

Identidades audiovisuales *post mortem*

Entre la preservación de la memoria y la amenaza de la manipulación



Jorge Caldera-Serrano

Universidad de Extremadura. Facultad de Ciencias de la Documentación y la Comunicación, Badajoz, España /
jcalser@unex.es | <https://orcid.org/0000-0002-4049-1057>

Resumen

El estudio analiza la identidad audiovisual digital *post mortem* desde la doble perspectiva de su preservación como parte de la memoria individual y colectiva, y los riesgos asociados a su manipulación mediante tecnologías de inteligencia artificial. Para ello, se realiza una revisión bibliográfica sistemática en bases de datos académicas de alto impacto y fuentes especializadas, identificando los principales enfoques sobre identidad digital, preservación audiovisual y *deepfakes*. Los hallazgos destacan la creciente relevancia de la identidad audiovisual en la construcción de la memoria en la era digital, así como la vulnerabilidad de estos registros ante la manipulación. Se discuten estrategias de preservación mediante archivado digital, gestión de metadatos y autenticación con *blockchain*, contrastadas con los desafíos que plantea la evolución tecnológica. En conclusión, se enfatiza la necesidad de regulaciones claras y herramientas de verificación avanzadas para evitar la falsificación de la memoria digital. La preservación de la identidad audiovisual *post mortem* requiere un enfoque interdisciplinario que combine tecnología, ética y legislación para garantizar su autenticidad y protección en el tiempo.

Palabras clave

Identidad audiovisual post
mortem
Preservación digital
Manipulación digital
Deepfakes
Inteligencia artificial
Memoria digital

Post mortem audiovisual identities: between the preservation of memory and the threat of manipulation

Abstract

This study examines *post mortem* digital audiovisual identity from a dual perspective: its preservation as part of individual and collective memory and the risks associated with its manipulation through artificial intelligence technologies. To achieve this, a systematic literature review was conducted using high-impact academic databases and specialized sources, identifying key approaches to digital identity, audiovisual preservation, and deepfakes. The findings highlight the growing relevance of

Keywords

Post mortem audiovisual identity
Digital preservation
Digital manipulation
Deepfakes
Artificial intelligence
Digital memory

audiovisual identity in shaping memory in the digital age, as well as the vulnerability of these records to be manipulated. Preservation strategies such as digital archiving, metadata management, and blockchain authentication are discussed, and contrasted with the challenges posed by technological advancements. In conclusion, the study emphasizes the need for clear regulations and advanced verification tools to prevent the falsification of digital memory from happening. The preservation of *post mortem* audiovisual identity requires an interdisciplinary approach that integrates technology, ethics, and legislation to ensure its authenticity and long-term protection.

Artículo recibido: 19-02-2025. Aceptado: 30-10-2025.

Introducción

En la era digital, la identidad de una persona ya no se limita a su existencia física ni a su legado material, sino que se extiende a los entornos virtuales donde interactúa, genera contenido y deja una huella informacional que trasciende su propia vida. Las identidades digitales, entendidas como el conjunto de datos, interacciones y representaciones virtuales de los individuos en distintos espacios en línea, desempeñan un papel central en la construcción de la memoria individual y colectiva (UNESCO, 2003; Reda, 2024). Dentro de esta dimensión, la identidad audiovisual digital adquiere una relevancia particular debido a la preeminencia de la imagen y el sonido en la comunicación contemporánea. La proliferación de plataformas audiovisuales, redes sociales con un fuerte componente visual y archivos multimedia ha convertido a la imagen y la voz en elementos esenciales para la configuración y proyección de la identidad personal en el entorno digital (Robles-Carrillo, 2024). Su combinación permite construir narrativas con un alto grado de realismo e inmersión, dotando a los registros audiovisuales de un valor documental único para la preservación de la memoria.

A nivel institucional y colectivo, los archivos audiovisuales desempeñan un papel crucial en la conservación del patrimonio cultural e histórico. Videotecas, filmotecas y archivos de televisión constituyen repositorios fundamentales donde se almacenan imágenes y voces que documentan la evolución de sociedades y comunidades (León-Moreno, Zapico-Alonso y Caldera-Serrano, 2016). En el ámbito individual, la expansión de dispositivos móviles y redes sociales ha propiciado la creación de archivos personales espontáneos, generando un registro visual y sonoro de la vida cotidiana que, en muchas ocasiones, carece de una planificación orientada a su conservación a largo plazo (Stokes, 2012).

No obstante, esta riqueza documental enfrenta una problemática fundamental: la fragilidad de la identidad audiovisual *post mortem* ante las nuevas tecnologías de manipulación digital. Con el avance de la inteligencia artificial y la sofisticación de técnicas de edición, los contenidos audiovisuales pueden ser modificados, reinterpretados o falsificados con gran precisión. Herramientas como los *deepfakes* (Kietzmann et al, 2020) permiten la generación de videos sintéticos en los que rostros, expresiones y voces pueden ser alterados o reconstruidos, lo que representa un desafío significativo para la autenticidad de la memoria audiovisual (Boté-Vericad y Vállez, 2022). Estas manipulaciones pueden responder a intereses diversos, desde la experimentación tecnológica y el entretenimiento hasta la desinformación, la explotación comercial o la reescritura deliberada de la historia (Ajder et al, 2019).

La identidad audiovisual *post mortem* se encuentra, por tanto, en una encrucijada entre su preservación y su posible manipulación. Mientras que los archivos audiovisuales, tanto personales como institucionales, constituyen herramientas fundamentales para la continuidad de la memoria, las tecnologías emergentes facilitan la alteración

y resignificación de estos registros, comprometiendo su fiabilidad (Póveda López, Caldera Serrano y Polo Carrión, 2010). Este dilema no solo afecta a las identidades individuales, sino también a las colectivas, entendidas como aquellas que representan a movimientos sociales, partidos políticos, sindicatos o asociaciones (Vanhaecht, Mapgaonkar y Romanovski, 2020). En estos casos, la manipulación de materiales audiovisuales puede tener implicaciones profundas en la configuración del discurso público, la legitimación de narrativas históricas y la influencia en la opinión social (Vaccari y Chadwick, 2020), convirtiéndose en un recurso estratégico con impactos potencialmente significativos en múltiples ámbitos.

