

Panorama Internacional del Voto con Autenticación Biométrica: Avances, Debates y Desafíos para la Democracia

International Overview of Biometric Voting: Progress, Debates, and Challenges for Democracy

ARTÍCULO DE REVISIÓN

Gustavo Adrián Berón

Universidad Nacional de Quilmes, Argentina. Contacto: gustavoberon69@hotmail.com

Recibido: mayo de 2026

Aceptado: mayo de 2026

Resumen

Este artículo de revisión se enfoca en el desarrollo del estado del arte actual de la utilización de sistemas biométricos de autenticación aplicados a los sistemas democráticos de procesos electorales en el mundo, con especial observación en Latinoamérica y Argentina. En función de consolidar y fortalecer nuestra democracia, se hace necesario buscar e identificar las principales tendencias, desafíos y oportunidades que los nuevos desarrollos tecnológicos pueden ofrecer, analizando las recientes literaturas e informes provenientes de distintos organismos internacionales especializados. En este sentido, la biometría - particularmente la huella digital y el reconocimiento facial- se ha consolidado en algunos estados como un instrumento responsable de garantizar la seguridad del sufragio al asegurar la identidad de los ciudadanos votantes, en función de prevenir el fraude que históricamente ha tenido gran presencia en varios procesos electorales. Sin embargo, su adopción no resulta neutral, por lo que surge la necesidad de abrir debates vitales sobre el nivel de privacidad, la soberanía tecnológica e incluso la inoperabilidad de bases de datos, que generan riesgos de virar hacia sistemas o modelos de control social autoritario. El presente trabajo concluye que, incluso tomando en cuenta los desarrollos tecnológicos más avanzados, cimentados sobre verdaderas bases de madurez técnica, materializada en diversos prototipos (Faruk et al., 2024; Adeniyi et al., 2024), el éxito de la implementación de estos sistemas dependerá fundamentalmente de factores de confianza pública, así como de otros de tipo legal e institucional que promuevan el debate informado e importantes marcos regulatorios que anticipen cualquier implementación a gran escala.

Palabras Clave: Biometría electoral; Blockchain; Democracia digital; Soberanía tecnológica.

Abstract

This review article examines the current state-of-the-art in biometric authentication systems applied to democratic electoral processes worldwide, with a specific focus on Latin America and Argentina. To consolidate and strengthen democratic institutions, it is essential to identify the key trends, challenges, and opportunities offered by emerging technological developments, based on an analysis of recent literature and reports from specialized international organizations. In this regard, biometrics—particularly fingerprint and facial recognition—has emerged in several states as a tool to guarantee suffrage security by verifying voter identity and preventing historical patterns of electoral fraud. However, its adoption is not neutral; it triggers vital debates regarding privacy levels, technological sovereignty, and database interoperability, which pose risks of shifting toward authoritarian social control models. This paper concludes that even the most advanced technological developments, built on technical maturity and proven prototypes, depend fundamentally on public trust, as well as legal and institutional frameworks that promote informed debate and robust regulations prior to large-scale implementation.

Keywords: Electoral biometrics; Blockchain; Digital Democracy; Technological sovereignty.

Introducción

Con el desarrollo tecnológico y la presencia de la Inteligencia Artificial (IA) se puede visualizar una práctica electoral que combine estos desarrollos dejando atrás cierta idea de ilusión futurista para convertirse en una realidad cotidiana y al servicio de una construcción democrática moderna. La incorporación de herramientas digitales cuyo fin se enfoca en garantizar eficiencia y seguridad para toda la ciudadanía tuvo un lugar preponderante en las últimas décadas al buscar mayor transparencia en la consolidación de las democracias representativas. La autenticación biométrica de ciudadanos votantes, presente como una innovación destacada, se proyecta como una de las más significativas, aunque también controversial de cierto modo. Desde el uso de huellas digitales en Brasil llegando a los sistemas multimodales que combinan reconocimiento facial y dactilar en procesos experimentales como los que señala Faruk et al. (2024), la biometría se analiza como una posible solución a los eternos problemas que presentaban los procesos electorales asociados a la suplantación de identidad o la emisión del voto múltiple.

