Gac Méd Caracas 2026;134(1):343-353
DOI: 10.47307/GMC.2026.134.1.29

Intrusismo digital médico: conceptualización, clasificación y perspectivas bioéticas y pedagógicas

Digital medical intrusion: conceptualization, classification and bioethical and pedagogical perspectives

Freddy Antonio Bello Rodríguez[1], Jeiv Vicente Gómez Marín[2], Carlos Ramón Cabrera Lozada[3]

RESUMEN

El presente trabajo aborda por primera vez el concepto de intrusismo digital médico entendido como la práctica de emitir diagnósticos, tratamientos o consejos de salud en entornos digitales sin acreditación profesional. Mediante una metodología cualitativa inductiva, epistemológica y heurística, se analizan ejemplos nacionales e internacionales, se propone una clasificación del fenómeno y se discuten sus implicaciones filosóficas, bioéticas y pedagógicas. Se concluye que el intrusismo digital médico constituye un riesgo emergente para la confianza en la medicina y la seguridad de los pacientes, y se plantean recomendaciones para su regulación y prevención.

Palabras clave: *Intrusismo digital médico, bioética, epistemología, pedagogía, regulación profesional.*

SUMMARY

This paper introduces the concept of digital medical intrusion, defined as the unauthorized practice of providing medical diagnoses, treatment, or health advice in digital environments. Using an inductive qualitative, epistemological, and heuristic methodology, international and national examples are analyzed, a classification of the phenomenon is proposed, and its philosophical, bioethical, and pedagogical implications are discussed. The study concludes that digital medical intrusion poses an emerging risk to trust in medicine and patient safety and offers recommendations for regulation and prevention.

Keywords: *Digital medical intrusion, bioethics, epistemology, pedagogy, professional regulation.*

DOI: https://doi.org/10.47307/GMC.2026.134.1.29

ORCID: 0000-0001-8196-7579[1]
ORCID: 0000-0003-4833-5160[2]
ORCID: 0000-0002-3133-5183[3]

[1]Médico especialista en obstetricia y ginecología, bioestadística y bioética. Presidente Comité de Bioética del Hospital Universitario "Dr. Jesús María Casal Ramos".
[2]PhD en Ciencias de la Salud, MSc. en bioética, especialista en obstetricia y ginecología, medicina materno-fetal. Coordinador de investigación del programa de especialización en medicina materno-fetal. Universidad Central de Venezuela.
[3]PhD en Ciencias de la Salud, MSc. en bioética, especialista en obstetricia y ginecología, y en medicina materno-fetal. Director fundador emérito del programa de especialización en medicina materno-fetal. Universidad Central de Venezuela. Individuo de Número de la Academia Nacional de Medicina. Sillón VII.

Autor de correspondencia: Carlos Ramón Cabrera Lozada.
E-mail: carloscabreralozada@gmail.com

Recibido: 1 de febrero 2026
Aceptado: 21 de febrero 2026

INTRODUCCIÓN

Recientemente emerge la noción de que el ser humano posee una quinta dimensión, la digital, además de las cuatro convencionalmente descritas: biológica, psicológica-mental, social y espiritual. Si bien dentro de la concepción contemporánea de la sociedad del conocimiento y la información, los conceptos de libertad y ciudadanía digital emergen con fuerza, así como la aparición del *homo digitalis* dentro de las generaciones de nativos digitales (*millennials*, *centennials* y más recientemente la generación *alpha*), el juicio crítico reflexivo de la información a la que se es expuesto digitalmente, permanece como elemento clave, al punto que se establece como gran diferenciador del alfabetismo funcional en el siglo XXI. Dichas consideraciones ya han sido objeto de debate en el campo de la bioética a nivel global y en la región de América Latina y el Caribe (1-3).

El intrusismo médico ha sido tradicionalmente entendido como la práctica de ejercer la medicina sin título o acreditación, lo que constituye una amenaza directa para la seguridad de los pacientes, la legitimidad y la confianza en la profesión (4). No obstante, la transformación digital de la salud, expresada en la expansión de la telemedicina, el auge de las redes sociales, la proliferación de las plataformas educativas y el desarrollo de aplicaciones móviles, ha configurado un nuevo escenario que exige atención: el intrusismo digital médico.