Objetivo, objeto y metodología

El presente estudio tiene como objetivo analizar el fenómeno de la identidad audiovisual *post mortem* desde una doble perspectiva complementaria: por un lado, la preservación de la identidad digital audiovisual como un componente fundamental de la memoria individual (Stokes, 2012) y colectiva, explorando las estrategias y herramientas disponibles para su conservación a largo plazo; y, por otro, la problemática de la manipulación digital, con especial atención a las técnicas impulsadas por la inteligencia artificial, como los *deepfakes* (Boté-Vericad y Váñez, 2022; Kietzmann et al, 2020) y la alteración sintética de imágenes y voces. A través de este enfoque, se busca no solo comprender los desafíos que plantea la pervivencia de la identidad audiovisual tras la muerte de un individuo o la transformación de las representaciones de colectivos en el entorno digital, sino también proponer estrategias que permitan mitigar los riesgos asociados a su alteración indebida.

Los objetos de estudio de esta investigación se estructuran en torno a dos ejes fundamentales. En primer lugar, se abordan las identidades digitales *post mortem*, distinguiendo entre las individuales y las colectivas. Mientras que las primeras están vinculadas a la huella digital dejada por una persona fallecida, las segundas engloban a entidades como partidos políticos, asociaciones, movimientos sociales o sindicatos, cuyos registros audiovisuales pueden ser objeto de reinterpretación o manipulación con distintos fines. En segundo lugar, el estudio se centra en la manipulación digital, entendida como el conjunto de técnicas y procesos que alteran, distorsionan o falsifican la representación audiovisual de individuos o colectivos. A partir de estos objetos de estudio, se examinarán diversas estrategias para garantizar la preservación fiel de la identidad audiovisual en un contexto donde la tecnología permite intervenciones cada vez más sofisticadas y difíciles de detectar.

La metodología empleada en esta investigación ha consistido en una revisión bibliográfica sistemática realizada en el mes de febrero de 2025. Se han consultado bases de datos académicas de alto impacto, como Web of Science (WoS), Scopus y Google Académico, con el fin de identificar los estudios más relevantes sobre los conceptos clave del estudio. La búsqueda se realizó en español e inglés utilizando términos como “identidad digital”, “identidad digital *post mortem*”, “identidad audiovisual”, “preservación digital”, “memoria digital”, “archivos audiovisuales”, “*deepfakes*”, “manipulación de imágenes”, “manipulación audiovisual”, “ética de la inteligencia artificial”, “verificación digital”, “reconstrucción facial IA”, “sintetización de voz” y “desinformación audiovisual”. Adicionalmente, se han consultado fuentes complementarias en páginas web especializadas en el análisis de la manipulación audiovisual, como el Observatorio de Fake News y Desinformación, el MIT Media Lab, el Center for Humane Technology y el Forensic Architecture, con el objetivo de examinar la evolución reciente de las técnicas de manipulación y sus implicaciones éticas y sociales. La combinación de estas fuentes ha permitido construir un marco teórico robusto que sustente el análisis y la propuesta de estrategias para la protección de la identidad audiovisual *post mortem*. No

obstante, los resultados de la revisión bibliográfica fueron sometidos a una evaluación y valoración para realizar una selección operativa para alcanzar el objetivo del trabajo, dando como resultados este estudio prospectivo que marca el estado de la cuestión y los desafíos sobre las identidades audiovisuales *post mortem*.

El período temporal cubierto fue 2000–febrero de 2025, con el objetivo de incluir tanto la literatura clásica sobre preservación digital (incluido el desarrollo y adopción del modelo OAIS) como la literatura reciente relativa a técnicas de manipulación audiovisual y a la regulación emergente.

Se han tenido presente los siguientes criterios de inclusión: i) trabajos académicos (artículos, capítulos, tesis) publicados en dichas bases de datos; ii) estudios técnicos y revisiones relevantes para preservación digital, metadatos, autenticación o manipulación audiovisual; iii) documentos en español o inglés; iv) textos que abordaran explícitamente aspectos vinculados a la identidad audiovisual *post mortem*, preservación, estándares de metadatos o técnicas de verificación. Mientras que los criterios de exclusión son: i) materiales puramente divulgativos sin referencia a metodología o a evidencia; ii) duplicados; iii) trabajos cuya única mención a los temas de interés fuera tangencial y no aportara datos ni propuestas metodológicas.

Los documentos fueron evaluados para atender a su calidad y especificidad, sometiéndolos a una revisión crítica cualitativa según una rúbrica adaptada a la investigación documental (criterios: pertinencia temática, claridad metodológica, novedad, nivel de evidencia).

La identidad digital audiovisual *post mortem*

En el entorno digital, la identidad audiovisual se ha convertido en un componente esencial de la memoria individual y colectiva, moldeando la representación de personas y entidades tanto en vida como tras su fallecimiento. La proliferación de plataformas como YouTube, TikTok e Instagram, Facebook (Stokes, 2012), así como las videotecas de medios de comunicación, ha consolidado el contenido audiovisual como un archivo de memoria accesible y perdurable (León Gavilanez, 2023). Sin embargo, la permanencia de estos registros plantea cuestiones fundamentales sobre su preservación, control y posibles manipulaciones (UNESCO, 2003).

La identidad digital *post mortem* (Reda, 2024) comprende los registros audiovisuales que permanecen tras la muerte de un individuo o la desaparición de una entidad colectiva, generando debates sobre su gestión ética y legal. Más allá de la conservación de imágenes y grabaciones, esta dimensión involucra la posibilidad de alteración, resignificación o uso indebido de dichos materiales. Un aspecto central de este debate radica en la delimitación entre usos legítimos, como homenajes o reconstrucciones históricas, y prácticas que podrían distorsionar la memoria original de la persona o colectivo representado (Stokes, 2012).

