

UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO

FACULTAD DE DERECHO, POLÍTICA Y DESARROLLO

TÍTULO: GARANTÍAS JURÍDICAS FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DIGITAL MEDIANTE INTELIGENCIA ARTIFICIAL EN ECUADOR

TRABAJO DE TITULACIÓN QUE SE PRESENTA COMO REQUISITO PREVIO A OPTAR EL GRADO DE ABOGADO

NOMBRE DEL ESTUDIANTE:

BERTHA PAULINE TIMM DUQUE

NOMBRE DEL TUTOR:

AB. ENRIQUE EFRAÍN ARGÜELLO ARELLANO, MSC.

SAMBORONDÓN, JULIO, 2026

GARANTÍAS JURÍDICAS FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DIGITAL MEDIANTE INTELIGENCIA ARTIFICIAL EN ECUADOR

CARTA DE APROBACIÓN DEL TUTOR

En mi calidad de tutor de BERTHA PAULINE TIMM DUQUE, estudiante de la Facultad de Derecho, Política y Desarrollo de la Universidad de Especialidades Espíritu Santo,

CERTIFICO

Que, una vez analizado el trabajo de titulación titulado **"GARANTÍAS JURÍDICAS FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DIGITAL MEDIANTE INTELIGENCIA ARTIFICIAL EN ECUADOR"**, presentado como requisito previo a obtener el grado de Abogado, el mismo cumple con los requisitos y méritos académicos, razón por la cual lo **APRUEBO** en su totalidad.

AB. ENRIQUE EFRAÍN ARGÜELLO ARELLANO, MSC.

TUTOR

GARANTÍAS JURÍDICAS FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DIGITAL MEDIANTE INTELIGENCIA ARTIFICIAL EN ECUADOR

INFORMACIÓN DEL AUTOR

Apellidos y nombres: Timm Duque, Bertha Pauline

Universidad de Especialidades Espíritu Santo – Ecuador (UESS)

Correo institucional: btimm@uees.edu.ec

Dirección de correspondencia: Facultad de Derecho Edificio P, Universidad Espíritu Santo, Km. 2.5 Vía Puntilla Samborondón.

GARANTÍAS JURÍDICAS FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DIGITAL MEDIANTE INTELIGENCIA ARTIFICIAL EN ECUADOR

Resumen

Tras identificar que el ordenamiento jurídico ecuatoriano no contempla mecanismos específicos para prevenir, identificar y sancionar la suplantación de identidad digital realizada mediante inteligencia artificial generativa y la manipulación de datos biométricos sintéticos, se ha desarrollado la presente investigación para analizar la suficiencia de las garantías jurídicas ecuatorianas en tal ámbito, con el fin de identificar vacíos normativos y proponer mecanismos jurídicos que fortalezcan su protección. A través de un estudio cualitativo que se valió del método inductivo-deductivo y la técnica de revisión documental, se constató que la arquitectura técnica de la inteligencia artificial generativa diluye los principios clásicos de la imputación de responsabilidad jurídica. Se concluye que el ordenamiento jurídico actual tiene una limitada eficacia frente al fraude biométrico por problemas de tipicidad y competencia administrativa. Asimismo, las garantías jurisdiccionales resultan inviables frente a la falta de una base de datos centralizada o de un legitimado pasivo identificable en redes cifradas y el delito de suplantación de identidad no protege contra la instrumentalización algorítmica de la inteligencia artificial generativa, todo lo cual determina la necesidad de reformas jurídicas en tales direcciones.

Palabras clave: Dato biométrico sintético, inteligencia artificial, suplantación de identidad.

GARANTÍAS JURÍDICAS FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DIGITAL MEDIANTE INTELIGENCIA ARTIFICIAL EN ECUADOR

Abstract

After identifying that the Ecuadorian legal framework lacks specific mechanisms to prevent, detect, and penalize digital identity theft carried out via generative artificial intelligence and the manipulation of synthetic biometric data, this research was conducted to analyze the adequacy of Ecuadorian legal safeguards in this area. The aim was to identify regulatory gaps and propose legal mechanisms to strengthen protection. Through a qualitative study employing the inductive-deductive method and a documentary review, it was found that the technical architecture of generative artificial intelligence dilutes classical principles regarding the attribution of legal liability. The study concludes that the current legal framework has limited effectiveness against biometric fraud due to issues concerning the definition of offenses and administrative jurisdiction. Furthermore, judicial safeguards prove unfeasible given the absence of a centralized database or an identifiable defendant within encrypted networks, and the crime of identity theft fails to protect against the algorithmic instrumentalization of generative artificial intelligence; all of which underscores the need for legal reforms in these areas.

Keywords: Synthetic biometric data, artificial intelligence, identity theft.

GARANTÍAS JURÍDICAS FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DIGITAL MEDIANTE INTELIGENCIA ARTIFICIAL EN ECUADOR

Índice

CARTA DE APROBACIÓN DEL TUTOR 1

INFORMACIÓN DEL AUTOR 2

Resumen 3

Abstract 4

Índice 5

Introducción 6

1. Marco normativo 9

2. Garantías constitucionales y legales para la protección de la identidad digital 13

3. Inteligencia artificial generativa y riesgos jurídicos 16

4. Insuficiencias del ordenamiento jurídico ecuatoriano 19

Conclusiones 23

Recomendaciones 24

Bibliografía 29

Introducción

La estructura conceptual de la Constitución de la República del Ecuador (en adelante, CRE) y la Ley Orgánica de Protección de Datos Personales (en adelante, LOPDP) concibe intrínsecamente que el dato personal es siempre un rastro o evidencia material dejada por un sujeto real. Otras normas como el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación regulan el derecho a la propiedad intelectual, pero no comprenden precisiones sobre la identidad digital en las obras humanas, menos aún en cuanto a la inteligencia artificial y los problemas jurídicos asociados a la creación o manipulación de contenidos que esta puede realizar[1].

El avance de la inteligencia artificial generativa (en adelante, IAGEN) ha roto el paradigma de integridad del dato al desvincular inclusive el dato biométrico de la presencia física del titular; esto se produce a través de la síntesis digital, por lo que se habla actualmente del dato biométrico sintético como una nueva categoría con un notable impacto jurídico[2]. Estas inquietudes son relevantes porque sitúan el eje de preocupación en la posibilidad de la suplantación de la identidad digital no solo por personas físicas, sino por entidades digitales avanzadas como la propia IAGEN.