Por otra parte, Barrat y Esteve (2025) señalan, en su informe para la Internacional IDEA, que el uso de cierta tecnología aplicada al sistema electoral debe contemplarse no solo desde una cuestión de ingeniería, sino que es vital remitir el asunto a debates más profundos vinculados a la autenticación de la identidad del votante en entornos digitales, ya

que se hace necesaria la intervención de voces especializadas en la naturaleza de la influencia de la inteligencia artificial y el impacto social del uso de software electorales en procesos democráticos. En este sentido, podemos visualizar que la sociedad se encuentra en un nuevo escenario que plantea un sistema electoral con "democracia digital", donde los ciudadanos o electores deben coexistir con otros participantes influenciados por esta nueva realidad de formación de opinión pública, asociados a menores de edad que se integran a las redes sociales, personas jurídicas y diverso tipo de comunidades virtuales que trascienden las instituciones clásicas, como señala Galindo Vácha (2025). Es por ello que implementar sistemas biométricos en procesos electorales no se presenta como una simple actualización administrativa, sino más como una decisión política con serias implicancias dentro de un nuevo ecosistema social digital.

El legado del argentino Juan Vucetich, cuyo descubrimiento de identificación dactilar revolucionó los sistemas de reconocimiento civil y criminal a principios del siglo XX (Neira Orijuela, 2024), hace de América Latina una región que cimentó bases para la identificación biométrica, aunque recientemente se fueron sumando tecnologías de vigilancia aportadas por actores de otros países que generaron cierta opacidad y a la vez desigualdad en su desarrollo con respecto a la disponibilidad local. El informe de AISur (Ibarreche, Martínez Elebi & Di Lorenzo, 2025) documenta cómo empresas como IDEMIA (Francia), NEC (Japón), Dahua e Hikvision (China) compiten por posicionarse en el mercado latinoamericano en cuestiones de desarrollo de control migratorio y seguridad urbana, en un contexto donde la posible falta de transparencia en las contrataciones, las sospechas de corrupción y la debilidad de los marcos regulatorios logran generar alertas sobre el posible uso indebido de datos sensibles.

En tal sentido, este artículo de revisión se enfoca en desarrollar un panorama internacional del voto con sistemas biométricos de autenticación que involucra la evolución técnica de los sistemas (blockchain, machine learning, criptografía), los debates políticos y jurídicos que abordan cuestiones de privacidad, soberanía y confianza, y toda experiencia que pueda aportar al caso argentino. El análisis de fuentes literarias actualizadas es una condición relevante y necesaria, por lo cual se deben realizar revisiones sistemáticas de un corpus de fuentes como ser (Revelo Sánchez et al., 2026; Ohize et al., 2024), estudios de caso con implementación empírica (Faruk et al., 2024; Omoze, Omaji & Edegbe, 2025; Shaikh et al., 2025; Adeniyi et al., 2024), informes de organismos intergubernamentales (Barrat i Esteve, 2025; Juneja, 2024), investigaciones regionales (Neira Orijuela, 2024; Ibarreche et al., 2025; Papagni, 2024; Martínez, 2024) y desarrollos locales concretos (Lessio & Riveros Salomón, 2025), entre otros. Cabe destacar que guiar esta revisión implica realizar la siguiente pregunta: ¿en qué medida la implementación de sistemas de autenticación biométrica para el voto puede fortalecer la democracia sin perjudicar o socavar

derechos fundamentales, y qué condiciones institucionales y regulatorias son necesarias para ello?

