

¿JUSTICIA SIN ROSTRO O JUSTICIA PROTEGIDA? AVATARES DIGITALES EN AUDIENCIAS DE ALTO RIESGO EN ECUADOR

FACELESS JUSTICE OR PROTECTED JUSTICE? DIGITAL AVATARS IN HIGH-RISK HEARINGS IN ECUADOR

Abg. Cinthya Geovanna Solórzano Álava, Mg.^{1*}

¹ Docente de la Carrera de Derecho, Facultad de Ciencias Sociales, Humanísticas y de la Educación, Universidad Estatal del Sur de Manabí, Jipijapa, Manabí, Ecuador. ORCID: <https://orcid.org/0009-0007-3177-5940>. Correo: cinthya.solorzano@unesum.edu.ec

Dr. C. Fabián Elí Montesdeoca Villavicencio²

² Docente de la Carrera de Derecho, Facultad de Ciencias Sociales, Humanísticas y de la Educación, Universidad Estatal del Sur de Manabí, Jipijapa, Manabí, Ecuador. ORCID: <https://orcid.org/0009-0009-4317-7176>. Correo: fabian.montesdeoca@unesum.edu.ec

Dr. C. Leopoldo Vinicio Venegas Loo³

³ Docente de la Carrera de Pedagogía de los Idiomas Nacionales y Extranjeros, Facultad de Ciencias Sociales, Humanísticas y de la Educación, Universidad Estatal del Sur de Manabí, Jipijapa, Manabí, Ecuador. ORCID: <https://orcid.org/0000-0002-3100-6320>. Correo: leopoldo.venegas@unesum.edu.ec

Dra. C. Paola Yadira Moreira Aguayo⁴

⁴ Docente de la Carrera de Pedagogía de los Idiomas Nacionales y Extranjeros, Facultad de Ciencias Sociales, Humanísticas y de la Educación, Universidad Estatal del Sur de Manabí, Jipijapa, Manabí, Ecuador. ORCID: <https://orcid.org/0000-0002-6380-2794>. Correo: paola.moreira@unesum.edu.ec

* Autor para correspondencia: cinthya.solorzano@unesum.edu.ec

Resumen

La aprobación en Ecuador del uso de avatares digitales institucionales en audiencias telemáticas de alta complejidad y riesgo introduce una tensión inédita entre seguridad judicial, protección biométrica y garantías del debido proceso. El objetivo fue analizar la compatibilidad constitucional y convencional de esta medida e identificar salvaguardas para impedir que la anonimización visual derive en anonimato jurisdiccional. Se desarrolló una investigación cualitativa, jurídico-dogmática y documental, con análisis de normativa

ecuatoriana, jurisprudencia interamericana, lineamientos internacionales y literatura científica sobre justicia remota y justicia procedimental. Los resultados muestran que la medida persigue una finalidad legítima frente a amenazas verificables contra operadores judiciales, pero su validez depende de la excepcionalidad, motivación, proporcionalidad, identificación jurídica del juzgador, autenticación tecnológica, preservación de la contradicción y protección de datos desde el diseño. Como aporte se propone el Modelo de Anonimización Visual Controlada con Doble Trazabilidad, que combina trazabilidad jurisdiccional y tecnológica. Se concluye que el rostro puede ser protegido cuando exista riesgo objetivo, pero la identidad jurídica, competencia, responsabilidad y presencia humana de quien ejerce jurisdicción deben permanecer verificables.

Palabras clave: justicia digital; avatares digitales; debido proceso; seguridad judicial; datos biométricos

Abstract

The approval in Ecuador of institutional digital avatars for high-complexity and high-risk remote hearings creates an unprecedented tension between judicial security, biometric protection and due process guarantees. This study aimed to assess the constitutional and conventional compatibility of the measure and to identify safeguards capable of preventing visual anonymization from becoming jurisdictional anonymity. A qualitative, legal-dogmatic and documentary design was applied through the analysis of Ecuadorian legislation, Inter-American case law, international guidance and peer-reviewed literature on remote justice and procedural justice. The findings show that the measure pursues a legitimate aim when judicial officers face verifiable threats, but its validity depends on exceptionality, reasoned authorization, proportionality, legal identification of the judge, technological authentication, preservation of adversarial participation and data protection by design. The study proposes a Controlled Visual Anonymization with Dual Traceability Model, combining jurisdictional and technological traceability. It concludes that a judge's face may be protected when an objective risk exists, but the legal identity, competence, accountability and human presence of the person exercising judicial power must remain verifiable.

Keywords: digital justice; digital avatars; due process; judicial security; biometric data

Fecha de recibido: 24/05/2026

Fecha de aceptado: 13/08/2026

Fecha de publicado: 17/08/2026

Introducción

La justicia digital ha dejado de ser una política complementaria para convertirse en una dimensión estructural del funcionamiento de los tribunales. La incorporación de expedientes electrónicos, notificaciones digitales, videoconferencias y plataformas de gestión modifica no solo la velocidad con la que circula la información, sino también la forma en que la ciudadanía percibe, experimenta y controla el ejercicio de la jurisdicción. Donoghue (2017) advirtió que la digitalización de los tribunales no puede juzgarse únicamente por sus

ganancias de eficiencia, porque altera las condiciones de participación pública y de acceso a la justicia. Años después, la expansión mundial de las audiencias remotas confirmó que la tecnología judicial incide en elementos centrales del proceso, entre ellos la publicidad, la participación efectiva, la percepción de imparcialidad y la construcción simbólica de la autoridad judicial (Legg, 2021; Kamber, 2022).

En ese escenario, Ecuador abrió el 7 de agosto de 2026 una etapa novedosa al anunciar la aprobación del Protocolo Técnico-Operativo para el Uso de Avatares Digitales como Medida de Seguridad en Audiencias Telemáticas. De acuerdo con la información oficial disponible al cierre de esta investigación, en determinadas audiencias digitales de alta complejidad y riesgo la imagen de jueces y otros servidores judiciales podrá ser sustituida por un avatar digital institucional. La finalidad declarada es reducir la exposición visual y evitar que imágenes capturadas durante una diligencia sean utilizadas para reconocimiento facial automatizado, elaboración de perfiles biométricos, inteligencia criminal o vigilancia ilícita (Consejo de la Judicatura, 2026a). La medida se orienta principalmente a causas penales, corrupción, crimen organizado y violencia, aunque puede extenderse a otros operadores expuestos a circunstancias que comprometan su integridad.

La decisión no surge en un vacío. Un día antes de anunciar el protocolo de avatares, el Consejo de la Judicatura aprobó el Plan de Seguridad Integral de la Función Judicial. El diagnóstico institucional que acompañó esa decisión reportó 127 servidores judiciales amenazados y 23 víctimas de hechos de violencia, además de establecer mecanismos de atención de solicitudes de seguridad, protección individual, teletrabajo en situaciones de riesgo, primeros auxilios psicológicos y coordinación con otras instituciones estatales (Consejo de la Judicatura, 2026b). Aunque esas cifras no permiten por sí solas medir toda la magnitud del riesgo, sí demuestran que la discusión sobre anonimización visual se relaciona con amenazas reales y no con un ejercicio puramente especulativo.

El problema científico aparece precisamente porque la seguridad judicial y el debido proceso no son bienes jurídicos opuestos de manera absoluta. La independencia del juez puede verse comprometida cuando existe una amenaza creíble contra su vida o la de su familia; al mismo tiempo, la defensa necesita saber quién ejerce la potestad jurisdiccional, comprobar su competencia, conocer eventuales conflictos de interés y utilizar los mecanismos de excusa o recusación previstos por el ordenamiento. El desafío no consiste, por tanto, en escoger entre seguridad o garantías, sino en determinar qué configuración tecnológica y normativa permite proteger la identidad biométrica sin ocultar la identidad jurídica de la autoridad.

Esta distinción adquiere especial relevancia en América Latina debido a la memoria jurídica de los denominados jueces sin rostro. La Corte Interamericana de Derechos Humanos examinó en Castillo Petruzzi y otros vs. Perú un régimen en el que las personas procesadas fueron juzgadas por tribunales cuya identidad se mantenía oculta, dentro de un contexto caracterizado por restricciones severas a garantías judiciales (Corte Interamericana de Derechos Humanos, 1999). El antecedente obliga a evitar analogías simplistas. Un avatar institucional que cubre la imagen de un juez plenamente identificado no es, por definición, idéntico a un tribunal anónimo. Sin embargo, la tecnología podría reproducir algunos de los riesgos históricos si impidiera a las partes conocer o verificar quién decide, si dificultara la recusación o si volviera imposible atribuir responsabilidad a la persona que ejerce jurisdicción.