El problema se acentúa cuando se observa que la IAGEN no puede constreñirse fácilmente a un espacio material o territorio concreto. El análisis del régimen de

[1] Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, 29 de noviembre de 2016 (Registro Oficial Suplemento No. 899, 9 de diciembre de 2016).
[2] ALDAWSARI, Hamad y ALAMMAR, Saad, "Integrating explainable AI with synthetic biometric data for enhanced image synthesis and privacy in computer vision systems" en *Image and Vision Computing*, vol. 162, 2025, DOI https://doi.org/10.1016/j.imavis.2025.105726 consultado 27/06/2026.

transferencias y flujos transfronterizos de datos tiene características regulatorias propias en la LOPDP, la que determina las directrices y responsabilidades para garantizar que dichas transferencias sean lícitas y establece niveles de protección y exigencias complementarias para asegurar la indemnidad de los datos transmitidos[3]. Sin embargo, la recreación de imágenes, voces o datos biométricos sintéticos producidos por la IAGEN no queda establecida, en especial porque las herramientas de esta operan de manera descentralizada y fragmentan la información a través de las jurisdicciones territoriales del mundo[4].

En síntesis, se establece como hipótesis que el ordenamiento jurídico ecuatoriano no contempla mecanismos específicos para prevenir, identificar y sancionar la suplantación de identidad digital realizada mediante IAGEN a través de la recreación de imágenes, voces o datos biométricos sintéticos. Esta ausencia normativa evidencia un vacío jurídico que puede afectar la protección efectiva de la identidad digital y los derechos de las personas frente a nuevas formas de suplantación tecnológica, por lo que se plantea como pregunta de investigación si: ¿son suficientes las garantías constitucionales y legales vigentes en Ecuador para proteger la identidad digital frente a la suplantación realizada mediante inteligencia artificial generativa?

El objetivo general de la presente investigación consiste en analizar la suficiencia de las garantías jurídicas ecuatorianas para proteger la identidad digital frente a la

[3] Arts. 55-60 Ley Orgánica de Protección de Datos Personales, 21 de mayo de 2021 (Registro Oficial Quinto Suplemento No. 459, 26 de mayo de 2021) (LOPDP).

[4] ABBAS, Fakhar et al., "Building trust in the generative AI era: a systematic review of global regulatory frameworks to combat the risks of mis-, dis-, and mal-information" en *AI & Society*, No. 41, 2026, DOI https://doi.org/10.1007/s00146-025-02698-9 consultado 27/06/2026.

suplantación realizada mediante inteligencia artificial generativa, con el fin de identificar vacíos normativos y proponer mecanismos jurídicos que fortalezcan su protección. Para su desarrollo, se trazan como objetivos específicos los siguientes: 1) examinar las garantías constitucionales y legales relacionadas con la protección de datos personales, identidad digital y derechos de la personalidad en Ecuador; 2) determinar los riesgos jurídicos derivados de la utilización de inteligencia artificial generativa para la recreación de imágenes, voces y otros datos biométricos; 3) identificar las insuficiencias del ordenamiento jurídico ecuatoriano frente a los supuestos de suplantación de identidad digital mediante inteligencia artificial; y 4) proponer mecanismos jurídicos orientados a fortalecer la protección de la identidad digital frente a nuevas formas de suplantación tecnológica.

El estudio se sustenta en un enfoque cualitativo orientado a determinar la suficiencia de las garantías constitucionales y legales vigentes en el Ecuador para proteger la identidad digital. A su vez, se examinan las implicaciones derivadas de la ausencia de una regulación específica para prevenir, identificar y sancionar la suplantación de identidad realizada mediante IAGEN. Se privilegian, en este sentido, los análisis doctrinales, jurisprudenciales y normativos del vacío jurídico identificado, evaluando críticamente el desfase entre el avance tecnológico algorítmico y el ordenamiento jurídico ecuatoriano.

El método de investigación utilizado es el inductivo-deductivo. Este permite examinar profundamente las disposiciones jurídicas nacionales junto con los criterios doctrinales contemporáneos sobre aprendizaje profundo o *deep learning*, a fin de deducir las vulneraciones de derechos derivadas de la simulación de la existencia

humana. A partir de estas premisas generales, se proyectan soluciones y mecanismos jurídicos específicos enfocados en mitigar los riesgos de la suplantación de identidad digital por la IAGEN. La técnica empleada es la de revisión documental, mediante la cual se analizan fuentes normativas y bibliográficas para construir una argumentación crítica sólida que sustente la pertinencia de la propuesta.

1. Marco normativo

El análisis de suficiencia jurídica en el contexto actual exige desentrañar la articulación jerárquica de nuestro ordenamiento, desde los mandatos constitucionales hasta la regulación infraconstitucional y las lógicas de aplicación transfronteriza de los datos personales. A continuación, se examina críticamente cómo la CRE y la LOPDP configuran un escudo protector de la intimidad y los datos biométricos que, pese a su amplitud teórica, empieza a exhibir grietas y limitaciones operativas frente a los riesgos emergentes de la IAGEN.

La protección constitucional en materia de derechos relacionados con la identidad digital encuentra en el artículo 66 numeral 19 de la CRE una regulación trascendente[5]. A través de esta norma se eleva a rango de derecho fundamental la protección de datos de carácter personal, lo que incluye el acceso y la decisión sobre la información de esta naturaleza. Aunque la CRE no indica expresamente el término digital en dicha norma, la Corte Constitucional del Ecuador (en adelante, CCE) ha interpretado que el marco de protección es independiente del medio donde se encuentren los datos o informaciones objeto de tutela jurídica, por lo que

[5] Art. 66.19. Constitución de la República del Ecuador (Registro Oficial No. 449 de 20 de octubre de 2008) (CRE).

la protección digital cae también dentro del ámbito mencionado[6].

No escapa al análisis, sin embargo, que la construcción constitucional se diseñó en la era anterior a la IAGEN. La norma concibe el dato como una unidad de información estática alojada en archivos o bases de datos, pero no abarca la dimensión dinámica y predictiva que adquieren, por ejemplo, los datos biométricos cuando son procesados, replicados o sintetizados mediante algoritmos de aprendizaje profundo o *deep learning*[7].

Por su parte, el artículo 66 numeral 20 de la CRE garantiza el derecho a la intimidad personal y familiar[8]. La doctrina constitucional más avanzada coincide en que la intimidad es el núcleo duro sobre el cual se erige la identidad digital y su esfera de protección[9]. Así, al producirse una suplantación de identidad mediante *deepfakes* de voz o imagen, no solo se vulnera el derecho a la información y a la protección de datos personales, sino también a la identidad. Ello se debe a que hay una clara intromisión en la esfera íntima de la persona que distorsiona la percepción social de esta.

