz de abordar adecuadamente la generación de contenidos falsos por medios automatizados.

La estructura clásica de la responsabilidad civil en el Ecuador, regulada en los artículos 2214 y siguientes del Código Civil, exige la existencia de (i) un daño cierto, (ii) una conducta antijurídica, (iii) un nexo causal, y (iv) un sujeto responsable. Sin embargo, este esquema se vuelve disfuncional ante los contenidos generados por algoritmos que actúan de manera autónoma, en redes descentralizadas y mediante plataformas transnacionales que no siempre están sometidas a la jurisdicción ecuatoriana (Mosquera Benalcázar, 2019). A esto se suma la dificultad técnica para identificar a los autores materiales o digitales del daño, lo cual genera un vacío estructural de imputación que pone en riesgo la efectividad del derecho a la reparación (Calo, 2020).

Este vacío ha sido ampliamente discutido en la literatura jurídica contemporánea. Calo (2020) advierte que el modelo antropocéntrico de la responsabilidad jurídica (basado en la existencia de un agente humano plenamente identificable y jurídicamente responsable) no puede responder adecuadamente a los efectos colaterales de los sistemas de IA, lo que exige repensar las bases mismas de la imputación normativa. De allí que se hayan propuesto tres alternativas para responder a este desafío:

1. Responsabilidad objetiva por riesgo tecnológico, en línea con la doctrina de la responsabilidad por actividades peligrosas (Luhmann, 2005), que permitiría imputar responsabilidad al agente que introduce una herramienta de IA en el mercado, sin necesidad de probar culpa. Responsabilidad solidaria en la cadena algorítmica, que permita distribuir la carga de responsabilidad entre programadores, proveedores de IA, plataformas digitales y usuarios que reutilicen o difundan el contenido, siguiendo criterios de razonabilidad y control (González Fuster, 2020).

3. Se propone la creación de un régimen especial de responsabilidad aplicable a los contenidos sintéticos, tomando como referencia los artículos 26 y 28 del Artificial Intelligence Act de la Unión Europea, que imponen obligaciones específicas en materia de transparencia, trazabilidad y deber de diligencia para los sistemas de inteligencia artificial clasificados como de alto riesgo. Este enfoque permitiría establecer parámetros jurídicos claros respecto a la autoría, supervisión y uso de tecnologías generativas que pueden afectar derechos fundamentales.

En ausencia de disposiciones similares en el marco normativo ecuatoriano, la consecuencia práctica ha sido la impunidad frente a los daños ocasionados por contenidos visuales artificiales, incluso cuando estos vulneran de forma demostrable el derecho al honor, la imagen o la integridad emocional de las personas afectadas. Este déficit normativo no solo vulnera el principio de reparación integral establecido en el artículo 11.9 de la Constitución ecuatoriana, sino que también infringe el estándar internacional de diligencia reforzada que deben observar los Estados para proteger a las personas frente a riesgos emergentes derivados de tecnologías disruptivas (UNESCO, 2021).

En conclusión, la manipulación de imágenes mediante IA no puede ser abordada eficazmente por el régimen de responsabilidad vigente en Ecuador, ni desde su vertiente civil, ni desde su tipificación penal actual, ni siquiera desde una lectura conservadora del sistema constitucional. La creación de un marco normativo específico que articule principios de prevención, atribución, remediación y supervisión algorítmica es una tarea impostergable, si se quiere garantizar un mínimo de seguridad jurídica y protección efectiva de los derechos personalísimos en la era digital.

Conclusiones y recomendaciones

A lo largo de este trabajo ha quedado en evidencia que el sistema de justicia ecuatoriano, en lugar de ser un escudo frente a los abusos, se asemeja más a un paraguas roto en medio de una tormenta digital: promete protección, pero deja empapados los derechos fundamentales. Mientras el desarrollo de la inteligencia artificial avanza a un ritmo vertiginoso, el ordenamiento jurídico continúa anclado en estructuras normativas propias de contextos ya superados. En este escenario, la protección de derechos como la imagen, la honra y la intimidad resulta no solo insuficiente, sino marginal frente a la complejidad de los nuevos desafíos tecnológicos.

