Universidad de Buenos Aires - Legalthon. Equipo: ADAworkers.

Autores: Bel, Edith Angelica Fernanda; Chauca Romero, Sebastian Antonio; Del Roio, Fernanda Anyelen; Meijide Garcia, Micaela; Singh, Sabrina.

Tutor: Rodriguez, Francisco.

IDENTIDAD DIGITAL NACIONAL Y SOBERANÍA INFORMATIVA.

Palabras clave: Identidad digital; Soberanía informativa; Identidad auto-soberana; Blockchain; Protección de datos; autodeterminación informativa.

Abstract

En la era digital, la gestión de la identidad personal enfrenta desafíos legales y técnicos crecientes. Este estudio plantea un modelo nacional de identidad digital auto soberana (SSI) para la Argentina que garantice la soberanía informativa del individuo sobre sus datos personales. Se empleó un enfoque metodológico doctrinario y comparado: se examinó el marco jurídico argentino en materia de identificación y datos personales (Constitución Nacional; Ley 25.326, 2000; Ley 17.671, 1968; Ley 25.506, 2001) y se analizaron estándares internacionales de privacidad junto con experiencias consolidadas de identidad digital como el Reglamento eIDAS en la Unión Europea y el modelo de Estonia (Unión Europea, 2014; Gobierno de Estonia, n.d.). Además, se exploraron desarrollos blockchain y arquitecturas descentralizadas aplicables al entorno argentino (Giungato et al., 2020; Polygon Labs, 2022). Los resultados muestran que, aunque la Constitución Nacional y las leyes vigentes reconocen de forma implícita el derecho a la identidad y a la privacidad, existen vacíos normativos frente a las demandas de la sociedad digital. Las experiencias comparadas confirman la factibilidad de una identidad digital segura, descentralizada y centrada en el usuario. Así, se propone un *Sistema de Identidad Digital Soberana en el cual el Estado* actúa como garante, mientras que cada ciudadano controla sus credenciales y comparte únicamente datos mínimos mediante credenciales verificables (*VC*) y pruebas de conocimiento cero (*ZKP*). En conclusión, dotar a la identidad digital de protección equivalente a la identidad física es posible y necesario para fortalecer la confianza pública y asegurar que la autonomía y la dignidad prevalezcan en cada interacción digital.

1.Introducción

La identidad constituye un elemento vital, de carácter absolutamente personal, que forma parte esencial de la estructura jurídica contemporánea. Se consolida como un requisito indispensable para la participación tanto física como digital y aunque trasciende la mera actuación individual solo es observarse a través de ella, especialmente al momento de garantizar el acceso a servicios financieros, registros sanitarios o trámites públicos.

Actualmente existe un notorio desfasaje entre la información necesaria para dicha actuación y el sistema argentino de protección de datos producto de la sobreexposición de los mismos y su tratamiento desproporcionado. En este contexto, la evolución de los marcos regulatorios internacionales en materia de identidad electrónica y protección de datos ha impulsado un cambio de paradigma hacia modelos basados en identidades criptográficamente verificables, interoperables y sustentadas en arquitectura de gobernanza descentralizada, consideradas imprescindibles para avanzar a la auténtica soberanía de la identidad.

Desde el punto de vista jurídico argentino, la ausencia de un régimen normativo orientado a regular identificadores descentralizados, credenciales verificables, ciclos de revocación de claves, interoperabilidad regional y gobernanza estatal de infraestructuras SSI (Self-Sovereign Identity) constituye una brecha normativa significativa.

Este trabajo tiene por objeto: (I) analizar el marco teórico, jurídico y técnico que sustenta la identidad digital moderna, con especial énfasis en la distinción entre identidad, identificación y autenticación; (II) evaluar la compatibilidad del ordenamiento jurídico argentino con un sistema de identidad digital autosoberana; (III) examinar experiencias internacionales y estándares técnicos aplicables a un eventual despliegue nacional; (IV) formular un modelo integral de Sistema Nacional de Identidad Digital Soberana (SNIDS) que articule arquitectura tecnológica, gobernanza institucional y principios de protección de datos; (V) identificar los riesgos sistémicos y desafíos operativos asociados a su implementación en un Estado federal.

La relevancia del estudio radica en la creciente demanda de esquemas de identificación que permitan preservar la dignidad y autonomía del ciudadano en entornos digitales altamente interconectados y, simultáneamente, habiliten modelos de servicio público más eficientes, seguros y trazables.

2.Perspectivas éticas y filosóficas sobre Identidad Digital

La discusión contemporánea sobre la identidad digital, la protección de datos y gobernanza tecnológica no puede desvincularse de los cimientos éticos que orientan a la toma de decisiones en entornos públicos y privados. Los desarrollos vinculados a la identidad auto-soberana, los identificadores descentralizados y las arquitecturas de gobernanza algorítmica exigen un marco normativo que, además de garantizar seguridad jurídica, incorpore principios éticos que permitan preservar la dignidad humana en contextos altamente digitalizados.