Desde una perspectiva analítica, es crucial diferenciar entre la identidad audiovisual individual y la colectiva. La primera abarca registros que representan a un individuo específico, como entrevistas, grabaciones de voz y videos personales, cuya gestión puede recaer en familiares, instituciones o plataformas tecnológicas. En cambio, la identidad audiovisual colectiva (Vanhaecht, Mapgaonkar y Romanovski, 2020) está vinculada a grupos, organizaciones o movimientos sociales que construyen su imagen a partir de materiales audiovisuales distribuidos a lo largo del tiempo. La manipulación de estos archivos no solo afecta la percepción de los individuos que

los integran, sino que también influye en la interpretación pública de los valores e ideologías que representan. A diferencia de la identidad individual, la colectiva suele estar sujeta a disputas sobre su autenticidad y significado en función de intereses políticos, sociales o económicos (Vanhaecht, Mapgaonkar y Romanovskiy, 2020).

El avance de la inteligencia artificial ha intensificado los riesgos de manipulación audiovisual *post mortem*, posibilitando la alteración de imágenes y voces con un realismo sin precedentes. Técnicas como los *deepfakes* (Kietzmann et al, 2020) han abierto la puerta a usos engañosos de registros audiovisuales, con implicaciones que van desde la creación de narrativas ficticias hasta la desinformación (Vaccari y Chadwick, 2020) y la explotación comercial. Ejemplos recientes evidencian la creciente sofisticación de estas prácticas: en 2019, una empresa de inteligencia artificial recreó digitalmente al actor Peter Cushing para la película *Rogue One: A Star Wars Story*, suscitando un debate sobre los límites éticos del uso póstumo de la imagen de una persona fallecida (Martin y Jonson, 2024). De igual forma, en 2020, un documental sobre Anthony Bourdain utilizó inteligencia artificial para sintetizar su voz sin una advertencia explícita, lo que generó controversia sobre la manipulación de su identidad *post mortem* (Arnold et al, 2017). En el ámbito político, los *deepfakes* han sido empleados para recrear discursos de líderes históricos en contextos alterados, lo que plantea preocupaciones sobre la integridad de la memoria histórica y la credibilidad de los archivos digitales (Paris y Donovan, 2019).

Estos desafíos han impulsado una reflexión sobre los derechos de control y uso de la identidad audiovisual *post mortem*. ¿Quién debe decidir sobre la permanencia de estos registros? ¿Hasta qué punto es legítimo modificar la imagen y voz de un fallecido sin su consentimiento? ¿Qué mecanismos pueden garantizar la autenticidad de los archivos digitales frente a la manipulación? Estas cuestiones siguen abiertas en el debate académico y profesional, evidenciando la necesidad de estrategias para proteger la memoria audiovisual en un contexto de creciente sofisticación tecnológica.

Preservación de la identidad audiovisual digital *post mortem*

La preservación de la identidad audiovisual digital *post mortem* se ha convertido en un desafío fundamental en la era de la información (Arnold et al, 2017). La memoria individual y colectiva está cada vez más vinculada a registros digitales, los cuales se encuentran expuestos a obsolescencia tecnológica, manipulación y falta de regulación específica. A medida que la inteligencia artificial ha facilitado la creación de contenido sintético, los riesgos de falsificación de la memoria digital han aumentado, comprometiendo la autenticidad de los archivos audiovisuales. En este contexto, la implementación de estrategias de preservación, autenticación y regulación se vuelve esencial para garantizar la protección de estos registros en el largo plazo.

Estrategias de conservación

La obsolescencia tecnológica constituye una amenaza significativa para la preservación de registros audiovisuales digitales, ya que la constante evolución de formatos de archivo, dispositivos de almacenamiento y sistemas operativos puede volver inaccesibles documentos sin la infraestructura adecuada (Rosenthal, 2010). A esta problemática se suma la obsolescencia programada (Malinauskaite y Erdem, 2021), estrategia adoptada por fabricantes de hardware y software para limitar artificialmente la vida útil de los dispositivos y sistemas, obligando a los usuarios a renovarlos periódicamente. En el ámbito de la preservación digital, la obsolescencia programada se evidencia en la discontinuación de formatos propietarios, la incompatibilidad de versiones de software y la falta de soporte

para dispositivos antiguos, lo que compromete la accesibilidad a largo plazo de los archivos audiovisuales (Caldera Serrano y Arranz Escacha, 2012). Para abordar estos desafíos, es necesario implementar estrategias de conservación a largo plazo, combinando estándares abiertos, almacenamiento distribuido y tecnologías emergentes que garanticen la accesibilidad y autenticidad de los registros digitales.

Una de las principales soluciones es el uso de formatos de archivo abiertos y de larga duración, como Matroska (MKV) y Broadcast WAV (BWF), que ofrecen mayor estabilidad y compatibilidad en el tiempo. El archivo digital de la BBC (BBC Archive), por ejemplo, ha migrado gran parte de su material audiovisual a formatos estándar abiertos para evitar la dependencia de tecnologías propietarias que podrían quedar obsoletas (Panorama Audiovisual, 2025). Junto con el uso de estos formatos, la implementación de estándares de metadatos como PREMIS y Dublin Core facilita la organización, gestión y recuperación de la información a lo largo del tiempo. Un caso relevante es el de la Library of Congress (Estados Unidos), que ha adoptado un sistema de archivado basado en estos estándares para la preservación digital de su vasta colección de materiales audiovisuales (León Gavilanez, 2023).

La normalización de esquemas de metadatos es una estrategia clave para la preservación digital. El modelo OAIS destaca la necesidad de disponer de la información de representación suficiente para que un objeto digital pueda ser interpretado por la comunidad designada en el futuro. En la práctica, esto exige combinar metadatos descriptivos (p. ej. Dublin Core), estructurales (p. ej. METS) y de preservación (p. ej. PREMIS) para garantizar tanto la recuperación como la comprensión y la trazabilidad de las acciones de preservación. En el caso de materiales audiovisuales, esquemas especializados (por ejemplo, EBUCore, PBCore) facilitan la captura de información técnica y contextual necesaria para mantener la integridad de la representación audiovisual a lo largo del tiempo.