Precisiones conceptuales

Para continuar adentrándonos en un panorama internacional, es fundamental analizar y determinar algunas precisiones que permitan abordar aspectos complejos del objeto de estudio. Neira Orjuela (2024) señala que la autenticación biométrica puede definirse como la medición estandarizada de características físicas de los individuos -huellas dactilares, voz, iris, características faciales, entre otras posibles- cuyo objetivo se enfoca en identificar la identidad del votante. Es importante aclarar que la unicidad y la irrepitibilidad de ciertas características físicas ofrecen un insumo invaluable que permite conformar métodos de identificación más sólidos que los tradicionales, basados en información que se retiene - como ser contraseñas- o algo físico externo -como un documento de identidad-. La biometría aplicada a la práctica electoral se ha utilizado en dos momentos clave: el registro de votantes para eliminar la duplicidad del sufragio, y la autenticación al momento de emitir el voto de forma remota o presencial.

En este sentido, es importante tener en cuenta los aportes de Juneja (2024), quien advierte que algunos sistemas biométricos no son del todo neutrales desde el punto de vista técnico, documentando en su análisis para Internacional IDEA que, al momento de ser utilizados, han mostrado sesgos significativos en detrimento de personas afrodescendientes al usar técnicas de reconocimiento facial. Esta situación genera interrogantes sobre su compatibilidad con los criterios de no discriminación y justicia electoral. A su vez, el avance en la complejización de estos sistemas -que incorporan algoritmos de machine learning como el Random Forest utilizado por Omoze, Omaji y Edegbe (2025), que logran una exactitud del 98% en autenticación multimodal- no logra resolver los problemas planteados de opacidad y auditabilidad. Cualquier solución, por compleja y eficaz que se presente, no deja de convertirse en un sistema de “caja negra” inescrutable para la ciudadanía y los partidos políticos, con la imposibilidad de fiscalizar el proceso por completo.

Considerando los avances en materia de espacios web, podemos abordar el concepto de “democracia digital” propuesto por Galindo Vácha (2025) como un eje disparador del debate. Para el autor, la tecnología es un factor transformador que reconfigura y cambia el espacio público, lejos de ser un mero instrumento al servicio de actividades políticas inmutables y sin evolución social. La realidad ciudadana se destaca por una gran presencia de actividades virtuales que han desarrollado nuevos actores asociados a menores conectados, personas jurídicas y comunidades virtuales; y nuevos espacios de deliberación e intercambio como foros, plataformas o aplicaciones de mensajería que conviven con todo lo históricamente tradicional e institucional. Ante dicha realidad, podemos reflexionar sobre

una introducción de autenticación biométrica en el sistema electoral no solo como una solución técnica, sino también como aquello que guarda cierta capacidad de redefinir el vínculo entre la ciudadanía y el Estado, considerando instancias de participación remota que en tiempos pasados estaban lejos de ser pensadas. Por otra parte, y acompañando todos los aspectos de este proceso, también se pueden generar nuevas vulnerabilidades que son la contracara del sistema.

Dándole forma y método a estos avances, las "arquitecturas tecnológicas" se proyectan como un concepto o pilares capaces de sostener y adaptar la autenticación biométrica en nuestro sistema electoral. Al respecto, Ohize et al. (2024), especializado en el análisis de blockchain para sistemas de voto electrónico, pone a disposición una diferenciación de tipos de arquitecturas designadas "centralizadas y descentralizadas". La primera se enfoca en un sistema en el cual los datos de los ciudadanos votantes y su voto se alojan en servidores controlados por una única entidad, cuyo riesgo radica en su poder para manipular la información e influir en los resultados. En la segunda, la tecnología blockchain permite distribuir la información en una red de nodos que garantizan seguridad, inmutabilidad y transparencia. Dentro de estas últimas, se identifican blockchains públicas (como Ethereum, utilizada en el prototipo ruso de Moscú o en el desarrollo de Lessio & Riveros Salomón para Argentina), de orden privado (como Hyperledger Fabric, empleada por Faruk et al., 2024) y de consorcio (administradas por un grupo predefinido de organizaciones). Cada una de estas opciones tiene implicancias diferentes en lo que respecta a la soberanía, en cuestiones de costos, de velocidad de procesamiento y de capacidad de auditoría.