En el plano infraconstitucional, la LOPDP ha materializado los mandatos constitucionales sobre protección de datos personales, información e identidad digital con mayor amplitud. El artículo 4 de dicha Ley introdujo definiciones normativas cruciales, como la de datos biométricos, datos sensibles, entre otras. De hecho, los

[6] Sentencia de la Corte Constitucional (SCC), 27 de enero de 2021 (2064-14-EP, Ponente: Carmen Corral Ponce), párr. 77.
[7] CORVALÁN, Juan Gustavo et al., *Licenciamiento de IAGen y Protección de Datos. Un análisis comparativo de riesgos y garantías desde una perspectiva de gobernanza*, 2026.
[8] Art. 66.20. CRE.
[9] SOLER MARTÍNEZ, José Antonio, "Protección constitucional de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías" en *Anuario de Derecho Canónico*, No. 11, 2022, URL https://dialnet.unirioja.es/descarga/articulo/8661053.pdf consultado 27/06/2026.

datos biométricos se consideran una categoría dentro de los datos sensibles, pues son aquellos obtenidos a través de un tratamiento técnicos específico relativo a las características físicas, marcadores biológicos o conductuales de una persona[10].

Los datos sensibles, en general, son una categoría especial de los datos personales[11]. Su tratamiento está prohibido, salvo que concurra alguna de las circunstancias que dispensa la Ley; entre ellas, se encuentran: a) el consentimiento expreso del titular, con conocimiento de finalidad del tratamiento; b) el cumplimiento de obligaciones y el ejercicio de derechos en el ámbito laboral y de seguridad social; c) la protección de intereses vitales; d) la preexistencia de publicidad del dato hecha por su titular; e) la autorización judicial; f) el interés público, científico, histórico o estadístico; g) razones de salud debidamente justificadas[12].

Sin embargo, la LOPDP no alcanzó a definir ni regular el estatus jurídico de los datos biométricos sintéticos, que son creados artificialmente por una IAGEN y emulan perfectamente a los originales[13]. La regulación sobre la recolección, el almacenamiento y el tratamiento de datos reales se ha establecido en un plazo distinto al físico, pero en un ecosistema digital de almacenamiento tradicional. La misma interrogante sobre las *deepfakes* esbozada en líneas anteriores queda sin respuesta jurídica clara tampoco en la Ley.

La transferencia internacional de datos personales es una situación regulada en la LOPDP. En general, propende a que se garantice la protección de dichos datos por

[10] Art. 4 LOPDP.
[11] Art. 25 LOPDP.
[12] Art. 26 LOPDP.
[13] ALDAWSARI & ALAMMAR, "Integrating explainable AI with synthetic biometric data for enhanced image synthesis and privacy in computer vision systems".

su condición de derecho fundamental[14], para lo cual la Autoridad de Protección de Datos Personales en Ecuador tiene identificados los países, organizaciones y personas jurídicas que brindan niveles adecuados para que dichos actos se ejecuten[15]. Cuando la transferencia se pretende realizar a otro ente no precalificado, es necesaria la suscripción de un convenio con rigurosos estándares de protección y con rango de norma vinculante entre partes[16], lo que será verificado por la Autoridad indicada previo a su aprobación[17]. En su defecto, podrán darse situaciones excepcionales como el consentimiento expreso del titular de los datos, el cumplimiento de obligaciones legales, la cooperación judicial internacional, entre otros[18].

Pero el problema con la IAGEN es más complejo, porque esta actúa transfiriendo normalmente datos a través de las fronteras y en servidores ubicados en distintos países[19], los que pueden estar, o no, dentro de la lista de la Autoridad de Protección de Datos Personales. Esto implica que las regulaciones contenidas en la LOPDP son insuficientes para establecer límites de legalidad o seguridad jurídica frente a los titulares de los datos personales, además de que las regulaciones específicas sobre inteligencia artificial en Ecuador son muy incipientes.

En general, el marco normativo ecuatoriano es anacrónico respecto al desarrollo tecnológico actual, especialmente en el manejo de la IAGEN y la protección de

[14] Art. 55 LOPDP.
[15] Art. 56 LOPDP.
[16] Art. 57 LOPDP.
[17] Art. 59 LOPDP.
[18] Art. 60 LOPDP.
[19] NIEVA FENOLL, Jordi, "Inteligencia artificial generativa (IAGEN) y defensa: ¿cómo lograr la "convicción" de una máquina?" en *Revista Ítalo-Española de Derecho Procesal*, vol. 32, No. 4, 2025, DOI https://doi.org/10.37417/rivitsproc/3204 consultado 28/06/2026.

los datos biométricos. La suplantación de identidad a través de la IAGEN o, incluso, la mera alteración de los datos biométricos de la persona por la tecnología puede dar lugar a delitos conexos como estafa o generar un daño reputacional, lo cual es contrario al derecho a la intimidad. La escasez regulatoria es nociva para la adecuada protección de los derechos constitucionales relacionados con los datos personales, en su dimensión digital.

2. Garantías constitucionales y legales para la protección de la identidad digital

Teniendo en cuenta que las garantías constitucionales y legales son herramientas procesales e institucionales diseñadas para prevenir la vulneración de derechos y, en su caso, reparar el daño causado, es necesario caracterizar el alcance efectivo de estas para la protección de la identidad digital en el ámbito estudiado. Por ello, se hace referencia sucinta a continuación a las garantías jurisdiccionales y los mecanismos administrativos de protección del problema de la suplantación de identidad a través de la IAGEN en Ecuador.

La garantía jurisdiccional por excelencia para la tutela de los datos personales es la acción de hábeas data[20]. Su objeto fundamental es garantizar el acceso a documentos, datos genéticos, bancos de datos o informes que sobre la persona que reclama tengan las instituciones públicas u otras personas naturales o jurídicas, al igual que poder solicitar su actualización, rectificación, eliminación o anulación, según corresponda; dichos datos pueden hallarse en cualquier soporte material o electrónico.

[20] Art 92 CRE.

