REVISTA JURÍDICA DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES | UNT
ISSN : 3072 - 8169 | VOL. 1, NÚM. 1, AÑO 2025

Protección de datos personales en salud digital: entre la innovación tecnológica y la bioética

Protection of personal data in digital health: between technological innovation and bioethics

Melisa Denise Veliz*

Autora:
Dra. Melisa Denise Veliz
Universidad Nacional de Tucumán (UNT).

Recibido: 13/08/2025
Aceptado: 01/10/2025

Citar como:
VELIZ, Melisa Denise (2025): "Protección de datos personales en salud digital: entre la innovación tecnológica y la bioética", *Revista Jurídica de la Facultad de Derecho y Ciencias Sociales UNT, Vol. 1, Núm. 1*.

Resumen: La digitalización de los sistemas de salud ha transformado radicalmente la forma en que se generan, almacenan, procesan y comparten datos relacionados con la salud de las personas. Este proceso ha traído consigo innegables beneficios en términos de eficiencia, accesibilidad, calidad de atención y capacidad para personalizar diagnósticos y tratamientos. Sin embargo, también ha creado un nuevo campo de tensiones jurídicas, éticas y sociales, especialmente cuando se trata de datos personales sensibles —como los datos biométricos, genéticos, de historial clínico o de hábitos de vida— que forman parte de la identidad más íntima del ser humano. Este trabajo analiza, desde una perspectiva integral, los desafíos que enfrenta la protección de datos personales en salud digital en el marco de la legislación argentina, contrastando con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y las recomendaciones de la Organización Mundial de la Salud (OMS). Asimismo, se examinan los principios fundamentales de la bioética como marco para garantizar que la innovación tecnológica en salud se desarrolle de manera compatible con los derechos humanos y la dignidad de las personas. A partir de un análisis crítico del régimen jurídico vigente, se propone la necesidad urgente de

* Abogada y Procuradora egresada de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Tucumán (UNT). Especialista en Derecho Civil y Cibercrimen por Universidad de Palermo (UP). Becaria del programa Voces Emergentes otorgada por la Fundación Federalismo y Libertad. Correo electrónico: milisaveliz@gmail.com ORCID 0009-0003-4178-0859.

reformas normativas e institucionales que permitan abordar los riesgos asociados al uso de inteligencia artificial, big data y plataformas de e-health. El artículo se nutre de doctrina especializada, jurisprudencia relevante, casos reales y propuestas concretas de política pública.

Palabras claves: salud digital, datos personales, consentimiento informado, bioética

Abstract: The digitalization of health systems has radically transformed how health-related data is generated, stored, processed, and shared. This transformation has brought undeniable benefits in terms of efficiency, accessibility, quality of care, and the ability to personalize diagnoses and treatments. However, it has also created a new field of legal, ethical, and social tensions, especially when it comes to sensitive personal data—such as biometric, genetic, medical history, or lifestyle information—that forms part of the most intimate identity of human beings.This paper analyzes, from a comprehensive perspective, the challenges faced by personal data protection in digital health within the framework of Argentine legislation, contrasting it with international standards such as the European Union's General Data Protection Regulation (GDPR) and the recommendations of the World Health Organization (WHO). It also examines the fundamental principles of bioethics as a framework to ensure that technological innovation in health develops in a manner compatible with human rights and human dignity.Based on a critical review of the current legal regime, this article proposes the urgent need for regulatory and institutional reforms to address the risks associated with artificial intelligence, big data, and e-health platforms. The paper draws on specialized doctrine, relevant case law, real-world examples, and concrete public policy proposals.

Keywords: digital health, personal data, informed consent, bioethics

I. INTRODUCCIÓN: EL AUGE DE LA SALUD DIGITAL Y EL PROBLEMA JURÍDICO

En las últimas dos décadas, pero especialmente a partir de la pandemia de COVID-19, los sistemas de salud han experimentado una acelerada digitalización como ser las plataformas de telemedicina, aplicaciones móviles para monitoreo de la salud, dispositivos portátiles que registran signos vitales en tiempo real, sistemas de historia clínica electrónica interoperable y algoritmos basados en inteligencia artificial para el diagnóstico y pronóstico, integrándose de forma casi imperceptible a la práctica sanitaria cotidiana.