Panorama internacional: experiencias y tendencias

1. Europa: entre la vanguardia y la cautela constitucional

En Europa, países como Estonia se han destacado mundialmente entre aquellos con grandes avances en gobierno electrónico al implementar, desde el año 2005, un sistema de voto por internet (i-voting) que utiliza la tarjeta de identidad digital con criptografía de clave pública para autenticar a cada votante (Barrat i Esteve, 2025). Este sistema ha logrado que más de un 50% de los votos en elecciones nacionales se emitan de forma remota con gran aceptación ciudadana, sin la utilización de biometría, pero potenciando un factor de autenticación sólido y confiable. Cabe destacar que este avance guarda un alto contenido de confianza ciudadana en lo público que no existe en la mayoría de los países, lo que hace que difícilmente pueda replicarse en otros estados democráticos, como advierte el informe de Internacional IDEA.

Desde Alemania se observan experiencias sociales y políticas de máxima cautela en el uso de sistemas tecnológicos e informáticos, urnas digitales u otros. El Tribunal Constitucional Federal declaró inconstitucional en el año 2009 el uso de urnas electrónicas o sistemas similares (sin conexión a internet) por la falta de transparencia y control que estos dispositivos presentaban. Básicamente, los ciudadanos no podían entender ni fiscalizar el proceso de conteo, cuyo funcionamiento se presentaba como un sistema de "caja negra" o sistema tecnológico ciego. Barrat i Esteve (2025) recupera y expone en su trabajo esta sentencia, estableciendo un principio básico y fundamental: las elecciones deben ser en su naturaleza pública, exigentes en los controles, haciendo especial énfasis en lo observable, lo comprensible y lo auditable del proceso por cualquier ciudadano. Cabe aclarar que los sistemas de voto digital difícilmente puedan satisfacer por completo estas demandas mencionadas, en especial aquellos que incorporan cierta tecnología avanzada o inteligencia artificial.

Suiza se ha inclinado por una opción intermedia tras varios años de experimentar con el voto por internet para ciudadanos residentes en el exterior. Este camino alternativo merece atención y análisis, ya que se logró desarrollar un modelo de auditoría basado en la apertura y colaboración directa de los sectores académicos. Como documenta Barrat i Esteve (2025), el sistema suizo actual exige la publicación del código fuente, la realización de "public intrusion tests" donde expertos independientes intentan vulnerar el sistema, y la consulta abierta a la comunidad científica y técnica. Este enfoque se ha considerado una de las mejores prácticas para cualquier nación que aspire a implementar tecnología electoral en permanente avance, por ofrecer prioridad a la transparencia radical por sobre cualquier certificación formal además de un control permanente.

2. África: laboratorio de innovación en contextos de debilidad institucional.

África se ha destacado por convertirse en un continente clave en materia de experimentación de sistemas y tecnología electoral para sorpresa de muchos. Los trabajos de Revelo Sánchez et al. (2026) dejan en evidencia una producción académica importante en países como Nigeria, Kenia, Sudáfrica y Marruecos, aunque advierten que la mayoría de los desarrollos se limitan a entornos académicos controlados o a sistemas piloto de pequeña escala en modo laboratorio. Nigeria, enfocándose en la utilización de blockchain, ha trabajado en diversos análisis de factibilidad para su sistema electoral; Sierra Leona experimentó con almacenamiento de votos en una plataforma distribuida; Sudáfrica ha explorado arquitecturas con Hyperledger Fabric y protocolos de cero conocimientos; y Marruecos ha utilizado la blockchain Solana en algunos de sus desarrollos, según exponen Ohize et al. (2024) sobre varias experiencias concretas.

Pero como en otros países, las experiencias africanas también dejan advertencias importantes. Autores como Cheeseman, Lynch y Willis (2018) analizan cómo pueden generarse nuevas formas de exclusión, llevando la conflictividad post electoral del terreno político al técnico por la introducción de tecnología electoral que puede no resultar masiva o de fácil uso y acceso. La posibilidad de que un sistema biométrico falle y deje a miles de votantes sin la oportunidad de participar del sufragio desataría un mar de dudas sobre la legitimidad del proceso, potenciando las acusaciones de fraude y corrupción por una posible manipulación técnica del resultado electoral. Es por eso que América Latina debe tener en cuenta que la tecnología por sí sola no resuelve todo aquello que implica la confianza en los sistemas, por lo que cada avance en esta área debe estar respaldado por instituciones sólidas y procesos transparentes que ofrezcan auténticas garantías a la población.