En esta línea, diversas tradiciones filosóficas y teorías éticas proporcionan elementos centrales para comprender los dilemas asociados a la gestión de datos, la automatización de decisiones y el rol del Estado en la administración de identificadores digitales. La ética clásica encuentra en ***Adam Smith*** *y* su *Teoría de los sentimientos morales* (1759) una reflexión temprana sobre la conducta moral y la responsabilidad social, mientras que la ética deontológica de ***Immanuel Kant*** agrega el imperativo categórico como criterio universal para evaluar la moralidad de las acciones, principios que resultan particularmente relevantes para la toma de decisiones automatizadas y el diseño de sistemas que procesan datos personales.

Más cercano a nuestros días, ***Mary Guy*** desarrolla modelos de ética organizacional orientados al comportamiento de las instituciones públicas (*Ethical decision making in everyday work situations, 1990*), y ***Treviño*** *(Ethical Decision Making in Organizations: An Issue Contingent Model, 1991)* examina los factores que condicionan las conducta ética en organizaciones complejas. Estas perspectivas resultan aplicables para evaluar si las instituciones, estatales o privadas, que intervienen en sistemas de identidad digital cumplen con principios de transparencia, motivación y rendición de cuentas.

Por su parte ***Zygmunt Bauman*** en *Ética posmoderna* (*2005*) introduce reflexiones sobre la fragilidad de los vínculos en la modernidad líquida y los riesgos asociados a sociedades altamente interconectadas, elementos directamente relacionados a la gestión de datos y a la tensión existente entre el control y la libertad. En paralelo, debates contemporáneos, como los expuestos por ***Manuel Velázquez*** en *Ética en los negocios. Conceptos y casos* (*2006*) o ***Crane y Matten*** en *Business Ethics (2007*) aportan criterios para

analizar si los actores privados que administran datos personales lo hacen bajo marcos de gobernanza ética y respeto por los derechos fundamentales.

Para concluir, la ética de la información y algorética, desarrolladas por ***Luciano Floridi*** introduce lineamientos para enfrentar desafíos asociados a la transparencia algorítmica, la prevención de sesgos y la necesidad de decisiones automatizadas explicables y auditables.Estos enfoques son sustanciales para fundamentar éticamente un Sistema Nacional de Identidad Digital Soberana, al articular tecnología, derechos primordiales y valores democráticos.

3.Marco teórico: Identidad Personal y su extensión digital

En las sociedades contemporáneas, la vida digital se ha convertido en un ámbito inevitable de interacción y participación, y por ello la identidad digital debe entenderse como una prolongación intangible de la persona en el ciberespacio. La identidad constituye una categoría fundamental dentro del pensamiento jurídico y filosófico, articulándose como un eje que permite comprender la continuidad del sujeto a lo largo del tiempo y su reconocimiento en el entramado social. Desde la hermenéutica filosófica, Paul Ricoeur distingue dos dimensiones esenciales: la identidad idem, vinculada a los aspectos permanentes y relativamente estables del individuo, y la identidad ipse, asociada a la capacidad reflexiva, la coherencia narrativa y la autocomprensión del sujeto a través de sus experiencias vitales (*Ricoeur, 1990*). Esta doble dimensión muestra que la identidad no se agota en atributos estáticos, sino que integra elementos dinámicos que expresan la autonomía y singularidad de cada persona.

En el ámbito jurídico, la afectación de la identidad; como ocurre en supuestos de falsificación, suplantación, robo de identidad, etc; constituye un ataque directo a la dignidad humana, al lesionar la esfera más íntima de la personalidad (*Felicetti, 1999)*. Para comprender los desafíos que plantea su traslado al entorno digital, resulta indispensable diferenciar la identidad en sentido filosófico y moral, de la identificación en su dimensión técnico-jurídica. Mientras la primera se refiere al núcleo personalísimo de la individualidad, la identificación alude al conjunto de datos, atributos y registros que permiten al Estado y a terceros verificar la existencia y legitimidad de un ciudadano en contextos institucionales (*Fernández Sessarego, 2015)*.

Esta extensión no constituye un mero dato accesorio, sino una manifestación directa de la individualidad que posibilita o impide el acceso a servicios esenciales, trámites administrativos, intercambios económicos y ejercicios cotidianos de la ciudadanía. Por ese motivo, la identidad digital exige una tutela equivalente a la que históricamente ha recibido la identidad física.

El tratamiento desproporcionado o la recolección indiscriminada de información personal vulnera la intimidad protegida por el artículo 11 de la Convención Americana sobre Derechos Humanos. En este escenario, el principio de autodeterminación informativa, conocido doctrinariamente y regulado en el derecho argentino, se constituye como un elemento central del modelo contemporáneo de protección de la persona (ver anexo 1). Este principio implica la facultad del individuo para decidir sobre el uso, circulación y destino de su información, asegurando control y transparencia sobre los flujos de datos que lo representan. Desde esta perspectiva, la identidad digital no puede considerarse una categoría secundaria, sino un derecho personalísimo inseparable de la dignidad humana y amparado por el bloque de constitucionalidad federal (Constitución Nacional, art. 75 inc. 22).