Este fenómeno se manifiesta en la creciente presencia de "*influencers*", "creadores de contenido" o "referentes en redes sociales" de salud que difunden consejos terapéuticos sin respaldo científico, o con niveles precarios de evidencia científica que respalden sus afirmaciones, en páginas web que ofrecen información médica sin regulación y en aplicaciones que generan diagnósticos automatizados sin supervisión profesional. Tales prácticas, aunque aparentemente accesibles y democratizadoras, introducen riesgos epistemológicos, bioéticos y pedagógicos al difuminar las fronteras entre el conocimiento validado y la opinión no cualificada, con repercusiones éticas y legales (1-4).

La ausencia de un marco conceptual y regulatorio específico para abordar el intrusismo digital médico plantea la necesidad de un análisis profundo que articule las dimensiones filosóficas, bioéticas y pedagógicas. Solo a través de esta reflexión crítica será posible comprender la magnitud del desafío y proponer soluciones que fortalezcan la confianza en la medicina, protejan la dignidad de los pacientes y orienten la práctica profesional en entornos digitales (1-5).

METODOLOGÍA

Con base en lo anteriormente mencionado, y con la finalidad de realizar la presente revisión narrativa cualitativa-inductiva sobre el intrusismo digital médico, partiendo de casos concretos de desinformación y de prácticas digitales en salud para construir categorías analíticas emergentes, por otra parte, se examinó el modo en que se valida y legitima el conocimiento médico en entornos digitales, considerando la tensión entre el saber científico, la opinión pública y los discursos no acreditados. Se aplicó un enfoque heurístico para explorar nuevas formas de clasificación y conceptualización del intrusismo digital médico, lo que favoreció la generación de modelos interpretativos abiertos y flexibles. Se realizó una búsqueda en los motores de búsqueda de las plataformas en línea y/o bases de datos PubMed, SciELO, LILACS, Google Scholar, SaberUCV y ResearchGate entre junio 2025 y enero 2026, mediante un muestreo no probabilístico, opinático y de representatividad cualitativa a juicio de los autores, de los documentos y publicaciones en revistas biomédicas y/o libros de autores nacionales e internacionales en bioética, epistemología y pedagogía médica, relacionados con el intrusismo y/o redes digitales. Los términos utilizados fueron: "Intrusismo Digital Médico", "Bioética", "Epistemología", "Pedagogía" y "Regulación Profesional".

DESARROLLO

El ***intrusismo digital médico*** puede definirse como la apropiación indebida de funciones, discursos y prácticas propias de la medicina en entornos digitales por actores sin acreditación profesional ni respaldo institucional, que se manifiesta en la emisión de información,

diagnósticos, tratamientos o procesos formativos en salud a través de plataformas tecnológicas, redes sociales y aplicaciones. Este fenómeno no solo implica la sustitución ilegítima del saber médico, sino también la distorsión epidemiológica del conocimiento científico, la vulneración bioética de la relación médico-paciente y la desorientación pedagógica de las comunidades que buscan información confiable. Aunque el término aún no ha sido definido en la literatura académica, existen aproximaciones conceptuales que permiten fundamentarlo (4,5).

Fitzgerald (5) ha señalado la necesidad de delimitar la autoridad médica en contextos digitales, advirtiendo sobre la proliferación de discursos pseudocientíficos en plataformas abiertas. Roland (6) ha analizado la fragilidad de la validación clínica en entornos virtuales, destacando cómo la ausencia de filtros institucionales facilita la difusión de prácticas no acreditadas. Por su parte, Fisher (7) ha estudiado la intersección entre la salud mental, la desinformación y la cultura digital, mostrando cómo la medicalización informal en redes sociales puede acarrear riesgos éticos y clínicos.

En el ámbito latinoamericano, Kottow (8) ha insistido en que la bioética debe adaptarse a los nuevos escenarios de la comunicación digital, mientras que Delgado (9) ha advertido sobre la responsabilidad ética del médico frente a la información pública en Venezuela. Estas perspectivas permiten sostener que el intrusismo digital médico no es solo una extensión del intrusismo profesional tradicional, sino también un fenómeno emergente que exige una conceptualización propia, una clasificación sistemática y una regulación específica.

Clasificación del intrusismo digital médico

Basado en la experiencia de los autores, se clasificó el intrusismo digital médico en las siguientes categorías:

Intrusismo informativo: difusión de datos médicos sin soporte científico ni validación académica. Ejemplo: blogs o páginas que promueven remedios caseros como sustitutos de tratamientos clínicos.