Visto así, el hábeas data es una garantía jurisdiccional de carácter reactivo, limitada a los supuestos constitucional o legalmente permitidos en relación con los datos o informaciones personales. Si bien la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional amplió su ámbito tutelar a la reclamación contra el uso de la información personal en violación de un derecho constitucional[21], la lógica procesal implica la determinación de quien lo haya hecho como legitimado pasivo, por lo que constituye un obstáculo notable si la violación se da por intervención de la IAGEN. Así, en un supuesto de suplantación de identidad mediante un *deepfake* que se viraliza de forma instantánea en redes sociales de mensajería cifrada, el hábeas data resulta procesalmente inútil, pues no existe una base de datos centralizada a la cual demandar, ni es posible identificar en fases iniciales quién ostenta el control del algoritmo origen.

Ante las limitaciones del hábeas data, podría pensarse que la acción de protección[22] es una garantía adecuada cuando el marco de aquella impide incoarla. Se alude para ello que la suplantación de la identidad digital por la IAGEN es una vulneración directa, grave e inminente de derechos constitucionales como la honra, la dignidad y la propia imagen, pero subsiste en definitiva el mismo problema en cuanto a quién dirigir la demanda. Además, la acción de protección solo procede si la vulneración de derechos no está protegida por otra garantía jurisdiccional – como el hábeas data[23] – por lo cual su viabilidad es casi nula.

[21] Art. 50.3. Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 10 de septiembre de 2009 (Registro Oficial Segundo Suplemento No. 52, 22 de octubre de 2009).
[22] Art. 88 CRE.
[23] Art. 39 LOGJCC.

Al margen de las disyuntivas anteriores, el problema principal de las garantías jurisdiccionales en este sentido es que puede reparar la violación padecida, pero no resuelve el problema jurídico de la titularidad del daño y los aspectos indemnizatorios propios de ello, ni asegura la eliminación definitiva del dato a partir del modelo fundacional de la IAGEN – que aprendió de los datos biométricos de la víctima para actos futuros que pueden estar asociados a ella, o no[24] – pues es asunto que compete a la justicia ordinaria.

En la esfera administrativa, la LOPDP instituyó la Superintendencia de Protección de Datos como entidad encargada de supervisar, controlar y sancionar el incumplimiento de las obligaciones de los responsables y encargados del tratamiento de datos. Los procedimientos administrativos que pueden incoarse por los afectados son de una utilidad profiláctica innegable, ya que se pueden emitir medidas cautelares de suspensión de tratamiento de datos[25], entre otras, pero el vacío de directrices técnicas sobre la IAGEN en Ecuador vuelve precario el sistema de protección. La Superintendencia puede sancionar a un banco de datos local que use indebidamente la huella digital de un usuario, pero se encuentra limitada cuando intenta fiscalizar plataformas internacionales que ofrecen servicios complejos de manejo de datos biométricos – como la clonación de voz en línea con un simple registro de correo electrónico[26] –, lo que deviene en una garantía de baja intensidad para el ciudadano común.

[24] JIMÉNEZ CASTELLANOS BALLESTEROS, Inmaculada, "La difícil convivencia entre la inteligencia artificial y los derechos fundamentales: la tecnología *deepfake*" en FEBLES POZO, Nayiber (Dir.) y NIETO ROJAS, Patricia (Dir.), *Inteligencia artificial y protección de datos: desafíos en la era digital*, 2025.
[25] Art. 19 LOPDP.
[26] UYÁ URREA, Virginia, *Clonación de voz mediante Inteligencia Artificial en el sector del doblaje: desafíos jurídicos y perspectivas regulatorias*, 2024.

Como se observa, la identidad digital vulnerada por la IAGEN se desplaza en dimensiones intangibles y en una globalización que elude los marcos tradicionales de protección jurídica basada en el territorio o la persona. Por ende, ni las garantías jurisdiccionales ni los procedimientos administrativos son suficientes porque fueron concebidos para proteger al individuo frente a abusos de terceros entendidos como personas naturales o jurídicas, pero no para resguardarlo de la simulación de la existencia humana controlada por algoritmos.

3. Inteligencia artificial generativa y riesgos jurídicos

El examen de los riesgos jurídicos de la IAGEN exige comprender, en primer término, la infraestructura técnica que viabiliza la simulación antropomórfica de las características humanas. A continuación, se analiza cómo la sofisticación de los algoritmos capaces de clonar datos biométricos de manera casi indetectable afecta la determinación de la responsabilidad y desborda la capacidad de respuesta desde una perspectiva normativa.

En el ámbito operativo, la IAGEN se define como aquel conjunto de metodologías y aplicaciones capaces de generar contenidos con propiedades virtualmente indistinguibles de aquellas producidas por el ser humano[27]. Aunque este adelanto tecnológico reviste capacidades altamente disruptivas, también supone desafíos en el orden legal. El riego jurídico principal no estriba en la tecnología *per se*, sino en

[27] GARCÍA LLAMAS, Juan José, "Inteligencia Artificial Generativa (IAG). El nuevo paradigma en el diseño y producción de contenido" en GARCÍA MACÍAS, José Antonio (Coord.) et al., *Inteligencia artificial. Transformación, retos y prospectiva social*, 2024.

la asimetría que existe entre su capacidad de simulación y las herramientas diseñadas para validar la autenticidad de los sujetos[28]. De esa forma, cuando las características humanas pueden replicarse sintéticamente, los conceptos clásicos de identidad y verdad jurídica entran en una crisis frente a la necesidad de acreditación de la identidad.

Para comprender la magnitud de los riesgos jurídicos asociados a la suplantación de identidad, es necesario examinar en sus bases la arquitectura del aprendizaje automático o *machine learning*. Este subcampo de la inteligencia artificial simula el comportamiento cognitivo humano para resolver tareas a través de los aprendizajes supervisado y no supervisado. El primero se fundamenta en el conjunto de datos previamente etiquetados por un programador, donde cada entrada de datos o información tiene una salida prevista como respuesta correcta; el segundo, en cambio, opera sobre datos no etiquetados y obliga al algoritmo a identificar patrones subyacentes de manera autónoma[29].

Los modelos generativos contemporáneos generalmente hibridan ambas técnicas. Esto dota a la IAGEN de una plasticidad y autonomía que dificulta la trazabilidad del proceso de origen[30], lo que incide en la dilución de la responsabilidad de los programadores frente a resultados potencialmente lesivos que pueden generar sus sistemas.