La propuesta de Identidad Digital Soberana parte justamente de este reconocimiento: dotar a los ciudadanos del dominio efectivo sobre su configuración digital mediante mecanismos técnicos y jurídicos que impidan apropiaciones indebidas, usos no consentidos y manipulaciones que comprometan su individualidad en entornos altamente interconectados. El desafío no consiste solamente en digitalizar la identificación, sino en asegurar que el entorno digital no desdibuje la centralidad del sujeto, ni erosione los fundamentos éticos que sostienen su personalidad jurídica a través de una practicidad en el ejercicio de la identificación.

4.Marco Normativo Argentino: Identidad y datos personales

El ordenamiento jurídico argentino ofrece un conjunto de normas que, si bien no fueron diseñadas específicamente para el ecosistema digital contemporáneo, establecen bases sólidas para desarrollar un sistema de identidad electrónica que respete la autonomía informativa y garantice altos estándares de seguridad. La Constitución Nacional constituye el punto de partida: el artículo 18 asegura la inviolabilidad de la documentación y de la correspondencia, el artículo 19 consagra el principio de reserva y protege la esfera privada frente a injerencias arbitrarias, y el artículo 16 exige un tratamiento igualitario en el acceso y

uso de instrumentos identificatorios. A su vez, el artículo 33 reconoce derechos implícitos derivados de la personalidad, lo que incluye la protección frente a interferencias indebidas en la configuración identitaria. Este plexo se complementa con los tratados de derechos humanos incorporados con jerarquía constitucional por el artículo 75 inciso 22, entre ellos la Convención Americana, que otorga una tutela reforzada a la privacidad y la identidad.

En el plano legislativo, la Ley 17.671 estructuró el régimen tradicional de identificación civil, otorgando al RENAPER la competencia exclusiva en la certificación de identidad. Sin embargo, su diseño responde a un paradigma analógico centrado en documentos físicos y bases de datos centralizadas, insuficiente para los desafíos tecnológicos actuales. Posteriormente, la Ley 25.326 definió los principios rectores del tratamiento de datos personales, licitud, finalidad, calidad y minimización, los cuales resultan esenciales para cualquier arquitectura digital moderna. Para la propuesta adquiere especial relevancia el principio de minimización, que obliga a evitar la recolección de datos innecesarios y a limitar el tratamiento al estricto propósito que justifica la operación informacional.

Por su parte, la Ley 25.506 introdujo la firma digital dentro del derecho argentino y estableció la infraestructura nacional de clave pública, habilitando la equivalencia jurídica entre documentos electrónicos y documentos en soporte papel. Esta disposición constituye un antecedente indispensable para reconocer la validez de credenciales digitales emitidas bajo estándares criptográficos avanzados.

La evolución jurisprudencial reciente revela una creciente preocupación por las vulnerabilidades del entorno digital. En el caso "*Toledo, Víctor c/ Perero, Pablo Ezequiel s/ejecutivo*" (CNCom., Sala C), la Cámara Comercial abordó una denuncia de supuesta suplantación de identidad en actuaciones electrónicas, destacando la vigencia del principio de publicidad judicial y la necesidad de que las restricciones de acceso a datos personales se ajusten estrictamente a los requisitos de la Ley 25.326. La respuesta judicial evidencia que la infraestructura normativa actual no ofrece soluciones específicas para escenarios de fraude identitario digital. En "*Bramajo, Norma Graciela c/ Mercado Libre SRL s/ ordinario*" (Sala E), el tribunal analizó la posible usurpación de identidad en plataformas electrónicas y ordenó la citación de terceros, señalando la complejidad probatoria que presentan las interacciones digitales y la ausencia de marcadores confiables de identidad.

Asimismo, el Decreto 744/2019 introdujo el DNI en formato digital, pero conservó un modelo centralizado y de revelación completa de datos, reproduciendo los riesgos de sobreexposición que caracterizan a los documentos físicos. No incorporó mecanismos de compartimentación ni control granular por parte del titular.

A pesar de estos avances, el marco normativo argentino requiere una actualización integral que incorpore estándares contemporáneos, reconozca la identidad digital como manifestación protegida y establezca reglas claras para sistemas basados en credenciales verificables, identificadores descentralizados y esquemas de verificación selectiva

5.Marco jurídico ampliado

La protección de datos personales y la gestión de la identidad digital se encuentran en un proceso global de estandarización que ha transformado las exigencias técnicas y jurídicas para los Estados. Las regulaciones internacionales no solo orientan buenas prácticas, sino que influyen directamente en la legitimidad e interoperabilidad de los sistemas nacionales.

En el ámbito europeo, el Convenio 108 del Consejo de Europa y su Protocolo de Enmienda 108+ constituyen instrumentos pioneros en la regulación del tratamiento automatizado de información personal. La actualización 108+ introduce obligaciones vinculadas a la supervisión de decisiones algorítmicas, la transparencia de procesos automatizados y la necesidad de evaluaciones de impacto, elementos esenciales para modelos de identidad digital basados en tecnologías avanzadas (Consejo de Europa, 1981; 2018). Paralelamente, el Reglamento General de Protección de Datos (RGPD) consolida principios de privacidad desde el diseño, proporcionalidad y control individual sobre los flujos informativos, estableciendo un estándar que ha influido en reformas legislativas en América Latina, incluida la propuesta argentina de actualización de la Ley 25.326.