En sociedades como la ecuatoriana, marcadas por profundas brechas estructurales y una institucionalidad judicial limitada por la burocracia y la falta de especialización, los riesgos asociados al uso indebido de tecnologías emergentes se intensifican y reproducen en cadena, ampliando la distancia entre la garantía formal de derechos y su exigibilidad real. Resulta casi irónico que, en plena era de algoritmos que predicen conductas, sigamos sin predecir cómo proteger a quienes ven su rostro manipulado, su identidad robada y su dignidad arrastrada por un software.

De ahí que el debate no pueda quedar en manos de juristas solitarios que, cual caballeros medievales, combaten dragones tecnológicos con espadas de papel. Se requiere una cruzada interdisciplinaria que convoque también a tecnólogos, comunicadores, psicólogos y filósofos, porque si el derecho no se repiensa, terminará siendo una reliquia en un museo de obsolescencia.

Una de las necesidades más apremiantes en el contexto actual es la reforma sustancial del marco normativo vigente. Pretender enfrentar fenómenos como los deepfakes o la clonación facial mediante disposiciones diseñadas para regular la circulación de fotografías convencionales

representa, en términos jurídicos, una respuesta desfasada frente a desafíos de naturaleza disruptiva. La Ley Orgánica de Protección de Datos Personales requiere una actualización profunda que permita delimitar con claridad los usos legítimos e ilegítimos de la inteligencia artificial, incorporando normas específicas sobre la generación y difusión de imágenes sintéticas. Dicha reforma debería contemplar, entre otros elementos, principios de transparencia algorítmica, consentimiento reforzado y trazabilidad tecnológica.

En el ámbito penal y civil, los mecanismos actuales de tutela permanecen anclados en una lógica tradicional que tiende a subestimar los efectos de los contenidos manipulados digitalmente. La idea de que un daño emocional o reputacional carece de gravedad por no materializarse en un soporte físico resulta anacrónica, especialmente a la luz de la evidencia empírica disponible. Las consecuencias de este tipo de afectaciones pueden incluir trastornos psicológicos, exclusión social, estigmatización pública y pérdida de oportunidades profesionales. Ignorar esta realidad equivale a desatender la dimensión humana de los daños causados en entornos digitales.

El derecho a la imagen no puede ser concebido como una figura menor o anecdótica. Se trata de una manifestación concreta de la dignidad humana, cuya protección exige una respuesta jurídica acorde a los riesgos contemporáneos. Minimizar su importancia o abordarla con categorías obsoletas es, en última instancia, renunciar a la función protectora que justifica la existencia del derecho en un entorno crecientemente mediado por algoritmos.

Asimismo, urge debatir el rol de las entidades virtuales y los sistemas inteligentes en la producción de daño. Aunque aún no les otorgamos derechos, sí deberíamos empezar a exigir responsabilidades. Porque si el cuchillo no tiene culpa, ¿quién responde cuando alguien lo lanza?

Diseñadores, usuarios y plataformas no pueden seguir amparados en la ficción de la neutralidad técnica mientras circulan contenidos que destrozan reputaciones y psiquis.

a ciencia jurídica debe actualizar sus categorías y marcos de análisis, no para someterse pasivamente al avance tecnológico como si este fuera una fuerza incuestionable, sino para asegurar que la persona humana no sea reducida a una línea de código perdida en el sistema de una legalidad indiferente. El derecho debe preservar su capacidad crítica y garantista frente a los nuevos poderes que configuran la vida social en entornos digitales.

En este contexto, abrir espacios para la construcción colectiva de nuevas reglas no es un gesto voluntarista, sino una exigencia impostergable. La inteligencia artificial puede convertirse en instrumento de creación o de exclusión, de reparación o de violencia. Su impacto dependerá de quién la utilice, en qué condiciones, con qué límites normativos y conforme a qué principios éticos y constitucionales.

Referencias

Andruet, A., Cesano, J., Carranza, G., Arias, A., Ciuro, M., Estigarribia, M., Shwoihort, S., Márquez, J., Richard, E., Sala, J., Saux, E., Sahaín, J., Martino, A., Silva, P., & Sobre Casas, R., (2022), Impactos y alcances de la inteligencia artificial en el derecho y en el derecho judicial, Ciudad Autónoma de Buenos Aires: La Ley; Córdoba: Academia Nacional de Derecho y Ciencias Sociales de Córdoba.