[28] ZARABOZO, Pedro Manuel, "La propiedad intelectual en la era de la Inteligencia Artificial Generativa: desafíos normativos, nuevas formas de creación y sus implicancias en el ejercicio profesional jurídico" en ZÁRATE, Hilda (Dir.) et al., *Cuadernos de Posgrado 2025*, 2026.
[29] JANIESCH, Christian et al., "Machine learning and deep learning" en *Electronic Markets*, No. 12525, 2021, DOI https://doi.org/10.1007/s12525-021-00475-2 consultado 29/06/2026.
[30] AHSAN, Nafis et al., "Generative Modeling in Smart Manufacturing: Applications, Challenges, and Future Directions" en *Manufacturing Letters*, No. 44, 2025, DOI https://doi.org/10.1016/j.mfglet.2025.06.148 consultado 29/06/2026.

Dentro de esta infraestructura, la doctrina especializada destaca tres pilares técnicos determinantes de la recreación biométrica: el aprendizaje profundo sobre redes neuronales o *deep learning*, las redes generativas adversarias y los autocodificadores variacionales. Las segundas resultan particularmente críticas para el problema de investigación, ya que operan mediante un juego de suma cero entre dos redes neuronales internas: una generadora, que fabrica datos sintéticos – como un rostro o fragmento de voz – y otra discriminadora, que evalúa de forma estricta si dicha información pertenece al mundo real o es un producto virtual, lo que le permite entrenarse a sí misma hasta que el fraude es casi indetectable[31].

Frente a estos escenarios riesgosos, los organismos internacionales han tratado de estructurar las bases regulatorias internacionales. Por ejemplo, la Organización para la Cooperación y el Desarrollo Económico, en su Recomendación revisada del Consejo sobre Inteligencia Artificial, ha diseñado principios orientados a la gestión responsable, exigiendo que la inversión científica e institucional en inteligencia artificial no descuide las profundas implicaciones ético-legales del sistema[32]. Europa se ha posicionado como vanguardia normativa a través de su Reglamento de Inteligencia Artificial, que cataloga a los sistemas de identificación biométrica como de alto riesgo, alertando que el despliegue desregulado de estos

[31] DE LA TORRE, Jordi, "Redes generativas adversarias (GAN). Fundamentos teóricos y aplicaciones" en *Survey*, No. 2, 2023, URL https://arxiv.org/pdf/2302.09346 consultado 29/06/2026.
[32] Organización para la Cooperación y el Desarrollo Económico, *Recomendación revisada del Consejo sobre Inteligencia Artificial*, 2024, URL https://legalinstruments.oecd.org/api/download/?uri=/public/db5053b5-93e0-4cf5-a7cf-edce5ee6e893.pdf consultado 29/06/2026.

algoritmos invade la esfera de los derechos fundamentales al trastocar las identidades de las personas[33].

En el contexto latinoamericano los esfuerzos son más tímidos. La ausencia de un bloque regional armonizado en temas de ciberseguridad e IAGEN diluye la rendición de cuentas frente a sesgos o suplantaciones de identidad facilitadas por los programas de esta naturaleza[34]. Existe en este escenario un ecosistema transfronterizo donde los servidores e/o infractores operan fuera del alcance de las jurisdicciones nacionales.

En Ecuador, la regulación de la IAGEN ha sido poco abordada. No obstante, destaca el Acuerdo No. MINTEL-MINTEL-2025-0005, el cual expide la Política Pública de Transformación Digital, donde se reconocen que estas tecnologías son esenciales para el desarrollo, pero deben garantizar la libertad de elección de las personas y sus restantes derechos constitucionales[35]. Cabe añadir que, al ser solo una política pública, es un reconocimiento del fenómeno, pero no dota a los operadores de justicia de las herramientas procesales indispensables para enfrentarlo.

4. Insuficiencias del ordenamiento jurídico ecuatoriano

El diagnóstico de las insuficiencias del ordenamiento jurídico ecuatoriano frente a la IAGEN revela brechas estructurales desde la perspectiva constitucional y legal.

[33] Comisión Europea, *Report on the need to review the list of prohibited AI practices and of high-risk AI systems listed in Annex III of AI Act*, 2026, URL https://ec.europa.eu/newsroom/dae/redirection/document/128788 consultado 29/06/2026.

[34] AGUILAR ANTONIO, Juan Manuel, "La brecha de ciberseguridad en América Latina frente al contexto global de amenazas" en *Revista de Estudios en Seguridad Internacional*, vol. 6, No. 2, 2020, DOI http://dx.doi.org/10.18847/1.12.2 consultado 29/06/2026.

[35] Ministerio de Telecomunicaciones y de la Sociedad de la Información, Acuerdo No. MINTEL-MINTEL-2025-0005, Política Pública de Transformación Digital 2025-2030 del 14 de marzo de 2025 (Registro Oficial Suplemento No. 15, 8 de abril de 2025).

A continuación, se examinan estos problemas, que desbordan los límites de la soberanía jurisdiccional y exigen repensar la protección de la dimensión extrapatrimonial de los derechos de la personalidad frente a la manipulación digital.

A partir de lo investigado, el primer gran nudo crítico que revela la insuficiencia del ordenamiento jurídico ecuatoriano es la inexistencia de una categoría dogmática para el dato biométrico sintético. Mientras que la LOPDP define de manera tradicional los datos biométricos, es decir, sobre la base de un tratamiento técnico de las características físicas o conductuales reales[36], el sistema jurídico no tiene herramientas para catalogar la información generada artificialmente por redes neuronales profundas cuando estas emulan la identidad de la persona. Al no separar dicho producto como una creación de *software*, de lo que se considera un dato personal, se queda desprotegida la esencia misma de la identidad digital.

Al contrastar esta realidad con el plano internacional, se aprecia la falta de un sistema de clasificación de riesgos tecnológicos dentro de la legislación ecuatoriana. A diferencia del Reglamento de Inteligencia Artificial de la Unión Europea, que categoriza taxativamente a los sistemas de identificación biométrica remota y manipulación sintética como de alto riesgo o riesgo inaceptable[37], Ecuador no tiene una norma preventiva que lo defina como tal. Es necesario, al menos en un primer momento regulatorio, imponer obligaciones estrictas de gobernanza y evaluaciones de impacto antes de la puesta en marcha de un producto informático de esta

[36] Art. 4 LOPDP.

[37] Cons. (17) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828, de 13 de junio de 2024 (Diario Oficial de la Unión Europea, Serie L, 12 de julio de 2024) (Reglamento de Inteligencia Artificial).

naturaleza.