La literatura contemporánea sobre justicia remota refuerza esa precaución. Rowden y Wallace (2018) demostraron que los enlaces de video transforman la imagen judicial y modifican la forma en que se representa

la autoridad del juez. Rossner y Tait (2023) observaron que la presencia y la participación en tribunales virtuales dependen de una arquitectura comunicativa que puede fortalecer o debilitar la intervención de los sujetos procesales. Factor et al. (2023) encontraron asociaciones relevantes entre videoconferencia y percepciones de justicia procedimental, mientras Mentovich et al. (2023) mostraron que el acceso y la experiencia procedimental influyen en la legitimidad atribuida por los usuarios a los procedimientos en línea. Estas contribuciones impiden considerar el avatar como una simple capa gráfica sin consecuencias jurídicas o institucionales.

También existe una dimensión de protección de datos. La Constitución ecuatoriana reconoce el derecho a la protección de datos personales y protege la imagen y la voz. La Ley Orgánica de Protección de Datos Personales incluye los datos biométricos dentro de las categorías que requieren tutela reforzada cuando permiten identificar de manera inequívoca a una persona. En consecuencia, una imagen facial capturada durante una audiencia puede adquirir valor que excede su función comunicativa inmediata, pues puede ser procesada mediante sistemas de reconocimiento, enlazada con otras bases de datos o utilizada para seguimiento. La preocupación expresada por el Consejo de la Judicatura se conecta, así, con una transformación más amplia: el rostro dejó de ser solo un atributo visible y puede convertirse en un identificador digital reutilizable.

No obstante, la protección biométrica tampoco autoriza un uso indiscriminado de técnicas de ocultamiento. La propia normativa ecuatoriana exige principios de proporcionalidad, minimización, seguridad y responsabilidad en el tratamiento de datos, y la Superintendencia de Protección de Datos Personales ha desarrollado lineamientos de gestión de riesgos y evaluación de impacto para tratamientos capaces de afectar significativamente derechos y libertades (Superintendencia de Protección de Datos Personales, 2026). Resultaría paradójico que una plataforma destinada a proteger el rostro generara, almacenara o transfiriera datos biométricos sin controles adecuados. La solución tecnológica debe, por tanto, ser coherente con la finalidad protectora que la justifica.

A partir de estas tensiones, la pregunta central de investigación es la siguiente: ¿bajo qué condiciones jurídicas y tecnológicas el uso de avatares digitales en audiencias judiciales de alto riesgo puede ser compatible con la seguridad de los operadores, la protección de datos biométricos y las garantías del debido proceso en Ecuador? Como preguntas específicas se plantean: a) qué diferencia debe establecerse entre anonimización visual y anonimato jurisdiccional; b) qué riesgos genera la intermediación gráfica para intermediación, publicidad, contradicción y confianza; c) qué requisitos de autenticación, registro y auditoría deberían acompañar la medida; y d) cómo debe aplicarse un examen de proporcionalidad antes de activarla.

El objetivo general es analizar críticamente la compatibilidad constitucional, convencional y tecnológica del uso de avatares digitales en audiencias de alto riesgo en Ecuador. De manera específica, se busca identificar los derechos e intereses en tensión, contrastar la medida con estándares interamericanos y estudios sobre justicia remota, construir una matriz de riesgos y salvaguardas y proponer un modelo de implementación basado en doble trazabilidad. La hipótesis de trabajo sostiene que la representación mediante avatar puede ser constitucionalmente admisible como mecanismo excepcional de protección cuando exista riesgo objetivo, siempre que no suprima la identificación jurídica del juzgador ni reduzca la capacidad real de las partes para controlar competencia, imparcialidad, autenticidad y regularidad de la audiencia.

La contribución del estudio consiste en desplazar el debate desde la oposición binaria entre jueces con rostro y jueces sin rostro hacia una categoría intermedia susceptible de control: la anonimización visual controlada. Bajo esta perspectiva, el elemento decisivo no es si la cámara reproduce literalmente las facciones del juez, sino si el sistema preserva dos cadenas de verificabilidad. La primera es jurisdiccional y permite saber quién ejerce la potestad, con qué competencia y bajo qué responsabilidad. La segunda es tecnológica y permite demostrar que la persona identificada fue efectivamente quien participó, habló y decidió durante la diligencia. La combinación de ambas se desarrolla en este trabajo como Modelo de Anonimización Visual Controlada con Doble Trazabilidad, en adelante AVCDT.

Materiales y métodos

La investigación se desarrolló bajo un enfoque cualitativo, de tipo jurídico-dogmático, documental y propositivo. El diseño se escogió porque el objeto de estudio es una medida normativa y tecnológica reciente cuya evaluación requiere integrar reglas constitucionales, disposiciones legales, estándares convencionales y evidencia científica sobre las consecuencias de la virtualización judicial. No se pretendió medir estadísticamente la eficacia de una herramienta que todavía no cuenta con una trayectoria suficiente de aplicación pública, sino determinar las condiciones de validez que deberían acompañar su implementación.

El corpus primario incluyó la Constitución de la República del Ecuador; el Código Orgánico de la Función Judicial; el Código Orgánico Integral Penal, en particular la regulación de audiencias telemáticas; la Ley Orgánica de Protección de Datos Personales; el Protocolo para la Realización de Videoaudiencias de 2021; la información oficial del Consejo de la Judicatura sobre el Plan de Seguridad Integral y sobre la aprobación del protocolo de avatares de agosto de 2026; la guía vigente de la Superintendencia de Protección de Datos Personales sobre gestión de riesgos y evaluación de impacto; y la sentencia Castillo Petrucci y otros vs. Perú. Como estándares comparados se incorporaron las directrices de la Comisión Europea para la Eficiencia de la Justicia sobre videoconferencia de 2021 y la guía sobre audiencias remotas de 2025.

El corpus secundario se integró con publicaciones científicas sobre justicia digital, audiencias remotas, participación, legitimidad y justicia procedimental. Se priorizaron artículos revisados por pares y documentos institucionales con trazabilidad editorial, dando preferencia a estudios de los últimos cinco años, sin excluir trabajos anteriores considerados fundacionales para comprender la transformación de la imagen judicial. Entre los criterios de inclusión constaron la relación directa con audiencias remotas o tecnología judicial, la identificación verificable de autoría y publicación, la disponibilidad de DOI o fuente institucional y la utilidad para alguna de las categorías de análisis. Se excluyeron notas periodísticas y publicaciones en redes sociales como fuente de evidencia jurídica, aunque una noticia difundida en medios motivó inicialmente el interés por el problema.

La fecha de cierre de la revisión fue el 8 de agosto de 2026. Esta precisión es relevante porque el Consejo de la Judicatura anunció la aprobación del protocolo apenas el día anterior. Las búsquedas realizadas no permitieron localizar en acceso público, a esa fecha, el texto técnico íntegro del nuevo protocolo. Por ello, el análisis distingue cuidadosamente entre características confirmadas por la comunicación institucional y salvaguardas que este artículo propone normativamente. No se atribuyen al protocolo reglas operativas no divulgadas, y la ausencia de texto completo se reconoce como limitación del estudio.

Para la interpretación se construyó una matriz con cinco dimensiones: legitimidad de la finalidad, garantías procesales, protección de datos, integridad tecnológica y gobernanza institucional. Cada dimensión se relacionó con preguntas de control. En legitimidad se examinó la existencia de un riesgo verificable; en garantías procesales, la conservación de juez competente, defensa, intermediación, contradicción y publicidad; en datos personales, minimización, finalidad y seguridad; en integridad tecnológica, autenticación, continuidad, registro y respuesta ante incidentes; y en gobernanza, motivación, temporalidad, auditoría y posibilidad de revisión.

El procedimiento analítico tuvo tres momentos. Primero, se realizó interpretación sistemática de las normas ecuatorianas para identificar derechos y competencias aplicables. Segundo, se aplicó análisis comparado funcional con jurisprudencia y directrices internacionales, evitando trasladar automáticamente instituciones desarrolladas en contextos diferentes. Tercero, se utilizó un examen de proporcionalidad compuesto por idoneidad, necesidad y proporcionalidad en sentido estricto para evaluar la activación del avatar. El modelo AVCDT se construyó mediante síntesis normativa de los riesgos detectados y se sometió a un criterio de consistencia: cada salvaguarda propuesta debía responder a un riesgo identificable y no podía anular la finalidad de seguridad.