Asimismo, Ochoa-Gutiérrez, Sáenz Giraldo y Tirado Tamayo (2021) destacan, a partir de experiencias en repositorios institucionales, la utilidad del modelo OAIS como marco de referencia para la gestión de la preservación digital. Su estudio enfatiza que la adopción del OAIS requiere articular políticas institucionales claras y esquemas de metadatos robustos que garanticen la interoperabilidad y la sostenibilidad a largo plazo.

Otra estrategia clave es el desarrollo de infraestructuras de conservación y copias de seguridad en entornos distribuidos. Iniciativas como LOCKSS (Lots of Copies Keep Stuff Safe), desarrollada por la Universidad de Stanford, utilizan múltiples copias de un mismo archivo almacenadas en diferentes servidores para prevenir la pérdida de datos debido a fallos técnicos o desastres naturales (Schonfeld, 2018). A nivel institucional, la Digital Preservation Network (DPN) ha desarrollado una infraestructura que permite replicar archivos en múltiples ubicaciones, reduciendo la dependencia de un único repositorio centralizado y asegurando su accesibilidad a largo plazo.

En respuesta a la obsolescencia tecnológica, la migración periódica de formatos se ha convertido en una práctica esencial (León-Moreno, Zapico-Alonso y Caldera-Serrano, 2016; Rosenthal, 2010). Organizaciones como la NASA, que en el pasado enfrentó dificultades para acceder a registros almacenados en cintas magnéticas de los años 60, han implementado políticas estrictas de conversión de archivos a formatos modernos. De manera similar, la Bibliothèque nationale de France (BnF) ha establecido protocolos de migración continua para garantizar que su acervo digital pueda ser leído por futuras generaciones de investigadores.

Otra alternativa eficaz es la emulación y virtualización, que permite acceder a archivos generados en sistemas obsoletos al recrear su entorno original en plataformas modernas. Un caso emblemático es el del Proyecto Emulation as a Service (EaaS), desarrollado por la Universidad de Friburgo, que ha permitido recuperar software y documentos antiguos mediante la emulación de sistemas operativos de diferentes épocas. En el ámbito audiovisual, la British Film Institute (BFI) ha utilizado técnicas de virtualización para preservar películas y archivos de video almacenados en formatos históricos (Norman, 2022).

El almacenamiento descentralizado mediante *blockchain* es otra solución emergente que puede contribuir a la preservación de archivos digitales al registrar la trazabilidad y autenticidad de los contenidos sin depender de una única entidad centralizada. Un ejemplo de su aplicación es el Archivo Nacional de Estonia, que ha incorporado *blockchain* en su estrategia de preservación digital para garantizar la inmutabilidad de documentos gubernamentales y audiovisuales (Sedlmeir et al, 2021). De manera similar, el Content Authenticity Initiative (CAI), respaldado por Adobe, The New York Times y X (ex Twitter), busca desarrollar un sistema basado en *blockchain* que permita rastrear modificaciones en imágenes y videos, asegurando la veracidad de los archivos en el tiempo (Lyon, 2021).

Para contrarrestar los efectos de la obsolescencia programada (Malinauskaite y Erdem, 2021), es necesario promover el uso de software libre y hardware de código abierto, lo que permitiría un acceso más prolongado a tecnologías de preservación sin depender de las decisiones comerciales de grandes corporaciones. Iniciativas como el Open Preservation Foundation (OPF) (<https://openpreservation.org/>) han impulsado herramientas de software libre diseñadas específicamente para la conservación digital, como JHOVE (Herramienta de Validación de Formatos) y Archivematica, utilizadas por instituciones como la Biblioteca Nacional de Australia y el Archivo Nacional de Canadá (<https://aabc.ca/Electronic-Records-%26-Digital-Preservation-Management>).

Además de las acciones estrictamente técnicas, la preservación digital requiere la definición de planes y políticas institucionales que orienten de manera coherente todas las decisiones relacionadas con la gestión de objetos digitales. Un plan de preservación digital establece el marco estratégico para garantizar la sostenibilidad de las acciones a largo plazo e incluye, entre otros aspectos, la definición de objetivos y alcance, la asignación de responsabilidades, la identificación de riesgos, la previsión de recursos económicos y humanos, y los criterios de selección y adquisición de los materiales.

Estos marcos estratégicos permiten articular las decisiones técnicas (por ejemplo, qué formatos priorizar, cuándo realizar migraciones o cómo implementar la emulación) con directrices de carácter organizativo y normativo. Asimismo, facilitan la rendición de cuentas, la justificación de inversiones y la creación de mecanismos de auditoría que aumentan la confianza de la comunidad usuaria en la continuidad del acceso. En consecuencia, los planes y políticas de preservación digital constituyen un componente esencial de cualquier estrategia institucional, al asegurar que las técnicas empleadas se sostengan en una planificación clara, transparente y con visión de futuro.

Métodos de autenticación y verificación de contenidos audiovisuales.

Dada la proliferación de técnicas de manipulación digital, la implementación de herramientas y métodos de autenticación y verificación se ha vuelto crucial para garantizar la integridad de los registros audiovisuales (Citron y Chesney, 2019). Si bien existen soluciones tecnológicas avanzadas, es igualmente importante considerar enfoques humanos y metodológicos que permitan evaluar la autenticidad del contenido audiovisual desde una perspectiva multidisciplinaria.

Uno de los métodos más efectivos es el análisis forense digital, que permite detectar modificaciones en imágenes y videos mediante el estudio de patrones de compresión, metadatos y estructuras de archivos. Herramientas como Forensically (<https://29a.ch/photo-forensics/#forensic-magnifier>) y FotoForensics (<https://fotoforensics.com/>) emplean técnicas como el Error Level Analysis (ELA) para identificar zonas en una imagen que han sido manipuladas, analizando la compresión diferencial en diferentes áreas del archivo. Adicionalmente, algoritmos de detección de falsificaciones en video pueden examinar inconsistencias en la iluminación, la sincronización de labios y los cambios abruptos en los patrones de movimiento, facilitando la identificación de *deepfakes* (Boté-Vericad y Vállez, 2022).