Esta revolución digital ha sido impulsada por varios factores como los avances tecnológicos en almacenamiento masivo de datos, procesamiento en la nube y *machine learning;* la demanda social de servicios de salud más rápidos, personalizados y accesibles; necesidades del sistema de optimizar recursos y reducir costos; pandemias y emergencias sanitarias, que aceleraron la adopción de modelos de atención a distancia.

Sin embargo, la digitalización trae aparejado un cambio cualitativo: los datos de salud ya no se encuentran encerrados en un archivo físico en la institución médica, sino que circulan por redes informáticas globales, muchas veces

gestionadas por empresas privadas con intereses comerciales y modelos de negocio basados en la monetización de la información. Y la pregunta es la siguiente: ¿dónde queda la confidencialidad en términos de privacidad y control personal?

El problema jurídico en este nuevo ecosistema tiene diferentes dimensiones. Los datos de salud se han convertido en un recurso estratégico, no solo para el tratamiento individual de pacientes, sino también para investigación médica, desarrollo de fármacos, creación de modelos predictivos y optimización de políticas sanitarias. Pero la recolección, almacenamiento y análisis masivo de datos sensibles plantea riesgos considerables como la pérdida de control por parte del titular de los datos, filtraciones o *hackeos* que exponen información médica, discriminación basada en información genética o de salud y "reidentificación" de datos supuestamente anónimos mediante técnicas de *big data*.

En Argentina, el marco legal se apoya principalmente en la Ley Nº 25.326 de Protección de Datos Personales y la Ley Nº 26.529 de Derechos del Paciente, ambas anteriores a la irrupción masiva de la inteligencia artificial médica y las plataformas globales de *e-health*. Esto genera un desfasaje entre la realidad tecnológica y la protección jurídica efectiva.

El objetivo de este artículo es analizar este desfasaje, evaluando si el régimen jurídico argentino y los principios bioéticos ofrecen una protección adecuada de los derechos fundamentales de las personas en entornos de salud digital.

II. MARCO NORMATIVO Y BIOÉTICO DE LOS DATOS EN SALUD

II.1. Salud digital: definición y alcance

La Organización Mundial de la Salud (OMS) define la salud digital como "el campo del conocimiento y la práctica asociado con el desarrollo y uso de las tecnologías digitales para mejorar la salud"[1]. Este concepto incluye, entre otros:

-Telemedicina y teleconsulta: atención médica a distancia mediante videollamadas u otros canales digitales.

-Historia clínica electrónica (HCE): registro digital de la información sanitaria del paciente, accesible de forma interoperable por diferentes actores autorizados.

-*Wearables* y dispositivos médicos conectados: relojes inteligentes, sensores y otros aparatos que registran parámetros fisiológicos en tiempo real.

-Aplicaciones móviles de salud (*mHealth*): apps para control de enfermedades crónicas, recordatorio de medicación, monitoreo de actividad física, etc.

-*Big data* y analítica predictiva: uso masivo de datos para identificar patrones y predecir riesgos de enfermedad.

-Inteligencia artificial aplicada a la medicina: algoritmos para diagnóstico, tratamiento personalizado o gestión de recursos hospitalarios.[2]

[1] OMS (2021)
[2] OMS (2021) (2020) (2025)

II.2. Datos personales y datos sensibles en salud

La Ley Nº 25.326 define como datos personales a “cualquier tipo de información referida a personas físicas o de existencia ideal determinadas o determinables”. Dentro de ellos, los datos sensibles son “aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, e información referente a la salud o a la vida sexual”.

En el ámbito sanitario, los datos sensibles incluyen historial clínico, diagnósticos y tratamientos, resultados de laboratorio, información genética y biométrica, registro de uso de medicamentos y datos sobre hábitos de vida que impacten en la salud.