El estudio no utiliza datos personales de participantes, entrevistas ni expedientes judiciales, por lo que no requirió tratamiento empírico de información sensible. La cifra de amenazas se incorpora únicamente como dato institucional agregado publicado por el Consejo de la Judicatura. La principal limitación es el carácter incipiente de la política, que impide evaluar todavía su impacto real sobre percepción de legitimidad, tasas de incidentes o conducta de los litigantes. En consecuencia, los resultados son de naturaleza jurídica y de diseño institucional, y deben complementarse en el futuro con investigación empírica una vez exista suficiente experiencia de uso.

Tabla 1. Matriz de fuentes y categorías de análisis

Fuente/categoría	Variable observada	Finalidad analítica
Normativa constitucional y procesal	Competencia, defensa, publicidad, oralidad, intermediación, seguridad jurídica	Determinar límites que la representación digital no puede vaciar.
Seguridad judicial	Riesgo, independencia y protección de servidores	Valorar la finalidad legítima y la excepcionalidad.
Protección de datos	Biometría, minimización, finalidad, riesgo e impacto	Evitar que la protección visual genere un tratamiento biométrico más intrusivo.
Jurisprudencia interamericana	Juez competente, imparcialidad y jueces sin rostro	Distinguir ocultamiento visual de anonimato jurisdiccional.
Literatura científica	Presencia, participación, legitimidad y justicia procedimental	Evaluar efectos de la mediación tecnológica sobre la experiencia procesal.
Gobernanza tecnológica	Autenticación, trazabilidad, registro, incidentes	Diseñar salvaguardas verificables y auditables.

Nota: elaboración propia a partir del corpus documental descrito.

Resultados y discusión

De la videoaudiencia a la protección de la identidad biométrica

El primer resultado es que el avatar no representa una ruptura completa con la digitalización judicial ecuatoriana, sino una nueva capa sobre una infraestructura procesal previamente legitimada. El artículo 565 del Código Orgánico Integral Penal admite audiencias telemáticas o medios técnicos semejantes, entre otras razones, por seguridad o utilidad procesal, bajo autorización judicial. El Protocolo para la Realización de Videoaudiencias de 2021 desarrolla esa posibilidad y procura coordinación técnica, acceso, publicidad cuando corresponde y continuidad de la diligencia (Asamblea Nacional del Ecuador, 2014; Consejo de la Judicatura, 2021). La novedad de 2026 no es, entonces, la distancia física entre tribunal y participantes, sino la decisión de modificar deliberadamente la imagen visible de determinadas personas conectadas.

Esa modificación cambia el objeto del control jurídico. En una videoconferencia convencional, la principal preocupación es que la comunicación sea sincrónica, estable y permita escuchar y observar a quien interviene. Con un avatar, además debe acreditarse que la representación corresponde en tiempo real a la persona autorizada y que no existe sustitución de identidad o generación autónoma de contenido. La fidelidad deja de ser equivalencia visual perfecta y pasa a significar autenticidad funcional: la voz, las decisiones, las respuestas y los actos deben proceder del juez humano competente, aunque la interfaz oculte facciones biométricas.

La comunicación oficial del Consejo de la Judicatura es clara al señalar que el avatar no supone delegación de funciones: los jueces continúan a cargo de la diligencia, resuelven incidentes, valoran la prueba y adoptan las decisiones (Consejo de la Judicatura, 2026a). Esta precisión es esencial para evitar una lectura equivocada que confunda avatar con juez artificial. El problema examinado en este artículo no es la automatización de la decisión, sino la mediación de la presencia visual. Si una futura versión de la tecnología incorporara generación autónoma de voz, síntesis de respuestas o apoyo decisorio no transparente, el análisis jurídico debería ampliarse de manera sustancial.

Las directrices internacionales sobre audiencias remotas coinciden en que el valor de la tecnología depende de su capacidad de preservar el proceso justo. La CEPEJ (2025) recomienda una integración equilibrada en la que la tecnología fortalezca y no obstaculice el acceso a la justicia. La misma idea se encuentra en Kamber (2022): la pregunta no es si una audiencia ocurre en línea, sino si las condiciones concretas permiten participación efectiva, defensa y control. Aplicada al avatar, esta lógica exige abandonar cualquier presunción de neutralidad tecnológica y evaluar el sistema como parte de la arquitectura del debido proceso.

Seguridad del juzgador como condición de independencia

El segundo resultado consiste en reconocer que la seguridad del juez no es un privilegio corporativo ajeno a los derechos de las partes. El Código Orgánico de la Función Judicial incorporó expresamente el artículo 90.1, que reconoce a servidoras y servidores judiciales el derecho a medidas de protección y seguridad. Esta disposición permite comprender la protección física y digital como componente del entorno necesario para ejercer la jurisdicción sin coacción. Un juez sometido a amenazas graves puede ver condicionada su independencia incluso cuando no exista una orden explícita de actuar de determinada manera, porque el riesgo personal introduce incentivos incompatibles con la libertad de decidir conforme a Constitución y ley (Asamblea Nacional del Ecuador, 2009).

El diagnóstico presentado en agosto de 2026 refuerza la necesidad de abandonar enfoques abstractos. El Consejo de la Judicatura identificó 127 servidores amenazados y 23 víctimas de violencia y aprobó un plan con medidas de protección, coordinación institucional y seguimiento (Consejo de la Judicatura, 2026b). No obstante, la existencia de un problema general no significa que todos los operadores tengan el mismo nivel de exposición. De ahí surge una primera salvaguarda: la activación del avatar debe vincularse a una evaluación individual o contextual de riesgo suficientemente documentada y no a una regla automática para todas las causas de una categoría penal.

Esta exigencia responde también al principio de necesidad. Si la finalidad puede alcanzarse con medidas menos restrictivas, por ejemplo control de acceso a la audiencia, reserva parcial, protección física, teletrabajo, distorsión selectiva de fondos o prohibiciones de grabación con mecanismos efectivos, la autoridad debe valorar esas alternativas antes de adoptar una anonimización visual más intensa. En determinados casos, sin embargo, esas herramientas pueden ser insuficientes: una audiencia pública retransmitida o una diligencia a la que acceden múltiples personas puede facilitar capturas de pantalla imposibles de controlar una vez difundidas. Allí el avatar puede constituir una medida idónea de reducción de superficie de exposición.

La independencia judicial posee así una dimensión de seguridad informacional. Tradicionalmente se pensó en escoltas, edificios, rutas de traslado o reserva de domicilio. En un ecosistema de reconocimiento facial, una fotografía de alta calidad puede convertirse en insumo para localizar perfiles, cruzar redes sociales, identificar familiares o inferir rutinas. El riesgo no desaparece porque la audiencia sea virtual; en ciertos escenarios aumenta porque la imagen puede capturarse sin aproximación física al juzgador. La política de seguridad contemporánea debe considerar esa transición desde la amenaza territorial hacia la amenaza basada en datos.

La frontera entre avatar protegido y juez sin rostro

El tercer hallazgo es conceptual y determina buena parte de la evaluación constitucional: anonimización visual y anonimato jurisdiccional no son equivalentes. El precedente interamericano de Castillo Petruzzi y otros vs. Perú constituye una advertencia relevante porque el proceso involucró tribunales sin rostro en un entorno de fuertes restricciones a garantías judiciales (Corte Interamericana de Derechos Humanos, 1999). Sin embargo, reducir aquel problema a la imposibilidad de observar las facciones del juzgador sería insuficiente. La afectación se relacionaba con la imposibilidad de controlar adecuadamente quién integraba el tribunal, su competencia e independencia dentro de un régimen excepcional.

Un avatar institucional podría funcionar de modo distinto si la identidad jurídica del juez permanece plenamente disponible para las partes y consta en el expediente. En ese escenario, el procesado sabe quién conoce la causa, puede verificar el mecanismo de asignación, plantear una recusación si identifica un conflicto y exigir responsabilidad por las actuaciones. La cara se oculta frente a la transmisión, pero la persona jurídica que ejerce jurisdicción no desaparece. Esta distinción permite formular un criterio operativo: la identidad biométrica puede someterse a protección reforzada; la identidad jurisdiccional debe conservarse en un nivel suficiente para el ejercicio efectivo de derechos procesales.

El límite se supera cuando la seguridad se utiliza para impedir que las partes conozcan el nombre del juez, cuando la identidad se comunica solo a una autoridad administrativa sin posibilidad de control procesal, cuando el sistema no permite comprobar que el juez conectado coincide con el designado o cuando la defensa

carece de mecanismos para impugnar la medida. En tales supuestos, la tecnología dejaría de ser una capa de protección y se acercaría a una forma funcional de tribunal anónimo.