Otra insuficiencia estructural tiene que ver con la inoperancia del régimen de responsabilidad objetiva y subjetiva frente a la autonomía algorítmica. El ordenamiento distribuye la responsabilidad basándose en dos categorías: el responsable del tratamiento y el encargado de tratamiento[38]. Sin embargo, la IAGEN introduce modelos autorregresivos que confunden la trazabilidad del proceso de origen[39]. Así, cuando un usuario utiliza una plataforma internacional descentralizada para simular la imagen de un tercero, por ejemplo, el derecho ecuatoriano no tiene un modelo claro para definir la responsabilidad; sobre ello, el programador original puede argüir que su modelo fundacional es neutral, la plataforma transfronteriza alegará inmunidad de jurisdicción extranjera y el infractor permanecerá oculto en las redes cifradas, por lo que la relación de causalidad parece casi imposible de demostrar.

Al no existir tampoco un derecho constitucional autónomo a la indemnidad de la identidad digital, por el cual se prohíba la alteración sintética del patrimonio biométrico, los operadores administrativos y de justicia carecen de un marco claro para declarar un contenido como ilícito en este ámbito. Ello se debe a la visión comercial que sigue impregnada a los derechos de imagen y voz de los individuos, sin un desarrollo profundo de su contenido extrapatrimonial, que es el más afectado por el sesgo algorítmico y la manipulación virtual. Por ahora, sí es posible

[38] Art. 37 LOPDP.

[39] ALDAWSARI & ALAMMAR, "Integrating explainable AI with synthetic biometric data for enhanced image synthesis and privacy in computer vision systems".

discernir que el bien jurídico lesionado frente a una *deepfake* es la dignidad e intimidad del individuo, lo que debe conectarse con la protección eficaz de los datos personales como derecho constitucional autónomo.

Incluso, si se avanzara hacia la protección penal del mentado bien jurídico, se puede notar una inadecuación típica sustancial del delito de suplantación de identidad en el Código Orgánico Integral Penal[40] (en adelante, COIP). Dicho tipo requiere que el sujeto activo – una persona – adopte la calidad física, documental o civil de la víctima – otra persona – para obtener un beneficio para sí o un tercero. La IAGEN rompe el esquema porque el infractor no asume la personalidad del afectado, sino que en su lugar instrumentaliza un algoritmo para generar un contenido que induce a error, cual una falsedad ideológica instrumental[41]. Entonces, al no estar tipificada la creación, difusión o comercialización no consentida de material biométrico sintético lesivo, se genera impunidad por atipicidad.

En el ámbito administrativo, si bien la LOPDP regula detalladamente las transferencias internacionales de datos[42], tales normas presuponen la existencia de un flujo formal e identificable entre corporaciones nacionales y extranjeras. Los modelos de IAGEN, por el contrario, capturan en masa los datos biométricos a través de raspado de datos sin autorización y los procesan en nubes de servidores distribuidos globalmente[43]. Entonces, la Autoridad de Protección de Datos Personales

[40] Art. 212 Código Orgánico Integral Penal, 28 de enero de 2014 (Registro Oficial Suplemento No. 180, 10 de febrero de 2014) (COIP).
[41] LUENGO, Ana, "La responsabilidad penal en el uso de inteligencia artificial y los *deepfakes*" en ECIJA, 2026, URL https://www.ecija.com/actualidad-insights/la-responsabilidad-penal-en-el-uso-de-inteligencia-artificial-y-los-deepfakes/ consultado 30/06/2026.
[42] Arts 55-60 LOPDP.
[43] ALDAWSARI & ALAMMAR, "Integrating explainable AI with synthetic biometric data for enhanced image synthesis and privacy in computer vision systems".

carece de competencia jurisdiccional y, con seguridad, de herramientas tecnológicas para fiscalizar, requerir información o sancionar a los operadores tecnológicos allende las fronteras.

Conclusiones

El bloque de constitucionalidad y la LOPDP configuran un marco normativo robusto en términos teórico-prácticos sobre la privacidad, la intimidad y los datos biométricos dentro de la amplia gama de datos personales. No obstante, destaca el anacronismo y naturaleza estática de las normas, porque fueron diseñadas bajo la premisa de que los datos son unidades de información almacenada, lo que no basta para incluir las dimensiones dinámica, predictiva y desmaterializada que adquiere el patrimonio biométrico en entornos virtuales.

Se identificó que la arquitectura técnica de la IAGEN diluye los principios clásicos de la imputación de responsabilidad jurídica. El hallazgo medular se relaciona con la capacidad de las GAN para autoperfeccionarse mediante juegos de suma cero de archivos sintéticos o *deepfakes* idénticos a los reales. De ese modo, se fracturan los sistemas tradicionales de validación de identidad y autoría, con la consiguiente imposibilidad de establecer la relación de causalidad entre el programador original, la plataforma transfronteriza y el usuario infractor.

A través de un análisis crítico, es posible colegir que el ordenamiento jurídico tiene una limitada fortaleza estructural frente al fraude biométrico por deficiencias de tipicidad y competencia. En efecto, se constató que: a) no existe definición de dato biométrico sintético; b) las garantías jurisdiccionales resultan inviables frente a la falta de una base de datos centralizada o de un legitimado pasivo identificable

en redes cifradas; c) el delito de suplantación de identidad no alcanza la instrumentalización algorítmica de la que puede ser capaz la IAGEN; y d) la Autoridad de Protección de Datos no tiene competencia para fiscalizar el raspado de datos o *data scraping* ejecutado de forma extraterritorial.

Para saldar estas brechas urgen reformas multisistémicas. En síntesis, se requiere desplazar el eje reactivo del derecho hacia una gobernanza anticipatoria y densa del algoritmo, que reconozca la simulación biométrica no consentida como un fenómeno autónomo. Además, las precisiones normativas deben enfocarse en dotar al Estado de herramientas procesales, penales, constitucionales y administrativas coordinadas para precautelar la dignidad y la intimidad de las personas como fines últimos de la protección de datos.

Recomendaciones

Se propone ante todo la ampliación de los derechos a la identidad y a la intimidad con la incorporación del derecho a la indemnidad biométrica y autenticidad digital. Asimismo, la LOPDP debería definir entonces al dato biométrico sintético como una categoría de dato sensible, que, al ser modificado artificialmente, tendrá un tratamiento estricto. Es decir, que cualquier generación o clonación de un dato biométrico sin el consentimiento expreso, inequívoco y revocable del titular del dato ha de estar terminantemente prohibida.