En materia de identificación digital, el Reglamento eIDAS de la Unión Europea define categorías de firmas electrónicas, principios de interoperabilidad transfronteriza y el reconocimiento legal de identidades electrónicas emitidas por los Estados miembros (*Reglamento n.º 910/2014*). Este modelo demuestra que la construcción de credenciales electrónicas exige tanto soporte técnico como armonización jurídica.

Entre las experiencias comparadas, Estonia representa el paradigma de infraestructura digital integral basada en autenticación fuerte, registro distribuido y auditoría ciudadana. Su

modelo permite al usuario verificar quién accedió a sus datos y con qué finalidad, lo que fortalece la confianza pública. En América Latina, Chile avanza en la modernización de documentos de identidad incorporando biometría para habilitar su uso seguro en entornos remotos (*Juárez, 2024*). A nivel nacional, el proyecto QuarkID implementado por el Gobierno de la Ciudad Autónoma de Buenos Aires constituye la primera iniciativa estatal basada en credenciales verificables y estándares SSI, demostrando la viabilidad técnica y política de adoptar modelos descentralizados (*ITSitio, 2025*).

Asimismo, tecnologías como identificadores descentralizados (DID), credenciales verificables y pruebas de conocimiento cero (ZKP) han sido incorporadas progresivamente en marcos regulatorios internacionales y guías técnicas del W3C, permitiendo materializar el principio de minimización de manera efectiva. Su eventual adopción en Argentina debe articularse con la validez jurídica de los instrumentos electrónicos prevista en el Código Civil y Comercial (arts. 286 y 319), integrando estándares globales sin perder coherencia interna.

La convergencia entre estos instrumentos demuestra que un sistema nacional de Identidad Digital Soberana debe alinearse con principios internacionales para garantizar interoperabilidad, legitimidad y protección reforzada de los derechos fundamentales en el entorno digital

6.Estándares Internacionales e iniciativas comparadas

El método comparado resulta indispensable para incorporar buenas prácticas globales en el diseño de un modelo argentino de identidad digital soberana. Las referencias internacionales en materia de protección de datos y sistemas de identificación electrónica proporcionan lineamientos técnicos y normativos útiles para orientar una transición ordenada. En el ámbito europeo, el Convenio 108 y su Protocolo de Enmienda 108+ establecen estándares avanzados en protección de datos, transparencia y supervisión de decisiones automatizadas (*Consejo de Europa, 1981; Consejo de Europa, 2018*). Asimismo, el Reglamento General de Protección de Datos enfatiza principios clave para la arquitectura digital contemporánea, incluyendo la privacidad desde el diseño y la privacidad por defecto, ampliamente reconocidos como referentes regulatorios *(Reglamento 679/2016 UE, 2016)*. Por su parte, el Reglamento eIDAS define principios de interoperabilidad y reconocimiento transfronterizo de identidades electrónicas, incluyendo la equivalencia legal entre firma digital

y manuscrita *(Reglamento N°910/2014 UE)*, elementos relevantes para un eventual esquema regional en el MERCOSUR.

Entre las experiencias comparadas de identidad digital, el caso de Estonia constituye un modelo paradigmático basado en infraestructura criptográfica y autenticación electrónica para servicios públicos y privados, generando eficiencia administrativa y transparencia en el acceso a datos personales mediante registros de auditoría accesibles al usuario (*Gobierno de Estonia, n.d*.). En el ámbito regional, Chile avanza con la incorporación de un documento de identidad dotado de soportes biométricos para habilitar su uso remoto en servicios digitales (Juárez, 2024).

Por último, en Argentina, el proyecto QuarkID implementado por el Gobierno de la Ciudad Autónoma de Buenos Aires aplica un enfoque SSI mediante blockchain para credenciales verificables oficiales, utilizando verificación fuera de línea como mecanismo de reducción de dependencia centralizada y de exposición de datos personales (*Redacción ITSitio, 2025)*. Estas iniciativas evidencian la viabilidad técnica y política de adoptar un modelo auto-soberano respaldado por el Estado y centrado en el ciudadano.

7.Propuesta de modelo de Identidad Digital Soberana para Argentina

Integrando los hallazgos normativos y las experiencias comparadas, se presenta un modelo técnico-jurídico para la implementación de un sistema nacional de Identidad Digital Soberana centrado en el ciudadano y basado en una arquitectura descentralizada. La transformación requiere la sanción de una Ley de Identidad Digital Soberana que reconozca la identidad digital como emanación directa del derecho personalísimo a la identidad, con la misma protección constitucional que su manifestación física, afirmando que pertenece exclusivamente al titular y que su tratamiento restrictivo debe guiarse por los principios de consentimiento, minimización de datos y confidencialidad previstos en la Ley 25.326. La normativa deberá definir responsabilidades de emisores y verificadores, mecanismos de auditoría accesibles y prohibiciones de almacenamiento indebido.