La Constitución ecuatoriana exige ser juzgado por una autoridad competente, garantiza la defensa, la publicidad con excepciones legalmente previstas y la seguridad jurídica (Asamblea Nacional Constituyente, 2008). Ninguna de esas garantías depende exclusivamente del reconocimiento facial del juez, pero todas requieren identificabilidad institucional. Por ello, el estándar propuesto es de identidad jurídica verificable: al inicio de la audiencia debe existir certeza documental y técnica sobre el nombre, cargo, órgano, competencia y autenticación de quien ejerce jurisdicción, aun cuando su rostro no se muestre al público.

La diferencia se resume en la Tabla 2. La comparación no pretende afirmar que todo avatar es compatible con derechos ni que todo ocultamiento facial sea inocuo. Su propósito es mostrar qué elementos permiten separar una medida de seguridad controlada de una justicia secretizada.

Tabla 2. Diferencias entre anonimización visual controlada y anonimato jurisdiccional

Elemento	Avatar protegido propuesto	Juez sin rostro problemático
Identidad del juzgador	Conocida y verificable en expediente y audiencia	Ocultada o inaccesible para las partes
Competencia	Puede ser controlada y discutida	Difícil o imposible de verificar
Recusación/excusa	Se mantienen operativas	Se debilitan por desconocimiento de identidad
Intervención humana	Juez real presente en tiempo real	Puede existir opacidad sobre quién actúa
Finalidad	Protección biométrica frente a riesgo específico	Anonimato institucional como regla
Temporalidad	Excepcional y revisable	Permanente o automática
Auditoría	Registros de autenticación e integridad	Trazabilidad insuficiente
Responsabilidad	Atribuible a persona y órgano determinados	Difícil atribución individual

Nota: elaboración propia con base en Constitución, jurisprudencia interamericana y criterios de trazabilidad.

El rostro como dato biométrico y la obligación de minimizar exposición

Un cuarto resultado es que el debate debe incorporar de manera explícita el derecho de protección de datos. La Constitución del Ecuador reconoce la protección de datos personales y tutela la imagen y la voz como ámbitos de la personalidad (Asamblea Nacional Constituyente, 2008). La Ley Orgánica de Protección de Datos Personales, por su parte, establece un marco de principios y obligaciones para el tratamiento de información que identifica o hace identificable a una persona, incluyendo categorías sensibles asociadas con rasgos biométricos (Asamblea Nacional del Ecuador, 2021). En este contexto, la imagen del rostro no es jurídicamente indiferente cuando puede transformarse mediante procesos técnicos en un patrón de identificación.

La finalidad declarada por el Consejo de la Judicatura, impedir reconocimiento facial automatizado, perfiles biométricos, inteligencia criminal o vigilancia ilícita, es coherente con el principio de minimización: si para dirigir una audiencia resulta suficiente la presencia autenticada del juez sin exhibición de rasgos faciales, reducir la exposición puede disminuir ciertos riesgos (Consejo de la Judicatura, 2026a). Esta idea es

compatible con la protección de datos desde el diseño, porque se intenta evitar que la información biométrica salga innecesariamente del entorno controlado.

No obstante, el análisis debe extenderse al funcionamiento interno de la solución. Para generar un avatar en tiempo real es probable que la plataforma procese video, puntos faciales o información de movimiento. No toda transformación de imagen implica necesariamente identificación biométrica, pero la arquitectura puede llegar a tratar datos biométricos si extrae características con finalidad de identificación o autenticación. Por ello, antes de implementar el sistema debe documentarse qué datos entran, qué datos se derivan, dónde se procesan, cuánto tiempo se conservan, quién accede, si existen proveedores externos y qué ocurre con la información una vez concluida la audiencia.

La guía de gestión de riesgos y evaluación de impacto de la Superintendencia de Protección de Datos Personales refuerza la necesidad de analizar escenarios de riesgo, consecuencias para titulares y medidas de mitigación (Superintendencia de Protección de Datos Personales, 2026). En una solución judicial, una evaluación de impacto debería contemplar, al menos, filtración del video original, acceso no autorizado a modelos o plantillas, reutilización de imágenes para finalidades incompatibles, transferencias internacionales no previstas, errores de asignación del avatar y persistencia de copias en servicios de terceros.

Existe además una tensión entre seguridad y auditabilidad. Para investigar una eventual suplantación podría parecer útil conservar el video real del juez; sin embargo, almacenar indefinidamente ese material destruiría parte de la finalidad protectora. La respuesta más consistente es una política de retención limitada y acceso escalonado. El registro público o entregable a sujetos procesales puede conservar la versión protegida, mientras un registro de alta seguridad, cifrado y con acceso estrictamente controlado puede mantenerse únicamente durante el tiempo necesario para resolver incidentes o recursos. La decisión sobre esta arquitectura debe constar en una política transparente y ser coherente con finalidad, proporcionalidad y minimización.

La protección de datos también exige diferenciar entre rostro y voz. La comunicación oficial se concentra en la imagen, pero la voz puede convertirse en identificador biométrico si se procesa técnicamente para reconocimiento. Una política de protección integral debe valorar si el riesgo proviene solo de la imagen o también de características vocales. La distorsión de voz, sin embargo, puede afectar más intensamente la comprensión, la solemnidad y la interacción; por ello no debería incorporarse por extensión automática, sino mediante una evaluación independiente de necesidad.

Inmediación, presencia y posibilidad real de participar

La quinta línea de resultados se refiere a la inmediatez. La digitalización obliga a separar inmediatez de copresencia física absoluta. El ordenamiento ecuatoriano ya admite que una audiencia se desarrolle mediante videoconferencia cuando concurren condiciones legales, lo que demuestra que la presencia procesal puede construirse tecnológicamente (Asamblea Nacional del Ecuador, 2014; Consejo de la Judicatura, 2021). Sin embargo, la admisión normativa de la videoconferencia no significa que cualquier mediación adicional preserve automáticamente el mismo nivel de interacción.

Rowden y Wallace (2018) mostraron que el video transforma la producción y recepción de la imagen judicial. Rossner y Tait (2023) subrayan que la sensación de presencia no depende exclusivamente de estar conectado,

sino de la posibilidad de intervenir, comprender lo que sucede y ser reconocido como participante del proceso. Factor et al. (2023) añaden que las características de la videoconferencia inciden en percepciones de justicia procedimental. El avatar debe diseñarse considerando estas conclusiones, porque una figura excesivamente rígida, desincronizada o inexpresiva puede producir distancia comunicativa incluso cuando el juez real esté prestando atención.

La intermediación relevante para el juez incluye escuchar directamente a las partes, formular preguntas, controlar la producción de prueba y responder a incidencias. Ninguna de esas funciones requiere mostrar cada rasgo facial del juzgador. En cambio, para quienes comparecen sí puede importar recibir señales de atención, turnos y comprensión. Por ello, el avatar institucional debería transmitir movimientos básicos y sincronización suficientes para que el participante identifique cuándo el juez habla, escucha o solicita una intervención, sin pretender reproducir expresiones faciales detalladas que restablezcan el riesgo biométrico.

El principio de presencia humana verificable propuesto en este estudio exige que la plataforma deje claro que detrás de la representación existe una autoridad humana conectada en tiempo real. Un indicador visual permanente, por ejemplo 'autoridad judicial autenticada, representación protegida', puede contribuir a reducir incertidumbre. Asimismo, al inicio de la audiencia debería realizarse una comprobación formal de identidad, cargo y causa, registrada en acta, sin necesidad de exhibir públicamente la imagen real.

La defensa debe conservar canales de comunicación privada con la persona procesada, acceso oportuno a documentos y capacidad de intervenir sin desventajas técnicas. Kamber (2022) sostiene que el derecho a una audiencia justa en línea depende de condiciones concretas que permitan participación efectiva. De Vocht (2022) también advierte que las ventajas de las audiencias virtuales varían según tipo de proceso y participante. En consecuencia, si la representación digital genera una falla que impide escuchar, identificar turnos o comprender al juez, la diligencia debe pausarse y, de ser necesario, pasar a una modalidad alternativa. La continuidad tecnológica no puede prevalecer sobre la posibilidad real de defensa.

Publicidad y transparencia: ver menos no debe significar controlar menos

El sexto resultado aborda una aparente paradoja. La publicidad procesal suele asociarse con la posibilidad de observar el tribunal, mientras el avatar reduce deliberadamente una parte de la información visual. Sin embargo, el principio de publicidad no equivale a un derecho irrestricto a capturar datos biométricos de todos los intervinientes. Su función constitucional es permitir control social del proceso, evitar decisiones clandestinas y ofrecer transparencia sobre cómo actúa la justicia. La pregunta relevante es si esas finalidades pueden mantenerse cuando el rostro del juez se encuentra protegido.