3. América Latina: tradición biométrica, desafíos estructurales y nuevos actores.

América Latina presenta una realidad muy especial en la cual, por un lado, las experiencias de identificación biométrica se remontan a principios del siglo XX, cuando el argentino Juan Vucetich desarrolla el sistema dactiloscópico que fue adoptado luego por varios países sudamericanos, según documenta exhaustivamente Neira Orjuela (2024). Cabe aclarar que dicha herencia ha facilitado de alguna forma la aceptación cultural de la biometría como medio de identificación estatal en la región. A su vez, el abordaje de sistemas biométricos aplicados a los sistemas electorales democráticos es de reciente utilización, destacándose un fuerte condicionamiento por dinámicas geopolíticas y comerciales que exceden el control de los estados nación.

En este sentido, Brasil se destaca por convertirse en el caso más relevante de la región. Neira Orjuela (2024) describe un programa ambicioso de identificación biométrica electoral que alcanzó a más de 50 millones de votantes, impulsado por el Tribunal Superior Electoral (TSE) en 2008. La innovación del argentino Juan Vucetich fue vital, ya que el sistema vinculó el uso de la huella digital con una urna electrónica que solo se habilitaba cuando un lector biométrico podía verificar la identidad del sufragante. Sin embargo, existe un riesgo relacionado a la conformación y uso de la información resultante desde la interconexión de bases de datos como en Brasil y la Ley 13.444/17 que unificó el Registro Civil con datos electorales y de la Policía Federal para la emisión de pasaportes, lo cual genera preocupaciones sobre el uso secundario de datos biométricos originalmente recolectados con fines enfocados a la optimización del sufragio.

Esta tendencia a la unificación de bases de datos no se hizo esperar en Argentina, por lo que el sistema SIBIOS (Sistema Federal de Identificación Biométrica para la Seguridad) articula información del Registro Nacional de las Personas (RENAPER), la Dirección Nacional de Migraciones y diversas fuerzas policiales, que a su vez se suman a conformar

intercambios de información con agencias como INTERPOL (Neira Orjuela, 2024). Un ejemplo argentino de caso paradigmático y de opacidad que ha sido judicializado lo genera la Ciudad de Buenos Aires, cuyo sistema de reconocimiento facial fue suspendido por la justicia por la recolección de datos de personas que no habían cometido delito alguno, constituyendo una violación al principio de finalidad que debe regir el tratamiento de datos personales (Ibarreche, Martínez Elebi & Di Lorenzo, 2025).

En lo que respecta al rol de los proveedores extranjeros, el informe de AISur (2025) aporta información sobre aspectos de los escenarios geopolíticos y su influencia en la región. No puede descartarse ni dejar de lado la importancia de la información que los sistemas masivos de control biométrico pueden otorgar a organizaciones de otros países. Empresas como IDEMIA (controlada por un fondo de inversión de EEUU), NEC (Japón), Dahua e Hikvision (China) compiten por vender sus servicios de vigilancia urbana, control migratorio y sistemas de identificación en toda la región, accediendo a la vez a información vital. La presencia de EUROFRONT, un programa financiado por la Unión Europea, en las fronteras de Bolivia, Perú, Colombia, Ecuador y la Triple Frontera, son la evidencia de cómo la tecnología biométrica gana terreno y se inserta en agendas de seguridad que trascienden lo electoral, alejándose de alternativas locales. Habiendo realizado alguna observación sobre la importancia de la información, nos queda preguntarnos: ¿qué garantías existen de que los datos biométricos recolectados para votar no terminen siendo el insumo de otras bases de datos relacionadas a la vigilancia, al control migratorio u otro tipo de control social?