Otro método ampliamente utilizado es la búsqueda inversa de imágenes, que permite rastrear el historial y la procedencia de un archivo visual en internet. Plataformas como Google Reverse Image Search (<https://www.reverseimagesearch.org/>), TinEye (<https://tineye.com/>) y Yandex (<https://yandex.com/>) comparan una imagen con bases de datos en línea para detectar duplicaciones, alteraciones o cambios contextuales en su uso. Esta técnica ha sido clave en la verificación de imágenes en el ámbito del periodismo y la investigación académica, permitiendo identificar manipulaciones en contenido viral y esclarecer el contexto original de fotografías y videos difundidos en redes sociales.

El uso de *blockchain* y marcas de agua digitales representa una solución innovadora para la autenticación de archivos audiovisuales. Tecnologías como la Content Authenticity Initiative (CAI) (<https://contentauthenticity.org/>) registran la trazabilidad de un archivo mediante un sistema descentralizado, certificando su procedencia y evitando alteraciones sin dejar rastro. De manera similar, las marcas de agua digitales invisibles, utilizadas en entornos archivísticos y de comunicación, permiten incrustar información en una imagen o video que puede ser verificada posteriormente para confirmar su autenticidad. Empresas como Truepic (<https://www.truepic.com/>) y Serelay han desarrollado sistemas de certificación basados en este principio, aplicados tanto en el periodismo como en la documentación forense.

El *blockchain*, o cadena de bloques, es un sistema de registro descentralizado que almacena datos en bloques enlazados criptográficamente, lo que garantiza la inmutabilidad de la información (Hakak et al, 2020). Esta tecnología permite registrar la trazabilidad de un archivo audiovisual desde su creación, certificando su autenticidad y evitando modificaciones sin dejar rastro. Cada vez que un archivo es creado o modificado, la información se registra en la cadena de bloques de manera transparente y verificable, lo que dificulta la manipulación o falsificación de su contenido (Sedlmeir et al, 2021).

Las marcas de agua digitales (Singh et al, 2025) son señales invisibles incrustadas en archivos de imagen, audio o video que permiten identificar su origen, detectar modificaciones y certificar su autenticidad. A diferencia de las marcas de agua visibles utilizadas tradicionalmente en la protección de derechos de autor, las digitales están diseñadas para ser imperceptibles al ojo humano, pero detectables mediante algoritmos especializados. Estas marcas pueden contener metadatos cifrados sobre el creador del archivo, la fecha y ubicación de su captura, así como cualquier alteración sufrida posteriormente. Existen dos tipos principales de marcas de agua digitales: robustas y frágiles. Las marcas robustas están diseñadas para resistir modificaciones como compresión, recorte o cambios de formato, asegurando la persistencia de la información incrustada. Por otro lado, las marcas frágiles se deterioran o eliminan cuando el archivo es alterado, lo que permite detectar manipulaciones. Empresas como Serelay y Digimarc (<https://www.digimarc.com/>) han desarrollado sistemas de certificación basados en marcas de agua digitales, aplicados en la industria del periodismo y la archivística para garantizar la autenticidad del contenido multimedia.

En el ámbito de la verificación audiovisual, estas marcas han sido implementadas en plataformas como YouTube (<https://www.youtube.com/>) y Getty Images (<https://www.gettyimages.es/>), permitiendo rastrear la distribución de contenido original y detectar copias no autorizadas. Asimismo, el Forensic Watermarking (<https://irdeto.com/>), una técnica utilizada en la industria del cine y la televisión, inserta identificadores únicos en cada copia de un archivo, facilitando la detección de filtraciones y la atribución de responsabilidades en casos de piratería digital.

Los sistemas de inteligencia artificial también han demostrado ser herramientas eficaces para detectar manipulaciones audiovisuales. Algoritmos desarrollados por el MIT Media Lab y Forensic Architecture analizan inconsistencias en los archivos mediante el reconocimiento de patrones atípicos en iluminación, profundidad de campo y movimiento de los píxeles. Estas técnicas han sido utilizadas para detectar *deepfakes* en contenido político y mediático, evitando la propagación de información errónea con fines propagandísticos o de desinformación (Paris y Donovan, 2019).

Sin embargo, la detección de manipulación audiovisual no debe depender exclusivamente de soluciones tecnológicas. Es fundamental incorporar métodos humanos y heurísticos que permitan evaluar la veracidad del contenido a través del análisis contextual y comparativo. En este sentido, el *fact-checking* manual desempeña un papel clave en la identificación de imágenes y videos alterados. Organizaciones como First Draft (<https://firstdraftnews.org/>), Bellingcat (<https://www.bellingcat.com/>) y diferentes observatorios de *fake news* han desarrollado metodologías de verificación que combinan el análisis de metadatos con la comparación de fuentes y la consulta de expertos en el área.

Otra estrategia efectiva es el análisis comparativo de fuentes, que implica examinar el contenido audiovisual en relación con otros registros históricos, documentales o testimoniales. Este enfoque es particularmente útil en el ámbito de la preservación patrimonial y la investigación judicial, donde la autenticidad de un material audiovisual puede verificarse mediante la comparación con registros previamente documentados en archivos institucionales (Maras y Alexandrou, 2019).

Además, el análisis semiótico y lingüístico del contenido audiovisual puede proporcionar información clave sobre su autenticidad. Especialistas en análisis del discurso y comunicación visual pueden identificar patrones en el lenguaje corporal, la estructura narrativa y la coherencia interna del contenido, detectando anomalías que indiquen posibles manipulaciones. Esta metodología ha sido utilizada en investigaciones sobre propaganda y desinformación (Vaccari y Chadwick, 2020), donde el análisis del tono, la entonación y el lenguaje visual ha permitido detectar videos alterados con fines políticos.