Desde el punto de vista técnico, la infraestructura descansa en una red de registros distribuidos utilizada como ancla de confianza para garantizar seguridad e inmutabilidad. Se propone el uso de blockchain pública, como Cardano, dada su orientación hacia seguridad, sostenibilidad y escalabilidad, para registrar únicamente identificadores descentralizados y

claves públicas de organismos emisores, sin almacenar datos personales, sino únicamente hashes verificables. Este enfoque permite preservar la privacidad desde el diseño y facilita la verificación distribuida. Para asegurar el desempeño en escenarios de millones de usuarios, la arquitectura puede complementarse con soluciones de segunda capa, como canales de procesamiento off-chain que reducen la carga sobre la red principal sin comprometer la integridad de las verificaciones.

El modelo prevé que cada ciudadano gestione uno o varios identificadores descentralizados vinculados criptográficamente a claves controladas exclusivamente por él, permitiendo incluso variantes seudónimas para limitar la correlación transversal de actividades. Sobre esa base, distintos organismos públicos emitirán credenciales verificables que afirman atributos concretos, por ejemplo, identidad, estado civil, formación académica, licencias, entre otros y que permanecen bajo custodia del ciudadano en una billetera digital instalada en su dispositivo. La verificación de estas credenciales se realiza mediante la firma del emisor y la clave pública registrada en la infraestructura distribuida, permitiendo verificaciones incluso sin conexión si el verificador dispone de claves actualizadas. Este esquema habilita la presentación selectiva de atributos, evitando la exposición de información irrelevante, y constituye una materialización operativa del principio de minimización.

Para maximizar la privacidad, el sistema incorpora pruebas de conocimiento cero, que permiten demostrar condiciones específicas sin revelar datos subyacentes: por ejemplo, acreditar mayoría de edad sin revelar la fecha de nacimiento. Las ZKP proporcionan garantías criptográficas robustas que reducen la sobre-recolección de información y limitan la posibilidad de perfilamiento por parte de terceros. La billetera digital debe contar con medidas de autenticación fuerte, mecanismos de recuperación ante pérdida de dispositivo y procesos de revocación simple y transparente en caso de incidentes.

Respecto del rol estatal, el Estado Nacional, a través de RENAPER u organismo especializado, actuará como autoridad certificante de raíz, encargada de validar atributos esenciales en la emisión inicial, sin centralizar el flujo cotidiano de datos ni apropiarse del manejo de credenciales. Debe asegurarse la equivalencia legal entre documentos físicos y credenciales verificables, garantizando su reconocimiento pleno en trámites públicos y privados conforme a la Ley 25.506. La implementación del sistema debe desarrollarse de manera progresiva mediante programas piloto voluntarios, auditorías públicas continuas, uso de software abierto, políticas de inclusión digital y cooperación entre organismos estatales,

sector privado y academia. El éxito del modelo dependerá de esta combinación equilibrada entre seguridad técnica, actualización normativa, transparencia institucional y construcción de confianza ciudadana.

8.Beneficios esperados

La adopción del modelo de Identidad Digital Soberana generará beneficios significativos alineados con los resultados observados en experiencias internacionales consolidadas. La problemática expuesta en fallos como Toledo y Bramajo, donde los tribunales debieron intervenir ante situaciones de suplantación de identidad y operaciones digitales fraudulentas, demuestra que la inexistencia de mecanismos seguros de verificación expone a los ciudadanos a daños que podrían evitarse a través de una arquitectura de identidad digital autosoberana. En primer lugar, se promueve el empoderamiento ciudadano mediante un control granular sobre los datos personales, reforzando la autonomía y reduciendo la necesidad de entregar copias físicas o exponer información sensible en trámites cotidianos. La presentación selectiva de atributos mediante credenciales verificables y pruebas criptográficas minimiza el riesgo de robo de identidad, filtraciones o usos indebidos. Un ejemplo cotidiano permite dimensionar la problemática actual: cuando una persona compra una bebida alcohólica en un supermercado y se le solicita acreditar su mayoría de edad, el DNI físico expone información innecesaria como nombre completo, domicilio, número de identificación y fecha exacta de nacimiento, aun cuando el único dato relevante es si posee o no más de dieciocho años.

La revelación indiscriminada de datos personales en situaciones de mínima relevancia constituye un riesgo concreto que favorece la suplantación de identidad, el fraude documental y la recolección abusiva de información por parte de actores públicos o privados sin control ciudadano. Un sistema de Identidad Digital Soberana permitiría validar únicamente el atributo requerido, “mayor de 18 años”, mediante credenciales verificables o pruebas criptográficas sin revelar datos subyacentes, materializando el principio de minimización previsto en la Ley 25.326 y reduciendo significativamente la exposición innecesaria de información personal.

Además, la transparencia otorgada por registros de acceso, como los implementados en Estonia, incrementa la confianza pública y obliga a un uso responsable de la información por parte de verificadores institucionales (*Gobierno de Estonia, n.d.*).