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea, en su artículo 9, prohíbe en principio el tratamiento de datos relativos a la salud salvo excepciones, estableciendo un nivel de protección reforzado.

II.3. Privacidad, confidencialidad y seguridad de la información

Estos tres conceptos, aunque relacionados, no son sinónimos. La privacidad es el derecho del individuo a decidir sobre el acceso y uso de su información personal. Por su parte la confidencialidad es la obligación del profesional o entidad que accede a datos de salud de no divulgarlos sin autorización. La seguridad de la información comprende medidas técnicas y organizativas para evitar accesos no autorizados, pérdidas o alteraciones de datos.

En el contexto de la protección de datos personales en la salud digital, un estudio relevante aborda el conocimiento de los profesionales médicos sobre la confidencialidad en la era de las nuevas tecnologías. Esta investigación titulada "Confidencialidad médica en la era digital: análisis de la relación médico-paciente",[3] realizada por Gabriela Kato Lettieri, Aline Hung Tai y Raquel Barbosa Cintra, entre otros, tuvo como objetivo analizar la confidencialidad en la relación médico-paciente, específicamente abordando la influencia de tecnologías emergentes como las redes sociales en el ejercicio de la profesión. También buscó medir el conocimiento de los profesionales sobre situaciones en las que la confidencialidad podría romperse sin consecuencias legales.

Para ello, se llevó a cabo una investigación exploratoria, cuantitativa y transversal, aplicada a 116 médicos entre octubre y noviembre de 2019. A los participantes se les administró un cuestionario estructurado de 19 preguntas, de las cuales cinco estaban diseñadas para evaluar su conocimiento sobre el secreto profesional, de acuerdo con el Código de Ética Médica y el sistema legal brasileño.

Los hallazgos revelaron una brecha significativa en la comprensión de los profesionales: apenas el 55,2% de los médicos encuestados demostró tener un conocimiento satisfactorio sobre el uso de las redes sociales y la confidencialidad médica. Este porcentaje indica que casi la mitad de los profesionales evaluados

[3] LETTIERI Y OTROS (2021)

poseía un conocimiento insatisfactorio en un área crítica para la protección de la privacidad del paciente en el entorno digital.

En este sentido, los resultados del estudio refuerzan la importancia crítica de la educación médica continua, especialmente en lo que respecta a la confidencialidad médica.

Es fundamental que los profesionales de la salud no solo adopten nuevas tecnologías, sino que también estén plenamente informados sobre las implicaciones éticas y legales de su uso, asegurando que la protección de los datos personales y la privacidad del paciente sigan siendo una prioridad indiscutible en la práctica de la salud digital[4].

II.4. Principios bioéticos aplicados a la gestión de datos

La bioética, en su formulación clásica[5], establece cuatro principios fundamentales en la gestión de datos: a) autonomía**:** respeto por la capacidad de las personas de tomar decisiones informadas sobre su propia salud y datos; b) beneficencia: obligación de actuar en beneficio del paciente, maximizando los resultados positivos; c) No maleficencia: evitar causar daño, lo que incluye prevenir filtraciones o usos indebidos de datos; d) Justicia: distribución equitativa de beneficios y riesgos, incluyendo el acceso igualitario a tecnologías y protecciones.

II.5. Legislación nacional vigente

El marco jurídico argentino que regula la protección de datos personales en salud se articula principalmente a través de dos leyes:

a) Ley Nº 25.326 de Protección de Datos Personales: Promulgada en el año 2000, esta norma establece los principios generales sobre recolección, almacenamiento y tratamiento de datos personales. Entre sus puntos más relevantes para la salud digital destacan:

-Consentimiento informado**:** todo tratamiento de datos personales requiere la autorización explícita del titular, salvo excepciones expresamente previstas.

-Finalidad específica**:** los datos solo pueden ser utilizados para el propósito declarado y no para fines secundarios sin autorización adicional.

-Acceso y rectificación**:** los titulares tienen derecho a acceder, corregir o actualizar su información personal.

-Seguridad de la información**:** obligación de garantizar medidas técnicas y organizativas que eviten accesos no autorizados o pérdidas de datos.