Por último, la alfabetización digital (Ajder et al, 2019) y la capacitación de profesionales juegan un papel crucial en la detección de manipulaciones audiovisuales. Iniciativas educativas como los programas de verificación digital de Google News Initiative (<https://newsinitiative.withgoogle.com/>) y Reuters Institute (<https://reutersinstitute.politics.ox.ac.uk/>) buscan formar a periodistas, investigadores y ciudadanos en el uso de herramientas de verificación (Citron y Chesney, 2019) y análisis forense, promoviendo una mayor conciencia sobre la importancia de la autenticación de contenido en la era digital.

Regulación y control normativo de la identidad digital post mortem

El control normativo de la identidad digital *post mortem* varía significativamente entre jurisdicciones, reflejando distintos enfoques sobre la gestión y el acceso a los datos digitales tras el fallecimiento de un individuo. En Estados Unidos, la Revised Uniform

Fiduciary Access to Digital Assets Act (RUFADAA) otorga a albaceas designados acceso a cuentas digitales, siempre que exista un consentimiento explícito. En la Unión Europea, el Reglamento General de Protección de Datos (RGPD) deja en manos de cada país la regulación de los datos digitales tras la muerte. Francia, por ejemplo, permite a los ciudadanos establecer directrices sobre el manejo de su identidad digital *post mortem*, mientras que España contempla este derecho en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

A nivel internacional, organismos como la ONU o la UNESCO han emitido directrices y recomendaciones para la preservación del patrimonio digital; no obstante, la adopción de normas vinculantes y su aplicación efectiva depende de la legislación de cada país, por lo que aún no existe un marco regulatorio global uniforme. La reciente Ley de Inteligencia Artificial de la Unión Europea (AI Act) busca establecer mecanismos para regular la generación y distribución de *deepfakes*, exigiendo transparencia en el uso de contenido sintético.

Para garantizar el uso legítimo de la identidad digital *post mortem*, es fundamental establecer un marco normativo que reconozca explícitamente este derecho como un componente esencial de la dignidad y privacidad de las personas (González Mendoza, 2020). Esto implica la creación de mecanismos de consentimiento en vida, permitiendo a los individuos decidir sobre la conservación, eliminación o cesión de sus archivos digitales tras su fallecimiento (Arnold et al, 2017). Además, es necesario regular el acceso a estos datos por parte de familiares, herederos y albaceas, asegurando un equilibrio entre la protección de la privacidad del fallecido y los derechos de sus allegados (Otero Creso, 2024). Un aspecto clave en esta regulación es la prevención del uso indebido de tecnologías como los *deepfakes* (Kietzmann et al, 2020), que pueden facilitar la manipulación de imágenes y voces con fines desinformativos o comerciales sin autorización. Para mitigar estos riesgos, se debe fomentar la implementación de sistemas de certificación de autenticidad basados en *blockchain* (Sedlmeir et al, 2021) y tecnologías forenses, garantizando la trazabilidad e integridad de los archivos digitales a lo largo del tiempo. La combinación de estas medidas contribuiría a la construcción de un marco ético y jurídico que proteja la memoria digital y prevenga su explotación indebida en la era de la inteligencia artificial (González Mendoza, 2020).

Cuestiones éticas de la manipulación de la identidad digital post mortem.

Uno de los principales peligros de la manipulación audiovisual *post mortem* es la desinformación y propaganda, ya que el uso de *deepfakes* permite modificar o crear imágenes y videos que distorsionan la realidad (Kietzmann et al, 2020). Esta tecnología puede ser utilizada para alterar hechos históricos, falsear declaraciones de figuras públicas fallecidas o influir en la opinión pública con narrativas fabricadas (Arnold et al, 2017). Al manipular la memoria audiovisual, se corre el riesgo de legitimar discursos falsos, lo que puede tener consecuencias políticas, sociales y culturales de gran impacto (Paris y Donovan, 2019). Ejemplos recientes han demostrado cómo los *deepfakes* han sido empleados para crear videos apócrifos de líderes políticos (Paris y Donovan, 2019), generando confusión y afectando la confianza en los archivos audiovisuales auténticos.

Otro riesgo significativo es la explotación comercial sin autorización, donde la imagen y voz de personas fallecidas pueden ser utilizadas con fines lucrativos sin respetar su voluntad o la de sus familiares. La recreación digital de artistas, escritores o figuras públicas en anuncios publicitarios o producciones cinematográficas ha generado un debate sobre los límites éticos y legales de estas prácticas (Robles-Carrillo, 2024). Casos como la resurrección digital de actores en películas o el uso de la voz sintética de celebridades fallecidas para promocionar productos plantean interrogantes sobre

la necesidad de consentimiento explícito y mecanismos de compensación para los herederos. Sin regulaciones adecuadas, la explotación comercial de identidades digitales *post mortem* podría convertirse en una práctica generalizada, despojando a los individuos del derecho a decidir sobre su imagen tras la muerte.

Asimismo, la manipulación audiovisual *post mortem* facilita el fraude y la suplantación de identidad, dado que el contenido sintético generado con inteligencia artificial puede ser empleado en estafas, engaños emocionales y fraudes financieros. La clonación de voces y la generación de videos falsos pueden utilizarse para engañar a familiares, amigos o instituciones, haciéndoles creer que están interactuando con una persona fallecida. En algunos casos, esta tecnología ha sido aprovechada para falsificar mensajes de despedida, solicitar transferencias de dinero o manipular voluntades póstumas. La ausencia de mecanismos de verificación confiables puede hacer que estos delitos sean difíciles de detectar, aumentando el riesgo de vulneraciones a la privacidad y la seguridad patrimonial de los afectados.

Para mitigar estos riesgos, es fundamental fomentar una cultura de transparencia y alfabetización digital (León Gavilanez, 2023), capacitando a la sociedad para identificar contenidos manipulados y cuestionar la autenticidad de la información audiovisual (Cerdán Martínez, García Guardia y Padilla Castillo, 2020). Esto debe ir acompañado del desarrollo de marcos normativos sólidos, que regulen el uso de la identidad digital *post mortem* y establezcan sanciones para quienes la utilicen de manera indebida (Cerdán Martínez, García Guardia y Padilla Castillo, 2020).