En segundo lugar, el sistema fortalece la seguridad jurídica al reconocer la equivalencia entre identidad digital y tradicional, respaldada por la infraestructura de clave pública establecida por la Ley 25.506 y por la solidez criptográfica en la atribución de autoría, lo que reduce conflictos y litigios asociados a transacciones electrónicas (Ley N.º 25.506, 2001). Asimismo, genera eficiencia administrativa y ahorro económico al habilitar verificaciones remotas y reducir exigencias presenciales, lo que simplifica trámites y disminuye costos operativos para ciudadanos, empresas y el Estado. En tercer lugar, impulsa la innovación y favorece la economía digital al habilitar procesos de verificación de identidad ágiles para sectores como fintech, salud, educación o comercio, fortaleciendo la competitividad y la inclusión financiera. Finalmente, el sistema contribuye al fortalecimiento democrático al posibilitar prácticas participativas seguras, como el eventual voto electrónico con autenticación robusta, así como permitir el acceso a derechos fundamentales incluso en casos de pérdida documental o desplazamientos forzados (*Caballero, 2021*). En conjunto, estos beneficios evidencian que la Identidad Digital Soberana constituye una infraestructura estratégica para el desarrollo digital, económico y ciudadano.

9.Desafíos y Riesgos

A pesar de los beneficios que ofrece el modelo de Identidad Digital Soberana, su implementación conlleva desafíos significativos que requieren abordaje integral y estratégico. En primer lugar, la brecha digital representa un riesgo concreto para la adopción equitativa del sistema, ya que la falta de acceso a dispositivos tecnológicos o de habilidades digitales podría excluir a sectores vulnerables. Para evitarlo, deben contemplarse alternativas físicas complementarias, como tarjetas inteligentes con chip y espacios de asistencia presencial, junto con políticas activas de alfabetización digital que garanticen accesibilidad plena. En segundo lugar, la seguridad informática y el riesgo asociado al dispositivo del usuario constituyen un desafío crítico: la descentralización reduce la exposición sistémica, pero exige medidas estrictas de protección individual, incluyendo certificación de aplicaciones oficiales, actualizaciones permanentes y educación sobre custodia de claves privadas, con mecanismos rápidos de revocación y reemisión frente a incidentes.

Un tercer desafío relevante es la adopción cultural y la construcción de confianza pública en torno al nuevo modelo. Las transformaciones estructurales en materia de identidad requieren transparencia institucional y comunicación clara para superar resistencias y temores vinculados al uso de tecnologías criptográficas y blockchain. La publicación de código

abierto, la realización de auditorías independientes y la implementación de programas piloto acotados permiten fortalecer la legitimidad social y reducir la incertidumbre.

Por esto, la interoperabilidad internacional constituye otro desafío, ya que el reconocimiento global de credenciales digitales requiere acuerdos de reciprocidad y armonización progresiva con estándares digitales emergentes como los desarrollados en la Unión Europea bajo el marco eIDAS (*reglamento 910/2014,2014*). La presencia de litigios vinculados a la usurpación y exposición indebida de datos personales, evidenciada en los casos Toledo y Bramajo, refleja que la ausencia de regulaciones claras genera incertidumbre jurídica y traslada al sistema judicial conflictos prevenibles mediante mecanismos seguros de validación de identidad digital.

En síntesis, el éxito del sistema dependerá de la combinación equilibrada entre solidez técnica y normativa, participación social y generación gradual de capital de confianza entre los actores involucrados.

10. Conclusión

La presente investigación examinó la necesidad de dotar a la identidad digital en Argentina de un marco de protección y validez equivalente al de la identidad física, asegurando la soberanía informativa del individuo y la tutela de los derechos personalísimos asociados a la dignidad humana. El análisis teórico, normativo y comparado permitió constatar la existencia de una brecha entre el reconocimiento jurídico del derecho a la identidad y la realidad tecnológica actual, que expone a los ciudadanos a riesgos de abuso y sobreexposición por la ausencia de un mecanismo de identificación electrónica seguro y selectivo basado en la minimización del tratamiento de datos (Ley N.º 25.326, 2000). Asimismo, la experiencia internacional y los avances tecnológicos asociados a arquitecturas autosoberanas demuestran la viabilidad de conciliar seguridad, eficiencia y privacidad mediante credenciales verificables e infraestructuras basadas en estándares descentralizados.

La propuesta de un Sistema Nacional de Identidad Digital Soberana constituye una hoja de ruta viable que busca reconfigurar los roles institucionales al establecer al Estado como garante de autenticidad e integridad, y al ciudadano como titular y controlador pleno de su identidad digital. Este modelo desplaza el esquema centralizado y de revelación total hacia uno descentralizado que respeta el espíritu de los artículos 19 y 33 de la Constitución Nacional (Constitución de la Nación Argentina, 1994). Su implementación exige un marco

normativo específico, inversión en infraestructura, transparencia tecnológica y políticas activas de inclusión. La evidencia analizada confirma que dotar a la identidad digital de igual protección que la identidad física no solo es posible, sino imprescindible para garantizar derechos fundamentales en la sociedad digital contemporánea. La Identidad Digital Soberana representa una evolución necesaria y estratégica, posicionando a la Argentina en condiciones de liderar un proceso regional de integración entre derecho y tecnología orientado a fortalecer la autonomía, la seguridad jurídica y la dignidad humana.