Sin embargo, la ley no contempla expresamente escenarios de IA médica**,** plataformas globales de *e-health* ni el análisis masivo de datos para investigación predictiva, lo que deja un vacío frente a la realidad tecnológica actual[6].

[4] LETTIERI Y OTROS (2021)
[5] BEAUCHAMP y CHILDRESS (2001)
[6] ARGENTINA, Ley Nº 25.326

b) Ley Nº 26.529 de Derechos del Paciente: Sancionada en 2009, esta norma regula la relación médico–paciente y establece derechos fundamentales, incluyendo:

-Confidencialidad de la información médica.

-Consentimiento previo, libre e informado para cualquier procedimiento clínico, extendido también a la recopilación de datos de salud.

-Acceso a la historia clínica y documentación sanitaria[7].

Al igual que la Ley N° 25.326, la Ley N° 26.529 fue concebida antes del auge de la telemedicina masiva y de la digitalización integral de la información médica, generando la necesidad de interpretación y adecuación a nuevos contextos.

II.6. Jurisprudencia relevante

El amparo de datos personales del 12 de junio de 2022 ante la Cámara Nacional en lo Contencioso Administrativo Federal constituye un ejemplo paradigmático. En este caso se discutió la utilización de bases de datos de pacientes por empresas privadas para fines comerciales sin consentimiento explícito. El fallo reafirmó el principio de autodeterminación informativa y la obligación de obtener consentimiento válido incluso en entornos digitales, aplicando los estándares de la Ley 25.326.[8]

Otros fallos recientes en Latinoamérica, como el caso I.V. vs. Bolivia (CIDH, 2016), han reforzado la noción de que la protección de datos de salud es un derecho humano fundamental, cuya vulneración puede generar responsabilidad internacional[9].

II.7. Derecho comparado

En el derecho comparado podemos destacar los siguientes:

a) Unión Europea – GDPR: El Reglamento General de Protección de Datos (UE 2016/679) establece estándares modernos que podrían inspirar reformas en Argentina:

-Datos sensibles: tratamiento prohibido salvo consentimiento explícito o situaciones de interés público.

-Portabilidad: el titular puede solicitar la transferencia de sus datos a otro proveedor.

-Minimización de datos: solo se deben recolectar los datos estrictamente necesarios.

-Responsabilidad proactiva: los responsables del tratamiento deben demostrar cumplimiento constante y auditorías periódicas.

[7] ARGENTINA, Ley N° 26.529

[8] CÁMARA NACIONAL EN LO CONTENCIOSO ADMINISTRATIVO FEDERAL, 12/06/2022, amparo de datos personales.

[9] CIDH, Caso I.V. vs. Bolivia, Sentencia del 30/11/2016, Serie C No. 329

b) Estados Unidos – HIPAA: La Health Insurance Portability and Accountability Act (1996) protege la información sanitaria y establece reglas estrictas de confidencialidad y seguridad, aunque no reconoce un derecho general a la autodeterminación informativa comparable al GDPR.

c) Brasil – LGPD: La Ley General de Protección de Datos (Ley N° 13.709/2018) se asemeja al GDPR e introduce consentimiento explícito y revocable, derechos de acceso, corrección, eliminación y portabilidad y obligación de notificar violaciones de datos sensibles en tiempo limitado.

Estas comparaciones muestran que Argentina podría fortalecer su marco legal incorporando principios de responsabilidad proactiva, portabilidad y minimización de datos**.**

III. INTELIGENCIA ARTIFICIAL Y *BIG DATA* EN SALUD

III.1. Aplicaciones y riesgos. Bioética y algoritmos médicos

La inteligencia artificial permite diagnósticos más rápidos y precisos, modelos predictivos de enfermedades crónicas y optimización de recursos hospitalarios. Pero también plantea opacidad algorítmica, donde los profesionales no comprenden cómo se generan las decisiones, sesgos en datos históricos que reproducen discriminaciones existentes y riesgos de privacidad al integrar datos de múltiples fuentes para entrenamiento de algoritmos. Aplicar los principios bioéticos a la IA implica: a) autonomía para garantizar que las decisiones asistidas por IA respeten la voluntad del paciente; b) beneficencia para evaluar riesgos y beneficios antes de implementar sistemas; c) Justicia para asegurar que los algoritmos no generen discriminación ni exclusión.