La protección de la identidad digital (Reda, 2024) *post mortem* requiere una colaboración interdisciplinaria entre desarrolladores tecnológicos, archiveros, legisladores y expertos en ética, quienes deben trabajar en conjunto para garantizar el uso legítimo y respetuoso de estos registros. La memoria individual y colectiva en la era digital depende de la implementación de mecanismos efectivos para evitar su manipulación, asegurando que los archivos audiovisuales mantengan su autenticidad y su valor como testimonio histórico y cultural.

Conclusiones

La preservación de la identidad audiovisual digital *post mortem* representa un reto interdisciplinario que exige un equilibrio entre avances tecnológicos, regulación legal y consideraciones éticas. En un contexto donde la imagen y el sonido se han convertido en elementos esenciales de la memoria colectiva e individual, es fundamental desarrollar estrategias de conservación que garanticen la autenticidad y accesibilidad de estos materiales en el tiempo. La gestión de metadatos, el archivado digital y las políticas institucionales han demostrado ser herramientas clave en este proceso, aunque deben actualizarse constantemente para hacer frente a la obsolescencia tecnológica y la manipulación digital (UNESCO, 2003; Rosenthal, 2010).

El uso creciente de inteligencia artificial ha incrementado el riesgo de alteración de identidades audiovisuales, permitiendo la generación de *deepfakes* y otras técnicas de síntesis digital con fines desinformativos o propagandísticos. Para mitigar estos riesgos, es esencial fortalecer los mecanismos de verificación mediante *blockchain*, marcas de agua digitales y algoritmos de detección de alteraciones (Sedlmeir et al, 2021). No obstante, estas soluciones deben complementarse con marcos regulatorios que delimiten el uso de la inteligencia artificial en la reconstrucción de identidades digitales *post mortem*, garantizando un equilibrio entre innovación tecnológica y protección de la memoria histórica.

Futuras investigaciones deberían centrarse en el desarrollo de metodologías más precisas para la autenticación de archivos audiovisuales, explorando tecnologías emergentes como la inteligencia artificial explicable y la verificación descentralizada de datos. Asimismo, es necesario profundizar en el impacto social de la manipulación audiovisual y en el diseño de normativas internacionales que regulen el uso póstumo de imágenes y voces en entornos digitales. La colaboración entre expertos en archivística, derecho digital y tecnologías de la información será clave para garantizar que la identidad audiovisual *post mortem* se preserve con integridad y se proteja de la manipulación en la era digital.

Agradecimientos

Esta investigación ha contado con el apoyo de la Junta de Extremadura y los Fondos FEDER “Una manera de hacer Europa” [Grupo de investigación QUINARI SEJ013 GR18130]

Referencias bibliográficas

- » Ajder, Henry, Giorgio Patrini, Francesco Cavalli y Laurence Cullen. 2019. *The state of deepfakes: landscape, threats, and impact*. Amsterdam: Deeptrace. <https://regmedia.co.uk/2019/10/08/deepfake_report.pdf> [Consulta: 30 septiembre 2025]
- » Arnold, Michael, Martin Gibbs, Tamara Kohn, James Meese y Bjorn Nansen. 2017. *Death and Digital Media*. Londres: Routledge. <<https://doi.org/10.4324/9781315688749>>
- » Boté-Vericad, Juan J. y Mari Vállez. 2022. Aplicaciones de deepfakes. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad. En *Documentación de las Ciencias de la Información*. Vol. 45, no. 1, 25-32. <<https://doi.org/10.5209/dcin.77256>>
- » Caldera Serrano, Jorge y Pilar Arranz Escacha. 2012. *Documentación audiovisual en televisión*. Barcelona: Editorial UOC.
- » Cerdán Martínez, Víctor, María Luisa García Guardia y Graciela Padilla Castillo. 2020. Alfabetización moral digital para la detección de deepfakes y fakes audiovisuales. En *CIC. Cuadernos de Información y Comunicación*. Vol. 25, 165-181. <<https://doi.org/10.5209/ciyc.68762>>
- » Citron, Danielle K. y Robert Chesney. 2019. *Deepfakes and the New Disinformation War*. En *Foreign Affairs*. No. Enero/Febrero. <https://scholarship.law.bu.edu/shorter_works/76> [Consulta: 30 septiembre 2025]
- » González Mendoza, Diana P. 2020. Los perfiles digitales después de la muerte, una perspectiva europea. En *Estudios En Derecho a La Información*. Vol. 1, no. 11, 3-26. <<https://doi.org/10.22201/ij.25940082e.2021.11.15298>>
- » Hakak, Saqib, Wazir Zada Khan, Gulshan Amin Gilkar, Basem Assiri, Mamoun Alazab, Sweta Bhattacharya y G Thippa Reddy. 2020. Recent advances in Blockchain Technology: A survey on Applications and Challenges. En *arXiv preprint arXiv:2009.05718*. <<https://arxiv.org/abs/2009.05718>> [Consulta: 30 septiembre 2025]
- » Kietzmann, Jan, Linda W. Lee, Ian P. McCarthy y Tim C. Kietzmann. 2020. Deepfakes: trick o treat? En *Business Horizons*. Vol. 63, 135-146. <<https://doi.org/10.1016/j.bushor.2019.11.006>>
- » León Gavilanez, Kevin F. 2023. Preservación digital. Estudio de alfabetización. Salamanca: Universidad de Salamanca. Programa de doctorado Formación en la Sociedad del Conocimiento. <<https://gredos.usal.es/bitstream/handle/10366/153058/Kevin%20Leo%CC%81n-Gavilanez-rep.pdf?sequence=1>> [Consulta: 30 septiembre 2025]
- » León-Moreno José A., Felipe Zapico-Alonso y Jorge Caldera-Serrano. 2016. ¿Archivos audiovisuales aún sin digitalizar? seguridad, preservación y amortización. En *Cuadernos de Documentación Multimedia*. Vol. 27, no. 2, 178-190. <<https://doi.org/10.5209/CDMU.54488>>
- » Lyon, Santiago. 2021. The case for content authenticity in an age of disinformation, deepfakes and NFTs. En *Adobe Blog*. <<https://blog.adobe.com/en/publish/2021/10/22/content-authenticity-in-age-of-disinformation-deepfakes-nfts>> [Consulta: 30 septiembre 2025]