Intrusismo terapéutico: recomendaciones de tratamientos, fármacos o procedimientos sin aval clínico ni supervisión profesional. Ejemplo: *influencers* que sugieren el uso de antibióticos o suplementos sin evidencia científica.

Intrusismo pedagógico: formación en salud impartida por personas o instituciones no acreditadas, que generan contenidos educativos sin respaldo académico. Ejemplo: cursos en línea de "medicina natural" sin certificación oficial.

Intrusismo institucional: plataformas digitales que simulan servicios médicos sin regulación y ofrecen consultas, diagnósticos o tratamientos sin cumplir con los estándares legales. Ejemplo: páginas web que ofrecen "**consultas médicas**" automatizadas sin supervisión profesional.

Intrusismo telemático: uso indebido de la telemedicina, definida como la prestación de servicios de salud (diagnóstico, tratamiento, seguimiento) a distancia mediante tecnologías de la información y la comunicación (TIC), como videoconferencias, aplicaciones y dispositivos conectados, por parte de actores no acreditados, que aprovechan la infraestructura digital para ejercer funciones médicas sin título, acreditación ni autorización. Este tipo de intrusismo es riesgoso porque se presenta bajo la apariencia de legitimidad tecnológica. Ejemplos: plataformas de video/llamadas que ofrecen consultas médicas sin certificación, o aplicaciones que permiten prescribir medicamentos sin control institucional.

Existen muchos ejemplos públicos, notorios al respecto, como los que se resumen a continuación (7,8,10,11):

1. Campañas antivacunas en redes sociales con precario o nulo nivel de evidencia respaldando sus afirmaciones (Estados Unidos de América y Europa) (11-17)

- Está comprobado que los *influencers* de la aplicación digital Instagram® de Meta, en Estados Unidos de América, crearon y difundieron desinformación antivacunas con fines de lucro, aprovechando la confianza de sus seguidores (11).
- El movimiento antivacunas digital se intensificó durante la pandemia de COVID-19, con campañas organizadas en las

aplicaciones digitales de Facebook® de Meta y X (previamente Twitter®, perteneciente a X Corp.), incluso vinculadas a actores estatales rusos.

2. Aplicaciones móviles con diagnósticos sin supervisión médica (16-18):

- Se ha comprobado que las aplicaciones digitales de salud basadas en inteligencia artificial (IA) ofrecen diagnósticos inseguros y sesgados, con riesgo de retrasar los tratamientos.
- La proliferación de más de 350 000 aplicaciones de salud en tiendas digitales carece de regulación y de una evaluación clínica rigurosa.

2. Difusión de tratamientos no comprobados durante la pandemia por la enfermedad por coronavirus 2019 (COVID-19) (18,19):

- En Venezuela y en la región de América Latina y el Caribe, se difundieron terapias no comprobadas en plataformas de redes sociales y mensajería (aplicaciones digitales de WhatsApp® y Telegram®), como supuestos antivirales o remedios caseros.
- Estudios sociológicos muestran cómo las representaciones sociales en redes influyeron en la aceptación de tratamientos; sin evidencia científica de peso y aceptada por las sociedades científicas y entes reguladores nacionales e internacionales, que los respaldara (19).

4. *Influencers* locales que recomiendan terapias alternativas sin evidencia científica (20-23):

- En Venezuela, *influencers* en las plataformas de las aplicaciones digitales de Instagram® y TikTok® (perteneciente actualmente a TikTok USDS y previamente a ByteDance) promueven terapias alternativas y productos naturales sin respaldo científico.
- El fenómeno de los **"*eco-influencers*"** en TikTok muestra que más del 60 % de los videos analizados contenían información médica contradictoria, especialmente en pediatría y vacunación.

Desde el punto de vista filosófico, el intrusismo digital médico plantea una profunda cuestión sobre la autoridad epistemológica de la medicina en la era digital. Tradicionalmente, el conocimiento médico se ha validado en instituciones académicas y clínicas, mediante protocolos rigurosos de investigación práctica. Sin embargo, la irrupción de plataformas como Instagram®, TikTok® y Telegram® ha generado un espacio en el que discursos no acreditados compiten con el saber científico.