Por un lado, como ya mencionamos, la GDPR impone reglas estrictas sobre toma de decisiones automatizada y perfilado; y por otro la OMS insta a crear guías de gobernanza ética, seguridad y equidad en el uso de IA en salud.

La ciberseguridad en el ámbito de la salud digital es un componente crítico para garantizar la protección de los datos personales y la confianza de los pacientes. A medida que la información médica se digitaliza y se comparte en plataformas interoperables, aumenta la exposición a ataques informáticos**,** filtraciones y uso indebido de la información.

Entre las amenazas más relevantes en salud digital se encuentran:

-*Ransomware*: ataques que bloquean el acceso a datos clínicos hasta que se paga un rescate. Casos recientes han afectado hospitales en Europa y América Latina, interrumpiendo la atención médica.

-*Phishing* y fraude electrónico: suplantación de identidad para obtener credenciales de profesionales de la salud y acceso a bases de datos sensibles.

-*Exfiltración de datos****:*** robo de información médica por actores maliciosos con fines comerciales o de espionaje.

-*Fugas accidentales*: errores humanos o fallas en la configuración de sistemas en la nube que permiten la exposición de datos.

Los sistemas de salud digital deben implementar medidas técnicas y organizativas basadas en estándares internacionales en ciberseguridad:

-Confidencialidad: garantizar que solo personal autorizado acceda a los datos.

-Integridad**:** asegurar que los datos no sean alterados de forma no autorizada.

-Disponibilidad: mantener acceso seguro y continuo a la información para la atención clínica.

-Trazabilidad**:** registrar accesos y modificaciones para auditoría y control.

Las normas ISO/IEC 27001 y guías de la OMS sobre ciberseguridad en salud proporcionan un marco de referencia para la protección de datos y la resiliencia de los sistemas frente a incidentes.

Por su parte la ciberprotección en inteligencia artificial introduce riesgos adicionales como ser:

-Manipulación de algoritmos: ataques que alteran la salida de sistemas diagnósticos.

-Entrenamiento con datos sesgados o inseguros**:** que pueden derivar en decisiones clínicas erróneas o discriminatorias.

-Exposición masiva de datos para *machine learning*: vulnera el principio de minimización de datos y aumenta la posibilidad de reidentificación.

Para mitigar estos riesgos, se recomienda implementar **a**uditorías periódicas de algoritmos y *datasets;* modelos de IA explicable (XAI) que permitan verificar cómo se generan las decisiones; **p**rotocolos de anonimización robusta y revisión ética antes de compartir información para investigación.

III.2. Gobernanza y protocolos de seguridad

La protección de datos en salud digital requiere un enfoque integral que combine marcos legales, políticas institucionales y capacitación del personal sanitario tales como políticas claras de acceso y manejo de datos, procedimientos de notificación de incidentes y violaciones de seguridad, formación continua en alfabetización digital para profesionales de la salud y monitoreo constante de la infraestructura tecnológica y actualización de sistemas.

La integración de estas medidas fortalece la confianza de los pacientes, requisito indispensable para el éxito de cualquier sistema de salud digital.

IV. PROPUESTAS DE REFORMA Y POLÍTICAS PÚBLICAS

A partir del análisis jurídico, bioético y tecnológico, se plantean reformas concretas para mejorar la protección de datos en salud digital en Argentina y alinearla con estándares internacionales, y destacamos:

1. Reforma legislativa:

-Incorporar principios de responsabilidad proactiva como el GDPR que los responsables del tratamiento deben demostrar cumplimiento continuo.

-Establecer normas específicas para IA en salud, incluyendo transparencia, auditoría y revisión ética de algoritmos, reforzar los derechos de los titulares, incluyendo **portabilidad de datos** y mecanismos claros de revocación del consentimiento.