Asamblea Nacional del Ecuador, (2005), Código Civil de la República del Ecuador, Registro Oficial Suplemento 46, 24 de junio de 2005.

Asamblea Nacional del Ecuador, (2008), Constitución de la República del Ecuador, Registro Oficial Suplemento 449.

Asamblea Nacional del Ecuador, Constitución de la República del Ecuador, Montecristi, 2008.

Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459, 26 de mayo de 2021.

Basabe-Serrano, S., & Cobo, P., (2022), La acción de protección y el sistema de justicia constitucional en Ecuador: entre la promesa y la realidad, Revista Ecuatoriana de Derecho Constitucional, (10), 13–35.

Boaventura, S., (2009), Una epistemología del sur: la reinvención del conocimiento y la emancipación social, Siglo XXI Editores.

Boediman, E. P., (2025), Exploring the impact of deepfake technology on public trust and media manipulation: A scoping review. Jurnal Komunikasi, 1(1). .

Bradshaw, S., & Howard, P., (2023), Industrialized Disinformation: 2023 Global Inventory, Oxford Internet Institute.

Calo, R., (2020), Artificial Intelligence Policy: A Primer and Roadmap, UC Davis Law Review, 51(2), 399–435.

Carrillo, M., (2007), El derecho a la propia imagen como derecho autónomo, Revista Chilena de Derecho, 34(2), 45–70. .

Chesney, R., & Citron, D. K., (2019), Deep fakes: A looming challenge for privacy, democracy, and national security, California Law Review, 107, 1753–1819.

Chesney, R., & Citron, D., (2019), Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, 107(6), 1753–1819.

Consejo de Europa, (2020), Recommendation CM/Rec, On the human rights impacts of algorithmic systems, Estrasburgo: Council of Europe, 2020.

Constitución de la República del Ecuador, (2008).

Corral, I., (2021), El principio de legalidad penal frente a las nuevas tecnologías, Revista de Estudios Penales.

Corte Constitucional del Ecuador, (2013), Sentencia No. 002-13-SAN-CC (Caso No. 0045-11-AN), Quito, 14 de mayo de 2013.

Corte Constitucional del Ecuador, (2019), Sentencia No. 11-18-CN/19, Caso sobre control de constitucionalidad de la Ley Orgánica Reformatoria a la Ley Orgánica de Comunicación.

Corte Constitucional del Ecuador, (2022), Sentencia No. 2032-20-JP/25 (Caso No. 2032-20-JP), Quito, 14 de diciembre de 2022.

Corte Constitucional del Ecuador, Constitución de la República del Ecuador. Montecristi, 2008.

Corte Constitucional del Ecuador. Sentencia No. 198-17-SEP-CC. Quito, 2017.

Corte Interamericana de Derechos Humanos, (2012, 3 de septiembre), Caso Vélez Restrepo y Familiares vs. Colombia (Serie C No. 248, Excepción Preliminar, Fondo, Reparaciones y Costas), párr. 263.

Corte Interamericana de Derechos Humanos, (2017), Opinión Consultiva OC-24/17: Entorno Digital y Libertad de Expresión.

Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-24/17, Entorno Digital y Libertad de Expresión, San José: Corte IDH, 2017.

De Gregorio, G., (2021), Digital constitutionalism in a global society. International Journal of Constitutional Law, 19(1), 146–178.

De Gregorio, G., (2021), The rise of digital constitutionalism in the European Union, International Journal of Constitutional Law, 19(1), 41–70.

DeepMind, (2025), Veo.

Dejusticia, (2022), Reconocimiento facial y DD.HH: 13 historias para entender sus implicaciones.

Eco, U., (2000), Tratado de Semiótica General, Barcelona, Editorial Lumen S.A., Quinta Edición.

EU Parliament, (2023), Tackling Deepfakes in Electoral Contexts, Policy Department for Citizens Rights and Constitutional Affairs.

Floridi, L., Cowls, J., & Beltrametti, M., (2018), AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations, Minds and Machines, 28(4), 689–707.