Illich (10) ya advertía que la medicalización excesiva podía derivar en una "expropiación de la salud" por parte de instituciones, pero hoy el riesgo se amplía: actores sin formación médica reclaman autoridad en entornos digitales. Floridi (24) sostiene que la ética de la información exige distinguir entre datos, conocimiento y sabiduría, lo cual se ve debilitado cuando *influencers* difunden consejos médicos sin validación.

En el plano filosófico, el intrusismo digital cuestiona la noción de la verdad médica. O'Neill (25) subraya que la confianza en la comunicación científica depende de la transparencia y la responsabilidad, valores que se diluyen en las redes sociales, donde prima la popularidad por encima de la evidencia. En Venezuela, Delgado (9) ha señalado que la ética médica debe defender la legitimidad del conocimiento frente a discursos públicos no regulados.

Así, el fenómeno obliga a repensar la epistemología médica: ¿Quién tiene derecho a hablar en nombre de la medicina en entornos digitales? La respuesta exige un marco filosófico que reconozca la pluralidad de las voces, pero que preserve la autoridad científica como garante de la salud pública.

Desde la perspectiva bioética, el intrusismo digital médico representa un riesgo directo para la seguridad de los pacientes. La difusión de tratamientos no comprobados durante la pandemia de COVID-19 en Venezuela y en la región de América Latina y el Caribe evidenció cómo la desinformación puede causar daños reales. La Organización Mundial de la Salud (OMS) (12) ha definido la "infodemia" como un exceso de información, cierta o falsa, que dificulta la toma de decisiones en materia de salud.

Kotow (8) sostiene que la bioética latinoamericana debe adaptarse a los nuevos

escenarios digitales, donde la vulnerabilidad del paciente se agrava debido a la falta de filtros institucionales. Fisher (7), al estudiar la relación entre salud mental y cultura digital, advierte que la medicalización informal en redes sociales puede generar dependencia, confusión e incluso causar daños irreparables físicos y mentales e incluso la muerte.

El principio bioético de no maleficencia se ve comprometido cuando *influencers* recomiendan fármacos sin evidencia científica o cuando aplicaciones digitales disponibles en teléfonos móviles inteligentes (smartphones) ofrecen diagnósticos, consejos o tratamientos médicos automatizados sin supervisión profesional, lo que puede retrasar una atención médica más eficiente. En palabras de Burki (13), *"la desinformación en línea se convierte en un vector de daño tan real como una práctica negligente"*.

En Venezuela, Sánchez y Naime (19) documentaron cómo las representaciones sociales en redes sociales durante la pandemia legitimaron terapias sin evidencia, lo que muestra la necesidad de marcos y auditorías bioéticas que regulen la comunicación digital en salud. La bioética, por tanto, debe ampliarse a la esfera digital, garantizando que la información médica en redes sociales respete la dignidad y la seguridad de los pacientes.

A su vez, el intrusismo digital en el ámbito médico plantea un desafío pedagógico. La alfabetización digital en salud, o pedagogía comunitaria digital, se convierte en una necesidad tanto para pacientes como para profesionales. Roldan (14) advierte que la validación clínica en entornos virtuales requiere nuevas competencias pedagógicas, pues los usuarios deben aprender a distinguir entre fuentes confiables y discursos pseudocientíficos.

En el ámbito internacional, estudios sobre TikTok® han mostrado que más del 60 % de los contenidos sobre pediatría contienen información contradictoria (16) e incluso no verificable. Esto evidencia la urgencia de implementar programas educativos que enseñen a los pacientes a evaluar críticamente la información digital. En Venezuela, Delgado (9) ha subrayado que la ética médica incluye la responsabilidad pedagógica de orientar a la sociedad ante la desinformación.

La enseñanza médica debe incorporar herramientas digitales, no solo para transmitir conocimiento, sino también para informar a los "**ciudadanos críticos**" capaces de identificar el intrusismo digital. Floridi (24) propone que la educación en salud digital debe integrar la ética de la información, mientras que Kottow (8) insiste en que la bioética pedagógica debe ser inclusiva y multicultural.

En este sentido, la alfabetización digital no es un lujo sino una estrategia de defensa frente al intrusismo. La pedagogía debe empoderar a pacientes y profesionales para que reconozcan la diferencia entre la información médica validada y los discursos ilegítimos. Solo así se podrá construir un entorno digital que fortalezca la confianza en la medicina y reduzca los riesgos asociados al intrusismo.