Inspirándose en la experiencia del Reglamento de Inteligencia Artificial de la Unión Europea[44], esta reforma debe obligar además a todos los proveedores y

[44] Art. 48 Reglamento de Inteligencia Artificial.

desarrolladores de herramientas de IAGEN que ofrezcan servicios dentro del territorio ecuatoriano y/o para personas sujetas a su jurisdicción, que implementen marcas digitales criptográficas e indelebles y metadatos de procedencia de cada imagen, video o comportamiento sintético generado. Esta obligación coadyuva a identificar sin dificultad el origen algorítmico del contenido.

En el ámbito procesal constitucional es factible incorporar la figura del hábeas data algorítmico o descentralizado, lo que ampliaría la legitimación pasiva de dicha garantía jurisdiccional. Sobre esta base, puede dirigirse la acción no solo contra el administrador de una base de datos local o estática, sino contra cualquier intermediario de servicios de internet, motores de búsqueda y plataformas de redes sociales que alojen o distribuyan el contenido sintético suplantador. El juez constitucional quedaría facultado para ordenar medidas como la indexación inversa o *take down*, que obligaría a las plataformas a entrenar sus propios filtros para bloquear la replicación futura de la huella biométrica clonada de la víctima[45].

En el COIP, la solución requiere tipificar el delito de suplantación digital por simulación biométrica no consentida. Se sancionaría a quien, mediante IAGEN o cualquier otra tecnología de síntesis digital, recree, altere o utilice los datos biométricos de una persona natural sin autorización, con el fin de inducir a error sobre su identidad, menoscabar su reputación o cometer cualquier otro delito. Este modelo legislativo se ha empleado con éxito en varios estados norteamericanos, lo

[45] YANG, Wencheng et al., "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics" en *Sensors (Basel)*, vol. 23, No.7, 2023, DOI https://doi.org/10.3390/s23073566 consultado 30/06/2026.

que resolvería el problema de atipicidad estructural que padece el artículo 212 actual de dicho Código.

Aunque no es una solución a corto plazo, frente a la insuficiencia jurídica que plantea el carácter extraterritorial de la IAGEN, Ecuador podría instar a la adopción de un tratado multilateral sobre gobernanza transfronteriza de la inteligencia artificial, inspirado igualmente en el alcance del mentado Reglamento de Inteligencia Artificial de la Unión Europea[46]. Podrían plantearse importantes mecanismos de cooperación judicial y administrativa simplificados, lo que instaría a los proveedores de infraestructura en la nube e IAGEN a adoptar medidas de protección y someterse a la jurisdicción de los Estados firmantes cuando sus algoritmos faciliten la suplantación de identidad digital en la región.

Se sugiere la adopción de un sello de identidad digital en las transacciones de los sectores público y privado nacionales. La Dirección Nacional de Registros de Datos Públicos (en adelante, la DINARDAP), el Registro Civil y el Consejo de la Judicatura coordinarían lo necesario para migrar desde los sistemas de validación biométrica facial actuales hacia otros más avanzados. La ley exigirá entonces que cualquier trámite notarial o contractual desde plataformas digitales valide no solo la concordancia biométrica, sino la presencia física activa del usuario a través de pruebas de aleatoriedad imposibles de replicar en tiempo real por la IAGEN, lo que favorecerá la exclusión del fraude por suplantación de identidad digital.

Se recomienda la modificación de la LOPDP para incorporar, por un lado, la definición técnica de dato biométrico sintético como categoría especial protegida, que

[46] Arts. 20 y 21 Reglamento de Inteligencia Artificial.

a su vez constituye una subcategoría del dato sensible. Este tipo de dato debe estar sujeto a un tratamiento muy estricto que prohíba su generación, clonación o uso sin el expreso consentimiento del titular, quien puede revocarlo en cualquier momento.

Asimismo, todos los desarrolladores y proveedores de IAGEN que operen o presten servicios en Ecuador deberían implementar medidas de seguridad especiales en relación con los datos biométricos. Entre ellas, pueden establecerse marcas de agua digitales criptográficas indelebles y/o metadatos de procedencia de cada imagen, audio o video sintético creado, todo ello bajo prevención de sanción administrativa masiva o bloqueo de acceso IP en el territorio nacional.

Las modificaciones normativas deberían alcanzar a la LOGJCC para instituir el hábeas data algorítmico, lo que ampliaría la legitimación pasiva y la posibilidad de adopción de medidas reparadoras integrales ante vulneraciones de derechos amparados por dicha garantía jurisdiccional. Ello permitiría dirigir la acción contra intermediarios en Internet, motores de búsqueda y plataformas de redes sociales – incluidas las transfronterizas – que alojen o distribuyan el contenido sintético suplantador, facultando al juez a dictar medidas automatizadas de *take down* o indexación inversa y remoción inmediata de contenidos, es decir, retirar o dar baja de un contenido de internet.

Se recomienda también a la Asamblea Nacional tramitar la incorporación de un artículo subsiguiente al 212 del COIP para tipificar el delito de suplantación digital por simulación biométrica no consentida. El tipo penal debe permitir la sanción específica de la recreación o alteración de datos biométricos de una persona natu-

ral a través de tecnologías de síntesis digital sin autorización. La norma debe excluir el requisito clásico de adopción física o civil de la identidad y resolver así la crisis de atipicidad actual del fenómeno.

Finalmente, se sugiere a la DINARDAP, al Registro Civil y al Consejo de la Judicatura – cada uno en el ámbito de sus respectivas facultades – emitir resoluciones regulatorias conjuntas para sustituir los sistemas de validación biométrica facial estática. En su lugar, se adoptará un sello de identidad digital en trámites notariales, contractuales y financieros virtuales que se fundamente en pruebas de aleatoriedad e historia de vida imposibles de replicar o emular en tiempo real por algoritmos de IAGEN.

Bibliografía

Constitución de la República del Ecuador (Registro Oficial No. 449 de 20 de octubre de 2008).

Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, 29 de noviembre de 2016 (Registro Oficial Suplemento No. 899, 9 de diciembre de 2016).

Código Orgánico Integral Penal, 28 de enero de 2014 (Registro Oficial Suplemento No. 180, 10 de febrero de 2014).

Ley Orgánica de Protección de Datos Personales, 21 de mayo de 2021 (Registro Oficial Quinto Suplemento No. 459, 26 de mayo de 2021).

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 10 de septiembre de 2009 (Registro Oficial Segundo Suplemento No. 52, 22 de octubre de 2009).

Ministerio de Telecomunicaciones y de la Sociedad de la Información, Acuerdo No. MINTEL-MINTEL-2025-0005, Política Pública de Transformación Digital 2025-2030 del 14 de marzo de 2025 (Registro Oficial Suplemento No. 15, 8 de abril de 2025).