- » Malinauskaite, Jurgita y Fatih B. Erdem. 2021. Planned obsolescence in the contexto f a holistic legal sphere and the circulas econonomy. En *Oxford Journal of Legal Studios*. Vol. 41, no. 3, 719- 749. <<https://doi.org/10.1093/ojls/gqaa061>>
- » Maras, Marie-H. y Alex Alexandrou. 2019. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. En *The International Journal of Evidence y Proof*. Vol. 23, no. 3, 255-262. <<https://doi.org/10.1177/1365712718807226>>
- » Martin, Carolyn W. y Isabel Jonson. 2024. Legal and ethical issues in phosthumous art and artificial intelligence. En *Lutzker y Lutzker*. <<https://www.lutzker.com/legal-and-ethical-issues-in-posthumous-art-and-artificial-intelligence/>> [Consulta: 30 septiembre 2025]
- » Norman, Michael. 2022. Open reel to open source: digital preservation of the UK´s videotape heritage. *Knowledge and Collections. BFI*. <<https://blog.bfi.org.uk/knowledge-and-collections/open-reel-to-open-source-digital-preservation-of-the-uks-videotape-heritage/>> [Consulta: 30 septiembre 2025]
- » Ochoa-Gutiérrez, Jaider, Andrés R. Sáenz Giraldo y Tatiana Tirado Tamayo. 2021. Experiencias de gestión de los procesos de preservación digital a partir del modelo OAIS en repositorios institucionales. En *Anales de Documentación*. Vol. 24, no. 1. <<https://doi.org/10.6018/analesdoc.428141>>
- » Otero Crespo, Marta. 2024. *Post-Mortem Data Protection and Succession in Digital Assets Under Spanish Law*. En Carneiro Pacheco de Andrade, Francisco A., Pedro M. Fernandes Freitas y Joana R. de Sousa Covelo de Abreu, eds. *Legal Developments on Cybersecurity and Related Fields*. Cham: Springer. Law, Governance and Technology Series. Vol 60. <https://doi.org/10.1007/978-3-031-41820-4_10>
- » Panorama Audiovisual. 2025. *BBC encarga a Memnon la digitalización de su amplio legado de archivos de audio*. <<https://www.panoramaaudiovisual.com/2023/09/08/bbc-encarga-memnon-digitalizacion-legado-archivos-audio/>> [Consulta: 30 septiembre 2025]
- » Paris, Britt y Joan Donovan. 2019. Deepfakes and cheap fakes: the manipulation of audio and visual evidence. En *Data y Society*. No. septiembre. <<https://datasociety.net/library/deepfakes-and-cheap-fakes/>> [Consulta: 30 septiembre 2025]
- » Póveda López, Inés C., Jorge Caldera Serrano y Juan A. Polo Carrión. 2010. Definición del objeto de trabajo y conceptualización de los Sistemas de Información Audiovisual de la Televisión. En *Investigación Bibliotecológica: Archivonomía, bibliotecología E información*. Vol. 24, no. 50. <<https://doi.org/10.22201/iibi.0187358xp.2010.50.21409>>
- » Reda, El Y. 2024. Exploring the Components of Digital Identity on Social Networks Sites: Identifier, Post, Profile Photo, and Selfie. En *European Scientific Journal, ESJ*. Vol. 20, no. 1, 1. <<https://doi.org/10.19044/esj.2024.v20n1p1>>
- » Robles-Carrillo, Margarita. 2024. Digital identity: an approach to its nature, concept, and functionalities. En *International Journal of Law and Information Technology*. Vol. 32, no. 1, eaaeo19. <<https://doi.org/10.1093/ijlit/eaee019>>
- » Rosenthal, David S. H. 2010. Format obsolescence: assesing the threat and the defenses. En *Library Hi Tech*. Vol. 28, no. 2, 195-210. <<https://doi.org/10.1108/07378831011047613>>
- » Schonfeld, Roger. C. 2018. Why is the digital preservation network disbanding? En *The Scholarly kitchen*. <<https://scholarlykitchen.sspnet.org/2018/12/13/digital-preservation-network-disband/>> [Consulta: 30 septiembre 2025]

- » Singh, Vishal, Ayush Aggarwal, Vidit Biswas y Amrit K. Agarwal. 2025. Advances in digital watermarking using Deep Learning: a comprehensive review. En *International Research Journal of Engineering and Technology*. Vol. 12, no. 1, 602-611. <<https://www.irjet.net/archives/V12/I1/IRJET-V12I191.pdf>> [Consulta: 30 septiembre 2025]
- » Stokes, Patrick. 2012. Ghosts in the Machine: Do the Dead Live on in Facebook? En *Philosophy & Technology*. Vol. 25, 363-379. <<https://doi.org/10.1007/s13347-011-0050-7>>
- » Sedlmeir, Johannes, Reilly Smethurst, Alexander Rieger y Gilbert Fridgen. 2021. Digital identities and verifiable credentials. En *Business y Information Systems Engineering*. Vol. 63, no. 6, 603-613. <<https://doi.org/10.1007/s12599-021-00722-y>>
- » UNESCO. 2003. *Directrices para la preservación del patrimonio digital*. <https://unesdoc.unesco.org/ark:/48223/pf0000130071_spa> [Consulta: 30 septiembre 2025]
- » Vaccari, Cristian y Andrew Chadwick. 2020. Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty and trust in news. En *Social Media + Society*. Vol. 6, no. 1. <<https://doi.org/10.1177/2056305120903408>>
- » Vanhaecht, Jan, David Mapgaonkar y Andre Romanovski. 2020. The future of digital identity. En *Deloitte*. <<https://www.deloitte.com/global/en/services/consulting-risk/perspectives/the-future-of-digital-identity.html>> [Consulta: 30 septiembre 2025]