Es imposible desligar de la reflexión crítica la consideración al valorar la utilización del término "intrusismo digital médico" en sentido jurídico-profesional del mismo, pudiera tener otras acepciones más relacionadas con el marco penal venezolano tales como "ejercicio ilegal de la medicina en entornos digitales", "práctica sanitaria no acreditada en línea" o "desinformación clínica con ejercicio de funciones", evitando un uso incorrecto del término en lo jurídico-profesional y estableciendo con claridad el límite entre opinión/divulgación en entornos digitales y ejercicio profesional médico en entornos digitales, y por ende, que pudiera generar responsabilidad jurídica y susceptibilidad a sanciones, en cuanto a lo jurídico o regulatorio.

Un uso responsable del concepto de intrusismo médico digital, evitando la confusión entre las consideraciones bioéticas y aquellas relacionadas con el bioderecho, resulta útil para el diseño de respuestas regulatorias y pedagógicas tanto para lo gremial-administrativo en las profesiones relacionadas con las ciencias de la salud y la vida, como para la sociedad en general. El análisis crítico reflexivo del intrusismo médico digital debe realizarse de forma interdisciplinaria, con aportes informativos de cada área de conocimiento sobre el fenómeno y su impacto social, así como con respuestas que produzcan cambios o mejoras, incluida la alfabetización digital. Entre las disciplinas que debieran estar involucradas en el discurso transdisciplinario sobre el tema, deben

prevalecer aquellas relacionadas con la medicina clínica, epidemiología, bioética, bioderecho, ciencias de la comunicación y la computación, psicología y ciencias del comportamiento, educación y pedagogía, y políticas públicas.

En una era digital, con la irrupción de la IA, que ha revolucionado la sociedad del conocimiento y la información, y en la que se requieren estándares probatorios que no siempre están previstos en las leyes (lo que genera brechas), ocurre que los "influencers" (titulados como profesionales de la salud y no titulados) aprovechan la situación para promover "pseudociencia", "pseudoterapias" o información no basada en la evidencia. El discurso transdisciplinario sobre intrusismo médico digital amerita ser preciso entre lo que puede considerarse opinión/divulgación y lo que puede considerarse ejercicio profesional médico, en el sentido jurídico-profesional del término. Para ser tipificado como delito, debe demostrarse que se trata de un acto propio de los profesionales de la medicina con potencial de ocasionar daño. De otra forma, si bien no calificarían de intrusismo, constituyen una serie de conductas que pueden causar daño a los ciudadanos o a la salud pública.

Respecto al marco regulatorio venezolano incluyendo las penas establecidas en caso de transgresión de la normativa (26-32), el intrusismo digital médico vulnera la Constitución de la República Bolivariana de Venezuela (26), en su artículo 58, que se refiere al derecho a recibir información veraz y oportuna y el artículo 60, referente al derecho a la honra, vida privada e intimidad, incluyendo la inviolabilidad de las comunicaciones digitales cuando se difunde información falsa o diagnósticos sin acreditación.

En las consideraciones penales del intrusismo médico digital, es obligatorio considerar que el Código Penal venezolano (27), en su artículo 213, tipifica el delito de usurpación de funciones, estableciendo que las personas que indebidamente asuman o ejerzan funciones públicas civiles o militares serán castigadas con prisión de dos a seis meses. De igual forma, en su artículo 214, se tipifica el delito de usurpación de títulos u honores, estableciendo que las personas que hagan uso indebido de uniformes, insignias o hábitos (militares, clericales, cargos públicos) o se atribuyan grados académicos/títulos profesionales sin poseerlos, conllevan multa de 50 a 1 000 unidades tributarias. Si bien no se tipifica como delito el intrusismo médico digital, las acciones relacionadas con el intrusismo médico, como la apropiación indebida de funciones, discursos y prácticas propias de la medicina en entornos digitales por actores sin acreditación profesional ni respaldo institucional, pueden ser susceptibles de responsabilidad jurídica según lo dispuesto en los artículos 213 y 214 del Código Penal.

Este ejercicio ilegal, incluso en la modalidad digital, constituye un delito previsto en la Ley de Ejercicio de la Medicina (28), que establece que solo los médicos titulados y colegiados pueden ejercer actos médicos. El Código de Deontología Médica (29) vigente define el intrusismo como una incursión ilegítima en el ejercicio médico y obliga a los profesionales a denunciar estas prácticas no acreditadas, incluidas las digitales.