Legg (2021) identifica la justicia abierta, la equidad procedimental y la imparcialidad como elementos esenciales que deben preservarse en la transición digital. Mentovich et al. (2023) muestran que la legitimidad de los procedimientos en línea se relaciona con percepciones tanto de acceso como de trato procedimental. La transparencia, entonces, requiere más que una cámara abierta: exige información comprensible sobre quién dirige la audiencia, qué reglas rigen la representación digital, por qué se aplicó la medida y cómo pueden las partes cuestionarla.

La publicidad puede fortalecerse mediante transparencia compensatoria. Cuando la imagen se reduce por seguridad, el sistema debería aumentar otros mecanismos de control: identificación jurídica visible del

juzgador, publicación de reglas generales de uso, registro de la decisión motivada, información sobre el carácter no autónomo del avatar y conservación de actas. La sociedad puede conocer qué juez intervino y qué resolvió sin acceder necesariamente a un primer plano de sus rasgos faciales. Este desplazamiento desde transparencia facial hacia transparencia institucional resulta central para evitar que seguridad sea sinónimo de opacidad.

La reserva también debe ser granular. Existen audiencias que por su naturaleza ya cuentan con limitaciones de publicidad, por ejemplo cuando se protegen víctimas o determinados datos. En esos casos, el avatar puede formar parte de un conjunto mayor de medidas de confidencialidad. En audiencias públicas, en cambio, la regla debería ser que únicamente se oculte aquello estrictamente necesario para mitigar el riesgo. No existe justificación para alterar nombres, cargo, contenido de decisiones o acceso al desarrollo de la diligencia cuando esos elementos no comprometen la seguridad.

Un protocolo robusto debería contemplar un mecanismo de información previa a las partes. Saber de antemano que se utilizará un avatar permite preparar objeciones, verificar identidad por canales institucionales y ajustar aspectos técnicos. La sorpresa tecnológica durante la audiencia puede generar desconfianza y desviar la atención del litigio hacia la plataforma. La transparencia ex ante es, por ello, una medida de justicia procedimental y no solo de gestión informática.

Autenticidad, ciberseguridad y el riesgo de suplantación digital

La séptima dimensión es tecnológica. Cuanto más se aleja la imagen visible de la apariencia real, mayor importancia adquieren los mecanismos de autenticación. En una videoconferencia ordinaria, el reconocimiento visual puede contribuir informalmente a confirmar la identidad de una persona conocida. El avatar elimina o reduce esa señal y obliga a sustituirla por evidencia institucional más fuerte. Esto no es necesariamente una desventaja: la identificación facial humana también puede fallar, mientras una autenticación multifactor bien diseñada puede proporcionar mayor certeza documental. El problema surge si el sistema elimina la señal visual sin añadir controles equivalentes o superiores.

El modelo propuesto exige al menos autenticación multifactor del juez antes de ingresar, vinculación de la sesión con la cuenta institucional, registro de inicio y cierre, control de cambios de dispositivo, monitoreo de interrupciones y generación de evidencia de integridad. Para audiencias especialmente sensibles podría incorporarse una comprobación de presencia o prueba de vida realizada en el entorno seguro del sistema, siempre que dicho mecanismo respete la normativa de datos personales. La clave es que la defensa y las instancias de revisión puedan confiar razonablemente en que la representación corresponde a la persona designada.

También debe prevenirse la manipulación del flujo de audio y video. La expansión de tecnologías generativas hace técnicamente posible sintetizar voz o imagen con alto nivel de realismo. Aunque el protocolo anunciado no constituye un sistema de inteligencia artificial decisorio, la infraestructura de representación debería impedir que una falla o intrusión introduzca audio generado, repeticiones o sustituciones. Un principio de no autonomía resulta útil: el avatar no debe producir contenido verbal, decidir turnos ni completar frases; su función se limita a representar visualmente señales provenientes en tiempo real del operador humano.

Los registros de auditoría deberían documentar eventos técnicos sin convertirse en una nueva fuente de vigilancia innecesaria. Deben registrarse autenticaciones, cambios críticos, interrupciones y acceso a archivos, pero evitarse la conservación excesiva de información biométrica. La ciberseguridad efectiva no equivale a almacenar todo; consiste en conservar evidencia mínima suficiente para reconstruir incidentes y asegurar la cadena de responsabilidad.

La existencia de un plan de contingencia es igualmente esencial. Si el avatar falla, se congela, se asigna a la persona equivocada o pierde sincronización, el juez debe poder suspender temporalmente la diligencia. Dependiendo del nivel de riesgo, la alternativa puede ser reiniciar en un canal seguro, continuar solo por audio con acuerdo y motivación, trasladar la audiencia o adoptar otra medida. Lo inadmisibles sería continuar una audiencia materialmente ininteligible por el temor administrativo de reprogramarla.

Jueces, víctimas y testigos: una misma tecnología, riesgos jurídicos diferentes

El octavo hallazgo consiste en que no puede aplicarse una única lógica de proporcionalidad a todos los usuarios del avatar. El Consejo de la Judicatura informó que la herramienta también podría utilizarse para sujetos procesales en casos de violencia contra la mujer, delitos de índole sexual y testigos protegidos (Consejo de la Judicatura, 2026a). La finalidad de protección puede ser igualmente legítima, pero las funciones procesales de cada persona son diferentes.

Cuando el avatar corresponde al juez, la cuestión principal es garantizar identidad jurídica, competencia, imparcialidad y presencia humana. El juez no es objeto de valoración testimonial por las partes; su rostro normalmente no constituye evidencia. Por ello, ocultar rasgos faciales puede tener una afectación relativamente limitada si la comunicación y autenticación permanecen intactas. En el caso de un testigo, en cambio, la defensa tiene derecho a interrogar y el tribunal puede valorar elementos de su declaración. La tecnología no debe impedir formular preguntas, percibir pausas relevantes o advertir interferencias externas.

Esto no significa que el derecho de defensa incluya una facultad absoluta de observar el rostro de toda víctima o testigo. Los sistemas jurídicos ya conocen medidas de protección que limitan exposición visual en situaciones justificadas. La cuestión es que la intensidad de la protección debe relacionarse con el riesgo y con la naturaleza de la prueba. Para víctimas de violencia sexual o testigos amenazados, la reducción de exposición puede evitar revictimización y represalias, pero requiere asegurar que la persona declara voluntariamente, sin asistencia indebida y con condiciones que permitan contradicción.

La matriz de decisión, por tanto, debe diferenciar roles. No basta una política general de 'usuarios protegidos'. Cada categoría requiere indicadores de riesgo y salvaguardas específicas. Esta diferenciación es coherente con de Vocht (2022), quien muestra que los efectos de la justicia remota no son homogéneos, y con las directrices de la CEPEJ (2025), que promueven análisis contextual de accesibilidad y equidad.

En términos prácticos, el avatar del juez puede orientarse a neutralidad institucional, mientras la representación de una víctima o testigo podría necesitar soluciones menos antropomórficas si una animación facial generara distorsiones que afecten percepción. La investigación empírica futura debería comparar diferentes interfaces para identificar qué formatos reducen exposición sin introducir sesgos o pérdidas significativas de comprensión.

Examen de proporcionalidad para activar la medida

El noveno resultado es la necesidad de incorporar un examen estructurado antes de utilizar el avatar. Una medida tecnológicamente disponible tiende a normalizarse con rapidez; por ello, la gobernanza debe impedir que lo excepcional se convierta en configuración predeterminedada. El test propuesto contiene cuatro fases: habilitación jurídica, idoneidad, necesidad y balance estricto.

La habilitación jurídica exige identificar la norma que permite la audiencia telemática y la competencia institucional para adoptar medidas de seguridad. Además, debe existir una base suficientemente clara para el tratamiento de datos que realice la plataforma. La idoneidad pregunta si ocultar la imagen reduce de forma plausible el riesgo identificado. Si la amenaza no guarda relación con exposición visual o identificación biométrica, el avatar podría ser irrelevante y otras medidas serían más adecuadas.

La necesidad requiere comparar alternativas. Debe explicarse por qué no bastan restricciones de acceso, medidas físicas, protección policial, cambios de ubicación, reserva de determinados datos u otras herramientas. No se exige demostrar que el avatar es la única opción imaginable, sino que ofrece una mejora relevante de seguridad con una afectación razonablemente menor que alternativas más invasivas, por ejemplo anonimato total de la autoridad.