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828, de 13 de junio de 2024 (Diario Oficial de la Unión Europea, Serie L, 12 de julio de 2024).

Sentencia de la Corte Constitucional, 27 de enero de 2021 (2064-14-EP, Ponente: Carmen Corral Ponce).

ABBAS, Fakhar, CHESTERMAN, Simon y TAEIHAGH, Araz, "Building trust in the generative AI era: a systematic review of global regulatory frameworks to combat the risks of mis-, dis-, and mal-information" en *AI & Society*, No. 41, 2026, pp. 3913-3950, DOI https://doi.org/10.1007/s00146-025-02698-9 consultado 27/06/2026.

AGUILAR ANTONIO, Juan Manuel, "La brecha de ciberseguridad en América Latina frente al contexto global de amenazas" en *Revista de Estudios en Seguridad Internacional*, vol. 6, No. 2, 2020, pp. 17-43, DOI http://dx.doi.org/10.18847/1.12.2 consultado 29/06/2026.

AHSAN, Nafis, ISLAM, Shafikul y BAPPY, Mahathir Mohammad, "Generative

Modeling in Smart Manufacturing: Applications, Challenges, and Future Directions" en *Manufacturing Letters*, No. 44, 2025, pp. 1285-1295, DOI https://doi.org/10.1016/j.mfglet.2025.06.148 consultado 29/06/2026.

ALDAWSARI, Hamad y ALAMMAR, Saad, "Integrating explainable AI with synthetic biometric data for enhanced image synthesis and privacy in computer vision systems" en *Image and Vision Computing*, vol. 162, 2025, DOI https://doi.org/10.1016/j.imavis.2025.105726 consultado 27/06/2026.

Comisión Europea, *Report on the need to review the list of prohibited AI practices and of high-risk AI systems listed in Annex III of AI Act*, 2026, URL https://ec.europa.eu/newsroom/dae/redirection/document/128788 consultado 29/06/2026.

CORVALÁN, Juan Gustavo, SÁNCHEZ CAPARRÓS, Mariana y PAPINI, Carina, *Licenciamiento de IAGen y Protección de Datos. Un análisis comparativo de riesgos y garantías desde una perspectiva de gobernanza*, IALAB, 2026.

DE LA TORRE, Jordi, "Redes generativas adversarias (GAN). Fundamentos teóricos y aplicaciones" en *Survey*, No.2, 2023, URL https://arxiv.org/pdf/2302.09346 consultado 29/06/2026.

GARCÍA LLAMAS, Juan José, "Inteligencia Artificial Generativa (IAG). El nuevo paradigma en el diseño y producción de contenido" en GARCÍA MACÍAS, José Antonio (Coord.), PALAZUELOS ROJO, Isaac de Jesús (Coord.) y PÉREZ RIVAS, Diego Alfredo (Coord.), *Inteligencia artificial. Transformación, retos y prospectiva social*, Astra Ediciones, 2024, Ensenada, pp. 241-259, DOI https://doi.org/10.61728/AE20240998 consultado 29/06/2026.

JANIESCH, Christian, ZSCHECH, Patrick y HEINRICH, Kai, "Machine learning and deep learning" en *Electronic Markets*, No. 12525, 2021, DOI https://doi.org/10.1007/s12525-021-00475-2 consultado 29/06/2026.

JIMÉNEZ CASTELLANOS BALLESTEROS, Inmaculada, "La difícil convivencia entre la inteligencia artificial y los derechos fundamentales: la tecnología *deepfake*" en FEBLES POZO, Nayiber (Dir.) y NIETO ROJAS, Patricia (Dir.), *Inteligencia artificial y protección de datos: desafíos en la era digital*, COLEX, 2025, pp. 151-178.

LUENGO, Ana, "La responsabilidad penal en el uso de inteligencia artificial y los *deepfakes*" en ECIJA, 2026, URL https://www.ecija.com/actualidad-insights/la-responsabilidad-penal-en-el-uso-de-inteligencia-artificial-y-los-deepfakes/ consultado 30/06/2026.

NIEVA FENOLL, Jordi, "Inteligencia artificial generativa (IAGEN) y defensa: ¿cómo lograr la "convicción" de una máquina?" en *Revista Ítalo-Española de Derecho Procesal*, vol. 32, No. 4, 2025, pp. 1-17, DOI

https://doi.org/10.37417/rivitsproc/3204 consultado 28/06/2026.

Organización para la Cooperación y el Desarrollo Económico, *Recomendación revisada del Consejo sobre Inteligencia Artificial*, 2024, URL https://legalinstruments.oecd.org/api/download/?uri=/public/db5053b5-93e0-4cf5-a7cf-edce5ee6e893.pdf consultado 29/06/2026.

SOLER MARTÍNEZ, José Antonio, "Protección constitucional de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías" en *Anuario de Derecho Canónico*, No. 11, 2022, pp. 93-126, URL https://dialnet.unirioja.es/descarga/articulo/8661053.pdf consultado 27/06/2026.

UYÁ URREA, Virginia, *Clonación de voz mediante Inteligencia Artificial en el sector del doblaje: desafíos jurídicos y perspectivas regulatorias*, Universitat Autonoma de Barcelona, 2024, Barcelona, URL https://ddd.uab.cat/pub/tfg/2023/tfg_2505359/TFG_DERECHO_Virginia_Uy_Urrea.pdf consultado 28/06/2026.

YANG, Wencheng, WANG, Song, CUI, Hui, TANG, Zhaohui y LI, Yan, "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics" en *Sensors (Basel)*, vol. 23, No.7, 2023, DOI https://doi.org/10.3390/s23073566 consultado 30/06/2026.

ZARABOZO, Pedro Manuel, "La propiedad intelectual en la era de la Inteligencia Artificial Generativa: desafíos normativos, nuevas formas de creación y sus implicancias en el ejercicio profesional jurídico" en ZÁRATE, Hilda (Dir.), PELLERANO, Nahuel (Comp.) y GALLARDO, Lorena (Comp.), *Cuadernos de Posgrado 2025*, Universidad Nacional del Nordeste. Facultad de Derecho y Ciencias Sociales y Políticas, 2026, Corrientes, pp. 134-149, URL https://www.dch.unne.edu.ar/wp-content/uploads/2026/04/Cuadernos-de-Posgrado-2025.pdf consultado 29/06/2026.