Por su parte, el Ministerio del Poder Popular para Ciencia y Tecnología (30) establece el imperativo ético de respetar los principios de responsabilidad, transparencia/explicabilidad y derecho a la intimidad y protección de datos, entre otros, tanto en el marco jurídico nacional como internacional, de manera tal que regula el uso de las tecnologías digitales o TIC y la práctica profesional. En función de lo cual fue recientemente establecido por dicho ministerio, el Código de Ética para el desarrollo y la aplicación responsable de la inteligencia artificial (IA) (30). La IA puede emplearse de forma irresponsable al incurrir en intrusismo médico digital, ya sea de forma directa o indirecta.

La Ley Especial contra los Delitos Informáticos (31), tipifica 21 delitos informáticos en 5 categorías distintas, a saber: delitos contra los sistemas que utilizan TIC (acceso indebido, sabotaje o daño a sistemas, favorecimiento culposo del sabotaje o daño, acceso indebido o sabotaje a sistemas protegidos, posesión de equipos o prestación de servicios de sabotaje, espionaje informático, falsificación de documentos) delitos contra la propiedad (hurto, fraude, obtención indebida de bienes y servicios, manejo fraudulento de tarjetas inteligentes o instrumentos análogos, apropiación de tarjetas inteligentes o instrumentos análogos, provisión indebida de bienes o servicios, posesión de equipo

para falsificaciones) delitos contra la privacidad de las personas y las comunicaciones (violación de la privacidad de la data o información de carácter personal, violación de la privacidad de las comunicaciones, revelación indebida de data o información de carácter personal) delitos contra los niños, niñas o adolescentes (difusión o exhibición de material pornográfico, exhibición pornográfica de niños o adolescentes) delitos contra el orden económico (apropiación intelectual, oferta engañosa). Las acciones relacionadas con intrusismo médico digital, si bien *per se* no están tipificadas como delito en dicha ley, potencialmente son susceptibles de responsabilidad jurídica por alguno de los 21 delitos mencionados previamente (31).

Si bien las TIC representan herramientas para el desarrollo de las sociedades, también pueden utilizarse para incurrir en una diversidad de actividades delictivas que ocasionan efectos adversos en todos los ámbitos de la sociedad, las instituciones, las operaciones y los sistemas de información, entre las cuales estarían incluidas las acciones relacionadas con el intrusismo médico digital. En Venezuela se estableció el Consejo Nacional de Ciberseguridad en el año 2024, como órgano asesor y de consulta en materia de prevención de los usos delictivos de las TIC (32).

Otras leyes que regulan el medio digital son la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (33), en la cual la difusión de diagnósticos falsos o tratamientos sin evidencia en redes sociales puede ser sancionada por constituir información engañosa que afecta la salud colectiva; en sus artículos 27 y 29, que regulan la difusión de contenidos en medios electrónicos estableciendo que la información debe ser oportuna, veraz y responsable; y el artículo 34, que prohíbe la difusión de mensajes que promuevan las prácticas contra la salud pública.

La Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (34), en sus artículos 4 y 6, establece la responsabilidad penal por el uso de medios digitales para actividades ilícitas. El artículo 8 tipifica delitos relacionados con la manipulación de la información digital que puedan poner en riesgo la seguridad ciudadana. Aunque su foco es el crimen organizado y el terrorismo, se puede aplicar, dado que la desinformación masiva en salud genera riesgos colectivos, como ocurrió con la difusión de tratamientos falsos durante la pandemia de COVID-19.

A nivel internacional, la regulación legal depende de la Constitución y de los códigos de procedimiento de cada nación. Sin embargo, existen normas que deben ser consideradas y tomadas en cuenta, como la Estrategia Global de Salud (2020-2025) publicada por la Organización Mundial de la Salud (OMS) en el 2021 (35); las normas de Protección de datos personales en servicios digitales de salud de la Unión Europea (GDPR) (36); y las normas de Privacidad y Seguridad de la información médica digital de Estados Unidos de América (HIPAA) (37). En conjunto, estas guías establecen principios universales: protección de datos, seguridad digital, consentimiento informado, equidad en el acceso y responsabilidad institucional. Estas referencias internacionales ofrecen un piso común para garantizar la confianza en la salud digital y enfrentar el intrusismo digital.