El balance estricto pondera la gravedad del riesgo frente a la afectación procesal residual. Cuanto más intensa sea la amenaza y más limitada la alteración de garantías, mayor será la justificación. Si la representación impide a la defensa identificar al juez, escuchar correctamente o cuestionar una falla, el costo constitucional aumenta hasta volver desproporcionada la medida. La decisión debe ser motivada y susceptible de revisión, aunque los detalles operativos de seguridad puedan mantenerse reservados.

Se propone además una regla temporal. La autorización debe cubrir una audiencia, etapa o período determinado y revisarse si cambian las circunstancias. El riesgo puede aumentar, disminuir o desaparecer, y una decisión adoptada meses atrás no debería convertirse automáticamente en permiso indefinido. La temporalidad reduce la posibilidad de que la excepción se institucionalice sin evaluación.

Tabla 3. Test de proporcionalidad para el uso de avatares judiciales

Fase	Pregunta de control	Evidencia mínima	Decisión
1. Habilitación	¿Existe base jurídica y competencia para la medida?	Normas aplicables, resolución o decisión identificable	No activar sin base suficiente
2. Riesgo e idoneidad	¿La exposición visual está vinculada con la amenaza?	Perfil o evaluación de riesgo	Activar solo si reduce el riesgo relevante
3. Necesidad	¿Existen alternativas menos restrictivas con eficacia comparable?	Comparación razonada de medidas	Preferir alternativa suficiente menos intensa
4. Balance	¿El beneficio de seguridad supera la afectación procesal residual?	Motivación sobre defensa, publicidad e intermediación	Autorizar, ajustar o rechazar
5. Temporalidad	¿La medida sigue siendo necesaria?	Revisión por audiencia, etapa o período	Mantener, modificar o cesar

Nota: propuesta de los autores. El examen debe adaptarse al rol procesal y al nivel de riesgo.

Modelo de Anonimización Visual Controlada con Doble Trazabilidad

El décimo y principal resultado propositivo es el Modelo de Anonimización Visual Controlada con Doble Trazabilidad (AVCDT). Su premisa es que la seguridad no requiere borrar toda identidad, sino separar aquello que debe protegerse de aquello que debe permanecer controlable. El modelo combina una trazabilidad jurisdiccional, orientada a las garantías procesales, y una trazabilidad tecnológica, orientada a autenticidad e integridad.

La trazabilidad jurisdiccional comprende la identificación del juez, cargo, órgano, competencia, mecanismo de asignación, constancia de participación, posibilidad de recusación y atribución de responsabilidad. Estos datos no necesariamente deben aparecer completos en una transmisión pública, pero sí deben ser accesibles para las partes por vías procesales regulares. La identificación al inicio de la audiencia puede quedar registrada en acta y en el sistema de gestión de causas. La protección del rostro no altera el deber de firmar resoluciones, motivar decisiones ni responder por la actuación jurisdiccional.

La trazabilidad tecnológica acredita que la persona jurídicamente identificada fue quien intervino durante toda la audiencia. Incluye autenticación, vinculación de sesión, registro de eventos críticos, control de integridad del audio y evidencia de que el avatar no produjo contenido autónomo. En vez de confiar en que 'se parece al juez', la plataforma debe ofrecer una cadena verificable de autenticidad. Esta lógica puede incluso superar la identificación informal propia de algunas videollamadas convencionales.

El modelo incorpora además seis principios transversales: excepcionalidad, minimización, presencia humana verificable, no autonomía del avatar, transparencia compensatoria y reversibilidad. La excepcionalidad impide uso rutinario sin riesgo; la minimización limita datos tratados; la presencia humana verificable confirma intervención real; la no autonomía prohíbe generación sustantiva de contenido; la transparencia compensatoria refuerza información institucional cuando se reduce información visual; y la reversibilidad exige que la medida pueda desactivarse o modificarse ante fallas o desaparición del riesgo.

En materia de gobernanza se proponen tres niveles de activación. Un nivel preventivo podría ocultar fondo, ubicación u otros datos no esenciales sin alterar el rostro, aplicable ante riesgo bajo. Un nivel de protección visual reemplazaría el rostro por avatar institucional cuando exista riesgo medio o alto relacionado con exposición biométrica. Un nivel reforzado, reservado para amenaza excepcional, combinaría avatar con controles adicionales de acceso, ubicación segura y medidas físicas. La distorsión de voz no debería integrarse automáticamente y requeriría justificación adicional por su mayor impacto comunicativo.

La arquitectura debe aplicar separación de datos. El sistema que autentica al juez no necesita exponer sus datos de autenticación a quienes visualizan la audiencia; del mismo modo, el motor gráfico no debería acceder a más información personal que la necesaria para representar el avatar. Una segregación adecuada reduce la posibilidad de que una única brecha comprometa simultáneamente identidad, credenciales y grabaciones.

El modelo requiere auditoría independiente. El Consejo de la Judicatura debería mantener indicadores agregados sobre número de activaciones, materias, duración, fallas técnicas, incidentes de seguridad, impugnaciones y resultados de revisión, sin revelar información que ponga en riesgo a operadores. La publicación periódica de datos agregados permitiría evaluar si la herramienta se concentra realmente en casos de riesgo o se extiende progresivamente por conveniencia administrativa.

Finalmente, el AVCDT incorpora una cláusula de revisión empírica. Tras un período inicial de aplicación, deberían estudiarse percepciones de abogados, jueces, fiscales, defensores, víctimas y personas procesadas. Los hallazgos de Mentovich et al. (2023), Factor et al. (2023) y Rossner y Tait (2023) muestran que legitimidad y participación dependen de la experiencia concreta. Una política tecnológica que se considere jurídicamente válida en abstracto puede requerir ajustes si produce confusión, sensación de despersonalización o barreras para determinados grupos.

Tabla 4. Matriz de riesgos y salvaguardas del modelo AVCDT

Riesgo	Efecto potencial	Salvaguarda AVCDT
Anonimato del juez	Imposibilidad de recusar o verificar competencia	Nombre y calidad jurisdiccional disponibles para las partes; constancia en expediente
Suplantación	Intervención de persona distinta a la designada	Autenticación multifactor, cuenta institucional, registro de sesión y eventos
Contenido sintético	Audio o decisiones no emitidas por el juez humano	Principio de no autonomía; bloqueo de generación sustantiva; auditoría
Falla del avatar	Pérdida de comprensión o sincronía	Protocolo de pausa, reinicio o migración a alternativa segura
Exposición biométrica interna	La plataforma conserva más datos que la audiencia pública	Minimización, retención limitada, cifrado y evaluación de impacto
Uso rutinario	La excepción se convierte en práctica general	Perfil de riesgo, motivación, temporalidad y revisión
Opacidad pública	Menor confianza por no ver el rostro	Transparencia compensatoria, identificación jurídica y reglas públicas
Impacto en testigos	Distorsión de señales útiles para contradicción	Evaluación diferenciada por rol, prueba de voluntariedad y condiciones de declaración
Acceso desigual	Partes con menor capacidad tecnológica	Soporte, pruebas previas, canales alternativos y suspensión ante desventaja material
Filtración del registro real	Reidentificación y seguimiento del operador	Acceso escalonado, cifrado, registro de accesos y eliminación segura

Nota: elaboración propia. Las salvaguardas son acumulativas y deben calibrarse según contexto.

Discusión integrada: legitimidad, humanidad y diseño institucional

Los resultados permiten rechazar dos extremos. El primero afirma que cualquier ocultamiento del rostro produce automáticamente una justicia sin rostro incompatible con el debido proceso. El segundo supone que, por tratarse de una medida de seguridad, la interfaz carece de relevancia constitucional. El análisis comparado muestra que ambas posiciones simplifican un problema más complejo. La constitucionalidad no depende exclusivamente de la apariencia gráfica, sino de la arquitectura de control que rodea su uso.

La experiencia de los tribunales sin rostro aporta una prohibición de fondo contra la opacidad sobre quién juzga y bajo qué garantías. No obliga necesariamente a exponer biometría facial en cualquier circunstancia. A su vez, la investigación sobre justicia remota demuestra que los medios modifican participación y

percepción, de modo que no basta declarar que el procedimiento mantiene intactas todas las garantías. La validez debe demostrarse mediante diseño, práctica y posibilidad de revisión.