4. Desarrollos tecnológicos con evaluación empírica

Diversos aportes recientes, como el de Faruk et al. (2024), examinan la implementación de sistemas de votación por internet (*i-voting*) que integran Hyperledger Fabric -una arquitectura de *blockchain* permissionada- con mecanismos de autenticación dactilar y reconocimiento facial. Los resultados de estas pruebas fueron alentadores, demostrando que la convergencia entre biometría y registros distribuidos constituye una base sólida para futuros estudios académicos orientados a su aplicación en organismos que demanden altos estándares de seguridad.

Las evaluaciones de este sistema, realizadas sobre una muestra de 100 votantes, arrojaron una efectividad notable: el 97% logró registrarse exitosamente en el primer intento y el 88% completó la autenticación y el sufragio. En cuanto a la eficiencia técnica, los tiempos de procesamiento promediaron los 1,8 segundos para la huella dactilar y 3,1 segundos para el reconocimiento facial. No obstante, los autores identificaron desafíos críticos: un 13% de los usuarios no logró autenticarse incluso tras un segundo intento, lo que representa una barrera significativa para proyectar su implementación a escala nacional en términos de universalidad del voto.

Paralelamente, Adeniyi et al. (2024) desarrollaron un protocolo sobre una muestra de 400 votantes, utilizando el conjunto de datos público SOCOFing. Mediante algoritmos de procesamiento de imágenes -como la binarización de Otsu y la esqueletización de Zhang-Suen- y la extracción de características vía Cross Number, el sistema genera claves criptográficas de 256 bits a partir de las huellas dactilares para operar en una billetera Ethereum mediante contratos inteligentes. La principal ventaja de esta propuesta radica en que la clave pública presente en la *blockchain* no guarda conexión directa con la identidad civil del votante, preservando el anonimato, mientras que la clave privada solo puede ser generada por el ciudadano al momento de emitir su voto.

Por otro lado, Omoze, Omaji y Edegbe (2025) emplearon técnicas de *machine learning* (Random Forest) para la autenticación multimodal. Aunque su modelo alcanzó una precisión del 98%, los datos se almacenaron en una base MySQL centralizada. Si bien esto confirma la alta efectividad de los algoritmos de clasificación, la ausencia de *blockchain* mantiene los problemas de centralización y vulnerabilidad ante manipulaciones externas que las soluciones descentralizadas intentan mitigar.

En una línea similar, Shaikh et al. (2025) analizaron el sistema de Omán comparando transacciones sincrónicas (individuales) con asincrónicas (por lotes), integrando biometría con contratos inteligentes de **Ethereum**. Sus hallazgos confirman que el procesamiento por lotes optimiza los tiempos operativos, aunque advierten que su éxito depende de un marco regulatorio sólido y de estudios que cuantifiquen la confianza ciudadana en la tecnología.

Finalmente, desde el contexto argentino, se destaca el proyecto "VoteChain" desarrollado por Lessio y Riveros Salomón (2025) de la Universidad Católica de Córdoba. Este sistema utiliza una *testnet* de Ethereum con una arquitectura de *frontend* en Angular y *backend* en .NET, incorporando autenticación mediante DNI y códigos generados por la autoridad de mesa. Aunque el prototipo no emplea biometría de forma explícita, su desarrollo materializa la capacidad técnica local para generar soluciones soberanas, reduciendo la dependencia de proveedores extranjeros y sentando las bases para una futura integración con los datos biométricos del RENAPER.

Referencias Bibliográficas

Adeniyi, J. K., Ajagbe, S. A., Adeniyi, E. A., Mudali, P., Adigun, M. O., Adeniyi, T. T., & Ajibola, O. (2024). A biometrics-generated private/public key cryptography for a blockchain-based e-voting system. *Journal of King Saud University - Computer and Information Sciences*, 36(1), 101900. DOI: <https://doi.org/10.1016/j.jksuci.2024.101900>

Barrat i Esteve, J. (2025). Online voting: Current and future practices. *International Institute for Democracy and Electoral Assistance*. DOI: <https://doi.org/10.31752/idea.2025.69>

Cámara Federal de Casación Penal de la Nación. (2024). Ciberdelitos y evidencia digital: Selección de jurisprudencia. Poder Judicial de la Nación. Secretaría de Jurisprudencia.