En síntesis, enfrentar el intrusismo digital médico demanda un esfuerzo interdisciplinario que articule bioética, filosofía y pedagogía y esté acompañado de políticas públicas y marcos regulatorios específicos. Solo así será posible proteger la integridad del conocimiento médico, fortalecer la confianza social en la medicina y asegurar que la digitalización de la salud se convierta en una oportunidad de inclusión y progreso, y no en un espacio de vulnerabilidad y riesgo.

El marco regulatorio venezolano e internacional en materia de intrusismo digital médico presenta avances importantes, contenidos en: la Ley de Ejercicio de Medicina, Código de Deontología Médica, la Constitución Nacional y el Código Penal en Venezuela, sin menoscabo de lo contenido en otras leyes como la Ley Especial contra los Delitos Informáticos, la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo, así como las guías de la OMS; GDPR en Europa y la HIPAA en los Estados Unidos de América, pero aún mantiene vacíos significativos frente a la práctica médica digital contemporánea (26-29,31-37).

La acelerada expansión de la telemedicina y las aplicaciones móviles han generado escenarios que no están plenamente contemplados en las normativas vigentes, amén del profundo impacto que ha provocado la IA en la sociedad de la información y el conocimiento, que incluso ha originado recomendaciones éticas por parte de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO por sus siglas en inglés) (38), la repercusión de las recomendaciones éticas de la UNESCO con las connotaciones nacionales propias, ha llevado a realizar el Código de Ética para el desarrollo y aplicación responsable de la inteligencia artificial (30), resaltando como principios éticos el humanismo, equidad-igualdad-no discriminación, responsabilidad ambiental, seguridad, privacidad, transparencia, rendición de cuentas, ciencia abierta y excelencia. Dichos principios no solo deben aplicarse al desarrollo y uso responsable de la IA, sino también al uso de las TIC en general y a que la opinión/divulgación en entornos digitales no incurra en intrusismo de la práctica profesional de la medicina en entornos digitales. Dicho enfoque garantiza que la información en salud difundida en entornos digitales respete la dignidad y la seguridad de los pacientes.

El intrusismo médico digital pone en riesgo la seguridad de los pacientes, la credibilidad de la profesión médica y la protección fundamental de la intimidad y del acceso a la información veraz. Por ello, se impone la necesidad de una revisión y actualización integrales del marco legal y regulatorio, que articule los principios constitucionales, penales y éticos con las nuevas realidades digitales; esta actualización debe garantizar que la digitalización de la medicina se convierta en un espacio de confianza, seguridad y progreso, y no en un terreno fértil para el intrusismo y la desinformación.

Partiendo de la revisión narrativa de la literatura realizada, *a priori* es recomendable ejecutar las siguientes acciones:

1. Creación de protocolos de certificación digital para profesionales de la salud: las universidades, facultades de medicina y Colegios/Federaciones médicas deben abocarse al diseño curricular de programas de certificación digital que garanticen que los médicos certificados en telemedicina y plataformas digitales cumplan con los estándares éticos y clínicos. Los colegios y las federaciones médicas deben validar y supervisar estos protocolos para asegurar su legitimidad profesional.
2. Promoción de la alfabetización digital en pacientes y comunidades: las universidades (a través de programas de extensión), las sociedades científicas y el Ministerio del Poder Popular para la Salud deben orientar la alfabetización digital en salud como política pública, pero también como tarea pedagógica de las universidades y las sociedades científicas, que pueden generar campañas educativas, realizar talleres comunitarios y distribuir materiales accesibles para pacientes y familias.
3. Establecimiento de observatorios bioéticos sobre prácticas médicas en redes sociales. Es perentorio que las Academias de Medicina, los Comités de Bioética nacionales y regionales y las Sociedades Científicas monitoreen la circulación de información médica en redes sociales (Instagram®, TikTok®, Facebook®, X®, Telegram®, etc.), identifiquen los casos de intrusismo digital y emitan alertas éticas. La Academia de la Medicina puede liderar este esfuerzo con el apoyo de sociedades científicas especializadas.
4. Incentivar la producción académica local sobre el tema corresponde a las universidades, a la Academia de la Medicina, al Centro Nacional de Bioética y a las comisiones nacionales ministeriales en bioética, como un elemento clave para combatir el intrusismo digital médico desde una perspectiva contextualizada. Las universidades deben fomentar la investigación sobre el tema, mientras que las academias y centros de investigación deben promover publicaciones y actividades divulgativas al respecto.
5. Conformación de una mesa nacional e internacional de revisión normativa integrada por universidades y facultades de medicina, Academia Nacional de la Medicina, sociedades científicas, colegios de médicos y Federación Médica Venezolana, Ministerio del Poder Popular para la Salud y el Ministerio del Poder Popular para Ciencia y Tecnología,