Anexo I. Consideraciones metodológicas

Este estudio se llevó a cabo mediante un enfoque de investigación cualitativa, combinando el análisis doctrinario jurídico, la revisión de estándares técnicos internacionales y el método comparado.

Construcción del marco teórico conceptual

Se inició con una exhaustiva revisión bibliográfica para construir un marco teórico robusto del concepto de identidad personal. Se consultaron fuentes primarias y secundarias de diversas disciplinas:

- Filosofía: Se recurrió a la obra de Paul Ricoeur (1990) para distinguir conceptualmente la identidad *idem* (permanencia en el tiempo) de la identidad *ipse* (fidelidad a sí mismo y coherencia biográfica).
- Psicología y sociología: Se analizaron las contribuciones sobre el autoconcepto, la continuidad de la conciencia (Erikson, citado en Fernández Sessarego, 2015) y la Identidad Social (Tajfel, 1981) para comprender las dimensiones interna y relacional de la identidad.
- Doctrina jurídica: Se examinó la literatura especializada en derechos personalísimos (Felicetti, 1999; Fernández Sessarego, 2015) para conceptualizar la identidad como un derecho fundamental, distinguiéndose del mero concepto de identificación.

Análisis normativo nacional e interpretación jurisprudencial

Se realizó un análisis sistemático del ordenamiento jurídico argentino para identificar los fundamentos y las brechas legales.

- Constitución nacional: Se examinaron en detalle los artículos 14, 16, 18, 19, 33, 43 y 75 inciso 22, interpretando su alcance para la tutela de la identidad, la privacidad y el hábeas data. Se prestó especial atención a la jurisprudencia relevante de la cámara nacional de apelaciones en lo contencioso administrativo federal. Capital federal. Ciudad autónoma de buenos aires (e.g. fallo Palazzi, Pablo c/ EN-Registro Nacional de las Personas s/ Hábeas data. 2025) para entender la interpretación legal de “autodeterminación informativa” y la acción de hábeas data.

- Leyes nacionales: Se revisaron las leyes fundamentales: Ley 17.671 (Identificación y RENAPER), Ley 25.326 (Protección de Datos Personales), Ley 25.506 (Firma Digital) y el Decreto 744/2019 (DNI Digital). El objetivo fue determinar cómo cada norma regula la identificación y la protección de datos, y qué competencias asigna al Estado.

Estudio de estándares internacionales

Se incorporó la perspectiva global mediante el estudio de estándares que influyen o son referentes para la política de datos argentina:

- Derechos humanos: Se analizaron instrumentos con jerarquía constitucional, como la Convención Americana sobre Derechos Humanos (1969) y la Convención sobre los Derechos del Niño (1989), por sus disposiciones vinculantes sobre identidad y privacidad.
- Protección de datos: Se examinó el Convenio 108 y su Protocolo 108+ del Consejo de Europa (2018), ratificados por Argentina, y los principios rectores del Reglamento General de Protección de Datos (GDPR) de la Unión Europea, considerados como el estándar global de *privacy by design*.

Método comparado y revisión tecnológica

Se empleó el método comparado para extraer lecciones aplicables y se investigaron las soluciones tecnológicas operativas:

- Modelos estatales: Se investigó la experiencia europea bajo el Reglamento eIDAS (UE 910/2014) y el caso pionero de Estonia (e-Estonia, 2021) en la implementación de identidad electrónica universal. Se relevó información sobre iniciativas regionales recientes, como la nueva cédula digital anunciada en Chile (Juárez, 2024).
- Soluciones SSI: Se exploraron desarrollos tecnológicos descentralizados basados en el estándar SSI, incluyendo la plataforma Polygon ID (Polygon Labs, 2022) y el proyecto QuarkID implementado por el gobierno de la Ciudad de Buenos Aires (Redacción ITSitio, 2025). Se analizaron los estándares del World Wide Web Consortium (W3C) para DID y VC (W3C, 2020) y los fundamentos de las Pruebas de Conocimiento Cero (ZKP) (Naor et al., 1998; Chaum, 1985).

Finalmente, se procedió al diseño propositivo de la arquitectura técnica y jurídica para la implementación del Sistema de Identidad Digital Soberana en Argentina. Este diseño integró los principios jurídicos identificados (consentimiento, minimización, equivalencia legal), las mejores prácticas técnicas observadas (uso de DLT, SSI) y las capacidades específicas de la tecnología *blockchain* seleccionada (*Cardano*, 2022). El trabajo es de naturaleza exploratoria y propositiva, fundamentando las recomendaciones en el análisis normativo y comparativo.

Referencias

Normativa y jurisprudencia.