-Regular la **interoperabilidad transfronteriza de datos**, garantizando residencia de información sensible en servidores seguros y bajo supervisión nacional.

2. Fortalecimiento institucional:

-Creación de un organismo especializado en vigilancia y fiscalización de datos de salud digital.

-Capacitación de jueces y funcionarios en tecnologías de IA, *big data* y seguridad digital aplicada a la salud.

-Promoción de protocolos estandarizados de ciberseguridad en hospitales públicos y privados.

3. Educación y alfabetización digital:

-Programas de alfabetización digital para pacientes, especialmente adultos mayores y comunidades vulnerables, para comprender riesgos y derechos.

-Formación en ética, privacidad y seguridad digital para personal sanitario, desarrolladores de aplicaciones y empresas de tecnología en salud.

4. Gobernanza ética de la inteligencia artificial:

-Establecer comités de ética en IA que supervisen la implementación de algoritmos médicos.

-Evaluar impactos sobre equidad, autonomía y privacidad antes de la implementación de nuevas tecnologías.

-Fomentar auditorías independientes de sistemas de IA para asegurar transparencia y mitigación de sesgos.

5. Incentivos para innovación responsable:

-Programas de financiamiento y certificación para empresas y *startups* que cumplan estándares de privacidad y seguridad.

-Reconocimiento público de buenas prácticas en salud digital mediante sellos de calidad y transparencia.

V. CONCLUSIONES Y RECOMENDACIONES FINALES

El desarrollo de la salud digital ofrece oportunidades sin precedentes para mejorar la atención médica, optimizar recursos y promover el bienestar de la

población. Sin embargo, su implementación plantea desafíos jurídicos, bioéticos y tecnológicos que requieren un enfoque integral:

La protección de datos sensibles debe ser prioritaria, garantizando la privacidad, autonomía y confidencialidad de los pacientes.

Las leyes argentinas actuales, aunque constituyen una base sólida, requieren actualización para integrar principios de responsabilidad proactiva, portabilidad, minimización de datos y regulación específica de IA.

La bioética ofrece un marco indispensable para equilibrar innovación tecnológica y derechos fundamentales.

La ciberseguridad y la gobernanza ética de algoritmos son componentes esenciales de la salud digital confiable.

Por último, las políticas públicas deben incluir educación digital, fortalecimiento institucional y mecanismos de auditoría y transparencia.

La convergencia entre derecho, tecnología y bioética es indispensable para que la digitalización de la salud no se traduzca en vulneración de derechos, sino en un avance seguro, equitativo y sostenible para toda la sociedad.

VI. BIBLIOGRAFÍA CITADA

BEAUCHAMP, Tom L. y CHILDRESS, James F. (2001): Principios de Ética Biomédica (Oxford, University Press)

CÁRCOVA, Carlos María (2020*): Bioética y Derecho: Perspectivas desde América Latina* (Buenos Aires: Eudeba).

LETTIERI, Gabriela K. y otros (2021): "Confidencialidad médica en la era digital: análisis de la relación médico-paciente", *Revista Bioética*, 29(4).

ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) (2021). *Global strategy on digital health 2020–2025*.Disponible en: https://www.who.int/publications/i/item/9789240020924

SÁNCHEZ DÍAZ, M. F. (2023): "El derecho a la protección de datos personales en la era digital", *Revista Eurolatinoamericana de Derecho Administrativo*, *10*(1), e235.

VII. LEGISLACIÓN CITADA

Ley Nº 25.326 de Protección de Datos Personales.

Ley Nº 26.529 de Derechos del Paciente.

Unión Europea (UE). *Reglamento (UE) 2016/679 (GDPR)*.

VIII. JURISPRUDENCIA CITADA

Cámara Nacional en lo Contencioso Administrativo Federal. *Amparo de datos personales* (12/06/2021).

Comisión Interamericana de Derechos Humanos (CIDH). (2016). *Caso I.V. vs. Bolivia*. *Fondo, Reparaciones y Costas, Serie C No. 329*.