Chan, K. F., & Smales, L. A. (2025). U.S. Presidential news coverage: Risk, uncertainty and stocks. *International Review of Economics and Finance*, 98, 103927. DOI: <https://doi.org/10.1016/j.iref.2025.103927>

Cheeseman, N., Lynch, G., & Willis, J. (2018). Digital dilemmas: The unintended consequences of election technology. *African Affairs*, 117 (467), 177-198. DOI: <https://doi.org/10.1093/afraf/adx043>

Faruk, M. J. H., Alam, F., Islam, M., & Rahman, A. (2024). Transforming online voting: A novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. *Cluster Computing*, 27, 4015-4034. DOI: <https://doi.org/10.1007/s10586-023-04261-x>

Galindo Vácha, J. C. (2025). La inteligencia artificial (IA) en el marco de la democracia digital. *Revista de Derecho Político*, (122), 159-184. DOI: <https://doi.org/10.5944/rdp.122.2025.44745>

Gelb, A., & Diofasi Metz, A. (2018). Identification revolution: Can digital ID be harnessed for development? *Center for Global Development*.

Ibarreche, X., Martínez Elebi, C., & Di Lorenzo, C. (2025). Reconocimiento facial y tecnologías de vigilancia en América Latina: casos, proveedores y dinámicas comerciales. *AlSur*. Recuperado de: <https://www.alsur.lat>

Juneja, P. (2024). La inteligencia artificial para la gestión electoral. *International Institute for Democracy and Electoral Assistance*. DOI: <https://doi.org/10.31752/idea.2024.89>

Lessio, J. C., & Riveros Salomón, F. A. (2025). VoteChain: Sistema de votación electrónica con tecnología blockchain [Tesis de grado]. Universidad Católica de Córdoba.

Martínez, Y. (2024). El rol de la innovación en la transformación pública digital. En Papagni L. y Prince, A. *Transformación pública digital en Latinoamérica II* (pp. 83-97). Buenos Aires: Fundación Sociedad de la Información para las Américas.

Neira Orjuela, F. (2024). El uso de datos biométricos en América Latina. En F. Neira Orjuela (Coord.). *Biometría, datos personales y derechos humanos: migrantes irregulares en tránsito por México y Colombia* (pp. 23-74). México: Universidad Nacional Autónoma de México.

Observatorio de Regulación Digital y Tecnología (Deloitte & Universidad de Navarra). (2025). Informe sobre Inteligencia Artificial. Deloitte.

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., Sheidu, V. B., & Ibrahim, M. M. (2024). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing*. DOI: <https://doi.org/10.1007/s10586-024-04709-8>

Omoze, S., Omaji, S., & Edegbe, G. N. (2025). Machine learning-based multimodal biometric authentication system (facial and fingerprint recognition) for online voting systems. *AJERD*, vol. 8(1), pp. 122–128. DOI: <https://doi.org/10.53982/ajer.2025.0801.13-j>

Papagni, L. (2024). La identidad digital descentralizada como modelo de inclusión social. En Papagni L. y Prince, A. *Transformación pública digital en Latinoamérica II* (pp. 32-44). Buenos Aires: Fundación Sociedad de la Información para las Américas.

Revelo Sanchez, O., Baron Salazar, A., & Bolaños González, M. (2026). Democratic innovation: Systematic evaluation of blockchain-based electronic voting (2022-2025). *Technologies*, 14(2), 95. DOI: <https://doi.org/10.3390/technologies14020095>

Shaikh, A., Adhikari, N., Nazir, A., Shah, A. S., Baig, S., & Al Shihi, H. (2025). Blockchain-enhanced electoral integrity: A robust model for secure digital voting systems in Oman. *F1000Research*, 14 (223), Versión 3. DOI: <https://doi.org/10.12688/f1000research.160087.3>