Fontaine, Guillaume, Sánchez, E., Córdova, M., & Velasco, S., The Politics of Accountability: Indigenous Participation in Colombian and Ecuadorian Oil and Gas Policies, Colombia Internacional 86 (2016): 17–50.

Fundamedios, (2021), La videovigilancia en Ecuador vulnera derechos ciudadanos.

Goffman, E., (1981), La presentación de la persona en la vida cotidiana, Buenos Aires, Amorrourtu editores, primera edición en castellano.

Goffman, E., (2006), Estigma: La identidad deteriorada, Buenos Aires, Amorrourtu editores.

González Fuster, G., (2020), The Emergence of Artificial Intelligence Regulation: A European Perspective, Brussels Privacy Hub.

Guerra, D., Neiva, J., Pabón, L., Vargas, O., Bonet, J., Ramírez, D., Bujosa, L., Meroi, A., Cárdenas, O., Rangel, D., Rivera, R., Yañez, D., Alarcón, A., Ramírez López, D., & Diaz, A, (2022), Constitución e inteligencia artificial en el proceso, Cúcuta, Universidad Libre -Cúcuta-, Revista Academia & Derecho. .

Human Rights Watch, (2023), Es hora de prohibir el reconocimiento facial en espacios públicos y fronteras.

Koch, T., & Padovani, C., (2023), AI, Imagery and Truth: The Disinformation Challenge. Ethics and Information Technology, 25(1), 1–17.

Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459, 26 de mayo de 2021.

Luhmann, N., (2005), Sociología del riesgo, Madrid: Trotta.

Martínez Hernández, D. F., (2021), Inteligencia artificial, derecho penal y Compliance, Revista Mexicana de Ciencias Penales, 4 (14), 63–70.

Martínez, A., Tradición democrática y sobrevivencia presidencial: el caso de Lucio Gutiérrez en Ecuador. Revista Ecuatoriana de Ciencia Política 1, no. 2 (2022): 44–66.

Morán, A., (2021), Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera?, Revista Del Instituto De Ciencias Jurídicas De Puebla, México. E-ISSN 1870-2147. Nueva Época Vol. 15, No. 48. Recuperado de: <https://www.denoticias.es/notas/> inteligencia-artificial-revienta-el-fraude-del-crimen-en-silicon-valley.html.

Mosquera Benalcázar, F., (2019), Responsabilidad civil en el Ecuador: fundamentos y jurisprudencia, Quito: Ediciones Legales.

NATO, (2022), Countering Hybrid Threats: Emerging Technologies and Disinformation.

Pisarello, G., (2001), Ferrajoli y los derechos fundamentales: ¿qué garantías?, Revista de Derecho Constitucional e Internacional, (volumen y número por completar).

Poncio de la Fuente, H. P., Pracedes, M. Z., & Castrejón, V. M., (2024), El uso ilícito de las técnicas de inteligencia artificial y la necesidad de su regulación: el deepfake. Vniversitas, 73.

Qu, Y., Shen, X., He, X., Backes, M., Zannettou, S., & Zhang, Y., (2023), Unsafe Diffusion: On the Generation of Unsafe Images and Hateful Memes From Text-To-Image Models, arXiv.

Quito-Guerrero, P. M., & Zamora Vázquez, A. F., (2025), La tutela judicial efectiva en la ejecución de las acciones de protección en el cantón Cuenca durante el año 2022, Revista Región, 10(46), e2501480.

Reglamento General de Protección de Datos (RGPD), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Russell, S. J., & Norvig, P., (2021), Artificial Intelligence: A Modern Approach, (4ª ed., p. 4), Pearson, .

Silva Sánchez, J., (2020), La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales, (13ª ed.), Tirant lo Blanch.

Tzanou, M., (2017), The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance, Oxford: Hart Publishing.

UNESCO, (2021), Recomendación sobre la ética de la inteligencia artificial.

Univision, (2025), El video del canguro que abordaba un avión no es real: fue generado por IA.

Xataka, (2025), DALL·E: qué es, cómo funciona y cómo puedes utilizar esta inteligencia artificial para crear imágenes.

Zhang, Y., Gopalan, N., & Narayanan, A., (2022), Who is at Risk of Being Deepfaked? Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), 1–23.

Zuboff, S., (2019), The Age of Surveillance Capitalism, PublicAffairs.