Onțanu y Tjong Tjin Tai (2025) plantean que la digitalización transforma la geografía de la justicia y obliga a reconsiderar cómo las tecnologías se relacionan con garantías procedimentales. La medida ecuatoriana constituye un ejemplo especialmente claro: la autoridad está presente, pero su representación se separa de su cuerpo visible; la audiencia es pública, pero no toda información visual se expone; la identidad existe, pero se distribuye en distintos niveles de acceso. Este desacoplamiento exige sustituir intuiciones basadas en presencia física por criterios jurídicos de verificabilidad.

La legitimidad del avatar dependerá también del lenguaje institucional utilizado. Presentarlo como una forma de 'ocultar al juez' puede activar asociaciones históricas negativas; describirlo simplemente como innovación tecnológica puede minimizar riesgos reales. Una comunicación adecuada debería explicar con precisión que se protege la representación biométrica sin eliminar identificación procesal, que el juez continúa siendo humano y que la medida está sometida a condiciones de activación. La claridad conceptual es parte del diseño de confianza.

La política puede producir beneficios adicionales si se implementa correctamente. Reducir exposición facial podría ampliar la capacidad de juzgadores amenazados para continuar determinadas diligencias sin desplazamientos o exposición innecesaria, disminuir incentivos de intimidación visual y fortalecer continuidad del servicio. Sin embargo, tales beneficios no deben presumirse; requieren medición. Indicadores de incidentes, suspensiones, impugnaciones y satisfacción de usuarios permitirán evaluar si la herramienta realmente mejora seguridad sin deteriorar calidad procesal.

La dimensión tecnológica tampoco debe quedar encapsulada en áreas informáticas. Los requisitos de autenticación, retención y diseño de interfaz son decisiones con consecuencias jurídicas. De forma inversa, las garantías procesales deben traducirse en especificaciones técnicas. Si la norma exige que la identidad del juez sea verificable, el sistema debe tener una función que lo haga posible; si se exige registro de incidentes, la plataforma debe producirlo; si el avatar no puede generar contenido, esa limitación debe ser comprobable. La gobernanza adecuada requiere diálogo continuo entre derecho, ciberseguridad, protección de datos y experiencia de usuario.

La comparación con la literatura internacional muestra además que la participación no es un efecto automático de la conectividad. Mentovich et al. (2023) evidencian la relación entre justicia procedimental, acceso y legitimidad; Factor et al. (2023) destacan la importancia de cómo se experimenta la videoconferencia; Rossner y Tait (2023) se concentran en presencia y participación. En conjunto, estos estudios sugieren que el avatar debería evaluarse no solo por si funciona técnicamente, sino por si los participantes comprenden quién habla, se sienten escuchados y pueden intervenir en condiciones efectivas.

El uso de avatares para víctimas y testigos exige un programa de investigación separado. La misma tecnología puede ser protectora para una víctima y, al mismo tiempo, generar preguntas sobre percepción de testimonio o apoyo externo. La solución no debe basarse en una oposición entre protección y contradicción, sino en un diseño que garantice ambas en el mayor grado posible. Esto puede implicar salas seguras, supervisión de entorno, canales diferenciados de verificación y decisiones motivadas sobre el nivel de transformación visual.

Otra cuestión relevante es la conservación de la solemnidad. La autoridad judicial posee una dimensión simbólica que no debe confundirse con teatralidad. Rowden y Wallace (2018) explican que la imagen del juez participa en la construcción del rol. Un avatar institucional demasiado lúdico o expresivo puede trivializar la diligencia; uno excesivamente robótico puede transmitir distancia. El diseño debería ser sobrio, estable y reconocible como representación oficial, sin intentar imitar fotorrealismo ni incorporar rasgos que permitan reidentificación.

Finalmente, la medida ecuatoriana puede convertirse en referencia regional si desarrolla un estándar exportable de protección con responsabilidad. En contextos donde crimen organizado y amenazas buscan influir en operadores, las instituciones necesitan herramientas adaptadas a riesgos digitales. Pero la innovación solo será sostenible si incorpora desde el inicio los límites que la hacen legítima. La ventaja del AVCDT es precisamente que no presenta seguridad y debido proceso como objetivos mutuamente excluyentes: organiza la tecnología para que la reducción de exposición biométrica se compense con mayor trazabilidad jurídica y técnica.

Implicaciones para la regulación y la práctica judicial ecuatoriana

Del análisis se desprenden varias implicaciones normativas. En primer lugar, las reglas esenciales de activación deberían ser públicas. La ciudadanía y las partes necesitan conocer qué autoridad puede disponer el avatar, cuáles son los criterios generales de riesgo, qué derechos conservan y cómo se registra la decisión. Pueden reservarse detalles operativos cuya divulgación facilite ataques, pero no la arquitectura jurídica básica. La seguridad informática no debe convertirse en argumento para ocultar reglas procesales.

En segundo lugar, la motivación debería formar parte del expediente. Una resolución breve puede indicar que existe una evaluación institucional de riesgo, la finalidad perseguida, el período de aplicación y las salvaguardas previstas, sin revelar domicilios, rutas, fuentes de inteligencia u otros datos sensibles. Este diseño permite control judicial y, a la vez, evita que la motivación se convierta en manual para el agresor.

En tercer lugar, debe definirse un mecanismo de objeción. La parte que considere afectado su derecho de defensa debería poder plantear de manera inmediata problemas de autenticidad, comprensión o proporcionalidad. No toda objeción obligará a mostrar el rostro real, pero sí a ofrecer una respuesta motivada y, cuando corresponda, una verificación alternativa de identidad. La garantía consiste en poder cuestionar la regularidad, no en imponer una forma específica de imagen.

En cuarto lugar, la protección de datos requiere gobernanza contractual si intervienen proveedores tecnológicos. Los contratos deberían definir roles de responsable y encargado, finalidades, localización y retención de datos, subencargados, medidas de seguridad, notificación de incidentes y prohibición de reutilizar imágenes o metadatos para entrenamiento, publicidad o finalidades propias del proveedor. La justicia no puede depender de términos de servicio diseñados para videollamadas comerciales ordinarias.

En quinto lugar, la capacitación debe incluir componentes jurídicos y comunicativos. El juez necesita saber cuándo solicitar o aceptar la medida, cómo informar a las partes, qué hacer ante una falla y cómo documentar incidentes. El personal técnico debe comprender por qué determinadas funciones, como sustitución automática de voz, pueden ser incompatibles con garantías. Abogados y defensores también requieren información para distinguir una representación protegida de una anomalía técnica.

En sexto lugar, el sistema debería someterse a pruebas de accesibilidad. Personas con discapacidad auditiva o visual, usuarios con conexiones limitadas y participantes que requieren intérprete pueden experimentar barreras diferentes. La CEPEJ (2025) insiste en que la integración de audiencias remotas debe preservar acceso a la justicia. Un avatar que dificulte lectura labial, por ejemplo, puede requerir subtítulos, intérprete o una configuración alternativa. La seguridad no puede trasladar el costo de protección a quienes ya enfrentan barreras de acceso.

En séptimo lugar, la evaluación institucional debe incluir un mecanismo de revisión periódica. Los sistemas tecnológicos cambian con rapidez y una solución segura hoy puede presentar vulnerabilidades futuras. Deben revisarse algoritmos de transformación, librerías, proveedores, protocolos de cifrado y compatibilidad con plataformas. También deben reevaluarse los riesgos biométricos conforme evolucionen técnicas de reidentificación.

Estas implicaciones muestran que el avatar es menos un objeto que un sistema socio-técnico. Su legitimidad emerge de la combinación entre norma, decisión judicial, infraestructura, interfaz, capacitación y auditoría. Un mismo gráfico puede ser constitucionalmente aceptable en una arquitectura con trazabilidad y problemático en otra sin controles. Por ello, el debate jurídico debe escapar de la imagen aislada y concentrarse en el conjunto de procesos que la producen y gobiernan.

Conclusiones

La aprobación del uso de avatares digitales institucionales en determinadas audiencias telemáticas sitúa a Ecuador frente a una de las expresiones más novedosas de la justicia digital regional. La medida no introduce, según la información oficial disponible, un juez artificial ni una delegación de la función jurisdiccional. Introduce una mediación visual destinada a reducir exposición biométrica de jueces y otros intervinientes que enfrentan riesgos. Esa precisión conceptual es el punto de partida para cualquier evaluación rigurosa.

El contexto de seguridad ofrece una finalidad constitucionalmente relevante. El marco ecuatoriano reconoce medidas de protección para servidores judiciales y el diagnóstico institucional de 2026 evidencia amenazas y hechos de violencia. Proteger al juzgador puede contribuir a preservar independencia y continuidad del servicio. Sin embargo, una finalidad legítima no elimina la obligación de justificar cada restricción. El avatar debe aplicarse de manera excepcional, motivada, temporal y vinculada con un riesgo que guarde relación real con la exposición visual o biométrica.