Toledo, Víctor c/ Perero, Pablo Ezequiel s/ ejecutivo. Cámara Nacional de Apelaciones en lo Comercial, Sala C, 16 de abril de 2024.

Bramajo, Norma Graciela c/ Mercado Libre SRL s/ ordinario. Cámara Nacional de Apelaciones en lo Comercial, Sala E, 30 de abril de 2024.

Palazzi, Pablo c/ EN-Registro Nacional de las Personas s/ Hábeas data. Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal, Sala 5, 13 de febrero de 2025.

Constitución de la Nación Argentina. (1994). Buenos Aires, Argentina: Boletín Oficial.

Ley N.º 17.671. (1968). Identificación, Registro Nacional de las Personas. Buenos Aires, Argentina: Boletín Oficial.

Ley N.º 25.326. (2000). Protección de los Datos Personales. Buenos Aires, Argentina: Boletín Oficial.

Ley N.º 25.506. (2001). Firma Digital. Buenos Aires, Argentina: Boletín Oficial.

Presidencia de la Nación. (2019). *Decreto 744/2019* - Implementación del DNI en formato digital. Buenos Aires, Argentina: Boletín Oficial.

Tratados y normas internacionales.

Abuelas de Plaza de Mayo. (2013). *Derecho a la Identidad: los "artículos argentinos" de la Convención sobre los Derechos del Niño.* Buenos Aires, Argentina: Organización Abuelas de Plaza de Mayo.

Consejo de Europa. (1981). *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* (Convenio 108). Estrasburgo.

Consejo de Europa. (2018). *Protocolo de Enmienda al Convenio 108 para la protección de las personas en relación con el tratamiento de datos de carácter personal* (Convenio 108+). Estrasburgo.

Convención Americana sobre Derechos Humanos. (1969). San José, Costa Rica.

Convención sobre los Derechos del Niño. (1989). Nueva York: Asamblea General de las Naciones Unidas.

Declaración Universal de Derechos Humanos. (1948). París: Asamblea General de las Naciones Unidas.

Unión Europea. (2014). *Reglamento (UE) N.º 910/2014* del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza (eIDAS). Diario Oficial de la UE L257/73.

Unión Europea. (2016). *Reglamento (UE) 2016/679* del Parlamento Europeo y del Consejo, *Reglamento General de Protección de Datos (GDPR).* Diario Oficial de la UE L119/1.

Doctrina y artículos académicos.

Caballero, F. (2021). *Democracia digital y voto electrónico: desafíos de la identificación remota.* Revista de Derecho Informático, 15(2), 45-67.

Felicetti, H. R. (1999). *Derecho a la identidad personal.* Buenos Aires, Argentina: Gráfica Yanel.

Fernández, D., & Lago, A. (2021). *Identidad digital y protección de datos en Argentina: Diagnóstico y propuestas.* Jornadas de Gobierno Abierto, 7(1), 30-35.

Fernández Sessarego, C. (2015). *Derecho y persona* (5.ª ed.). Lima, Perú: Palestra Editores.

Ricoeur, P. (1990). *Sí mismo como otro.* Madrid, España: Siglo XXI.

Rodríguez, M. (2019). *Autodeterminación informativa y protección de datos personales en la era digital.* Revista Jurídica de la Universidad de Palermo, 20(1), 99-120.

Tajfel, H. (1981). *Human groups and social categories: Studies in social psychology*. Cambridge, UK: Cambridge University Press.

Zúñiga, L. (2020). *Identidad digital autosoberana: La nueva frontera de los derechos personalísimos.* Revista Latinoamericana de Derecho y Tecnología, 5(2), 25-48.

Tecnología y experiencias comparadas.

Cardano. (2022). *Hydra Release Notes*. Obtenido de https://docs.cardano.org

Chaum, D. (1985). *Security without identification: Transaction systems to make Big Brother obsolete*. Communications of the ACM, 28(10), 1030-1044.

Giungato, P., Rana, R., Tarabella, A., & Tricase, C. (2020). *Blockchain applications and sustainability issues. Current Opinion in Environmental Science & Health,* 5, 13-18.

Gobierno de Estonia. (n.d.). e-Estonia: *The Digital Society.* Obtenido de https://e-estonia.com

Juárez, A. (2024, 27 de junio). *Chile introduce la identidad digital en su nueva cédula*. Sovos. Obtenido de https://sovos.com

Naor, M., & Yung, M. (1998). *Universal one-way hash functions and their cryptographic applications.* Proceedings of the 21st ACM Symposium on Theory of Computing, 33-43.

Polygon Labs. (2022, 29 de marzo). Introducing Polygon ID: *Zero-Knowledge Identity for Web3*. *Polygon Technology Blog*. Obtenido de https://polygon.technology

Redacción ITSitio. (2025, 3 de febrero). QuarkID: *el Gobierno de la Ciudad de Buenos Aires revoluciona la identidad digital*. ITSitio. Obtenido de https://www.itsitio.com

W3C. (2020). *Decentralized Identifiers* (DIDs) v1.0: Core architecture, data model, and representations. World Wide Web Consortium Recommendation