La principal conclusión jurídica es que anonimización visual y anonimato jurisdiccional deben mantenerse separados. El rostro de un juez puede ser protegido sin que desaparezcan su nombre, cargo, competencia, mecanismo de asignación y responsabilidad. El precedente interamericano sobre jueces sin rostro advierte contra sistemas en los que las partes no pueden controlar quién las juzga. El modelo ecuatoriano será compatible con ese estándar únicamente si la protección biométrica no impide recusación, verificación de competencia ni atribución de responsabilidad.

La intermediación tampoco exige necesariamente una reproducción facial fotorrealista. Lo indispensable es que el juez humano esté presente en tiempo real, escuche, intervenga, dirija la diligencia y adopte personalmente las decisiones. La literatura sobre justicia remota demuestra, no obstante, que la interfaz influye en

participación y legitimidad. Por ello, el avatar debe preservar señales comunicativas suficientes, evitar desincronización y dejar inequívocamente claro que representa a una autoridad humana autenticada.

La publicidad debe reinterpretarse como control institucional y no como derecho ilimitado a capturar datos biométricos. Una audiencia puede seguir siendo pública si la sociedad conoce quién juzga, qué ocurre y qué se decide, aunque determinadas características físicas se oculten por seguridad. La reducción de información visual debe compensarse con mayor transparencia sobre reglas, identidad jurídica, motivación y mecanismos de revisión.

Desde la protección de datos, la herramienta solo es coherente si minimiza realmente el tratamiento. El sistema debe documentar qué datos faciales procesa, evitar retención innecesaria, limitar accesos y evaluar riesgos. No sería aceptable que la versión pública oculte el rostro mientras la plataforma crea una base biométrica extensa sin finalidad definida. La protección desde el diseño exige que la arquitectura interna sea tan restrictiva como la interfaz externa pretende ser protectora.

El aporte de esta investigación es el Modelo de Anonimización Visual Controlada con Doble Trazabilidad. La trazabilidad jurisdiccional garantiza que pueda saberse quién ejerció jurisdicción, con qué competencia y bajo qué responsabilidad. La trazabilidad tecnológica acredita que esa persona fue efectivamente quien participó y que el avatar no generó contenido autónomo. Ambas cadenas de verificabilidad permiten sustituir el reconocimiento visual por mecanismos más robustos de autenticidad sin sacrificar control procesal.

El modelo se complementa con principios de excepcionalidad, minimización, presencia humana verificable, no autonomía, transparencia compensatoria y reversibilidad. También exige un test de proporcionalidad previo y mecanismos diferenciados según se trate de jueces, víctimas o testigos. La misma solución gráfica no produce idénticos efectos para todos los roles procesales y, por ello, la regulación debe ser funcionalmente diferenciada.

La principal limitación del estudio es temporal: al cierre de la revisión, el texto técnico íntegro del protocolo aprobado el 7 de agosto de 2026 no se encontraba localizado en acceso público mediante las búsquedas realizadas. Las conclusiones se basan en las características oficialmente comunicadas y en el marco jurídico vigente, no en supuestos sobre disposiciones no publicadas. Una vez que el documento completo esté disponible y exista experiencia de aplicación, será necesario contrastar estas salvaguardas con la regulación efectiva y desarrollar estudios empíricos sobre confianza, participación, incidentes y resultados.

En síntesis, el dilema no debe formularse como una elección entre mostrar el rostro del juez o renunciar al debido proceso. El desafío consiste en diseñar una justicia capaz de proteger a la persona que administra jurisdicción sin esconder la jurisdicción misma. La democracia constitucional puede admitir que, ante un riesgo objetivo, la pantalla no revele los rasgos biométricos del juzgador; lo que no puede admitir es que detrás del avatar se vuelvan inciertos su identidad jurídica, su competencia, su responsabilidad o su presencia humana.

Referencias

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

<https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-20/transparencia-2015/literal-a/a2/2018-08-01-constitucion-reformada.pdf>

Asamblea Nacional del Ecuador. (2009). Código Orgánico de la Función Judicial. Registro Oficial Suplemento No. 544, 9 de marzo de 2009, y reformas vigentes. <https://www.funcionjudicial.gob.ec/resources/pdf/normativa/codigoorganicoFJ.pdf>

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento No. 180, 10 de febrero de 2014, y reformas vigentes. https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-20/codigo_organico_integral_penal-registro-oficial.pdf

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Quinto Suplemento del Registro Oficial No. 459, 26 de mayo de 2021. <https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos>

Consejo de la Judicatura. (2021). Protocolo para la realización de videoaudiencias. Versión septiembre de 2021. <https://www.funcionjudicial.gob.ec/resources/pdf/CJ-Protocolo%20de%20video%20audiencias%20CJ%20-%20Versi%C3%B3n%20sept-2021.pdf>

Consejo de la Judicatura. (2026a, 7 de agosto). Pleno aprueba uso de avatares digitales para proteger a los servidores jurisdiccionales en audiencias telemáticas. <https://www.funcionjudicial.gob.ec/pleno-aprueba-uso-de-avatares-digitales-para-proteger-a-los-servidores-jurisdiccionales-en-audiencias-telematicas/>

Consejo de la Judicatura. (2026b, 7 de agosto). Plan de Seguridad Integral para servidores judiciales fue aprobado por el Pleno del Consejo de la Judicatura. <https://www.funcionjudicial.gob.ec/plan-de-seguridad-integral-para-servidores-judiciales-fue-aprobado-por-el-pleno-del-consejo-de-la-judicatura/>

Corte Interamericana de Derechos Humanos. (1999). Caso Castillo Petruzzi y otros vs. Perú. Fondo, reparaciones y costas. Sentencia de 30 de mayo de 1999. Serie C No. 52. https://www.corteidh.or.cr/docs/casos/articulos/seriec_52_esp.pdf

Council of Europe, European Commission for the Efficiency of Justice. (2021). Guidelines on videoconferencing in judicial proceedings. <https://www.coe.int/en/web/cepej/cepej-tools-on-cyberjustice-and-artificial-intelligence>

Council of Europe, European Commission for the Efficiency of Justice. (2025). Guide on the use and development of remote hearings. CEPEJ(2025)3. <https://rm.coe.int/cepej-2025-3-en-guide-for-remote-hearings-2763-8911-6430-1/1680b6bb7b>

de Vocht, D. L. F. (2022). Trials by video link after the pandemic: The pros and cons of the expansion of virtual justice. China-EU Law Journal, 8, 33-44. <https://doi.org/10.1007/s12689-022-00095-9>

- Donoghue, J. (2017). The rise of digital justice: Courtroom technology, public participation and access to justice. *The Modern Law Review*, 80(6), 995-1025. <https://doi.org/10.1111/1468-2230.12300>
- Factor, R., Kariti, D., Lernau, H., & Yaffe Ayubi, D. (2023). Videoconferencing in legal hearings and procedural justice. *Victims & Offenders*, 18(8), 1557-1579. <https://doi.org/10.1080/15564886.2023.2248465>
- Kamber, K. (2022). The right to a fair online hearing. *Human Rights Law Review*, 22(2), ngac006. <https://doi.org/10.1093/hrlr/ngac006>
- Legg, M. (2021). The COVID-19 pandemic, the courts and online hearings: Maintaining open justice, procedural fairness and impartiality. *Federal Law Review*, 49(2), 161-184. <https://doi.org/10.1177/0067205X21993139>
- Mentovich, A., Prescott, J. J., & Rabinovich-Einy, O. (2023). Legitimacy and online proceedings: Procedural justice, access to justice, and the role of income. *Law & Society Review*, 57(2), 189-213. <https://doi.org/10.1111/lasr.12653>
- Onțanu, E. A., & Tjong Tjin Tai, E. (2025). Digital technology and procedural justice: Towards a geography of justice. *Tilburg Law Review*, 30(2), 96-119. <https://doi.org/10.5334/tlrl.422>
- Rossner, M., & Tait, D. (2023). Presence and participation in a virtual court. *Criminology & Criminal Justice*, 23(1), 135-157. <https://doi.org/10.1177/17488958211017372>
- Rowden, E., & Wallace, A. (2018). Remote judging: The impact of video links on the image and the role of the judge. *International Journal of Law in Context*, 14(4), 504-524. <https://doi.org/10.1017/S1744552318000216>
- Superintendencia de Protección de Datos Personales. (2026). Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales, versión 2. https://spdp.gob.ec/wp-content/uploads/2026/06/guia_v2_vfinal.pdf