órganos legislativos y judiciales, organismos internacionales como la OMS, la Organización Panamericana de la Salud y el Banco Interamericano de Desarrollo con el objeto de realizar la actualización normativa que incluya: protocolos claros para la telemedicina y la medicina digital; regulación del uso de redes sociales y aplicaciones móviles en salud; garantía de protección de datos, intimidad y derecho a la información veraz y mecanismo de denuncia y sanción del intrusismo digital médico.

6. Promoción del abordaje del intrusismo médico digital como un tema que amerita un discurso transdisciplinario de profesionales de las ciencias de la salud y la vida, con la presencia de disciplinas como la medicina clínica, la epidemiología, la bioética, el bioderecho, las ciencias de la comunicación y la computación, la psicología y las ciencias del comportamiento, la educación y la pedagogía, y las políticas públicas.
7. Delimitación precisa del término "intrusismo digital médico" en su sentido jurídico-profesional, así como considerar el uso de otras acepciones más relacionadas con el marco jurídico venezolano, tales como "ejercicio ilegal de la medicina en entornos digitales", "práctica sanitaria no acreditada en línea" o "desinformación clínica con ejercicio de funciones".

CONCLUSIONES

El intrusismo digital médico constituye un fenómeno emergente que, aunque carece de una definición formal en la literatura académica, se manifiesta con creciente intensidad en plataformas digitales y redes sociales. Su presencia desafía la autoridad epistemológica de la medicina, debilita la confianza pública y expone a los pacientes a riesgos de desinformación, daño terapéutico y pérdida de credibilidad institucional.

La necesidad de conceptualizar y clasificar este fenómeno es urgente, pues solo a través de categorías claras y marcos analíticos rigurosos será posible reconocer sus múltiples formas: informativa, terapéutica, pedagógica, institucional y telemática. Esta clasificación no solo permite comprender la magnitud del problema, sino también orientar estrategias de regulación y prevención.

Desde la perspectiva bioética, el intrusismo digital médico exige la aplicación de principios de responsabilidad, transparencia y no maleficencia, garantizando que la información en salud difundida en entornos digitales respete la dignidad y la seguridad de los pacientes. En el plano pedagógico, se requiere una alfabetización digital en salud que capacite tanto a los profesionales como a las comunidades para discernir entre conocimiento validado y discursos ilegítimos.

REFERENCIAS

1. Gómez J, Cabrera Lozada C. Bioética en salud pública: propuesta de la digievolución. Gac Méd Caracas. 2023;131(2):434-438.
2. Gómez Marín J, Robayo Y, Cabrera C. Aspectos bioéticos del uso de redes sociales en obstetricia y ginecología. Rev Obstet Ginecol Venez. 2023;83(4):485-500.
3. Gómez J, Cabrera-Lozada C, Cabrera-Figallo C, Robayo Y, Faneite P. Bioética latinoamericana en salud pública. En: Nézer de Landaeta I, Sorgi-Venturoni M, editores. Colección Razetti. Volumen XXVII. Caracas: Editorial Ateproca; 2023.p.139-177.
4. Bello Rodríguez FA. Intrusismo médico y ejercicio ilegal de la medicina. Rev Obstet Ginecol Venez. 2022;82(4):478-486.
5, Fitzgerald J. Autoridad digital en la práctica médica. New York: Routledge; 2018.
6. Roland S. Validación clínica en entornos virtuales. London. Springer; 2020.
7. Fisher CE. El impulso: nuestra historia de la adicción. New York: Penguin Press; 2021.
8. Kottow M. Bioética: una disciplina necesaria. Santiago: Editorial Universitaria; 2005.
9. Delgado C. Ética médica en Venezuela. Caracas: Academia Nacional de Medicina; 2010.
10. Illichs I. Nemesis Médica: la expropiación de la salud. Londres, Reino Unido: Calder & Boyars; 1975.
11. Rendón EB, Coyago Loaiza XS. El marketing de influencia: La evolución y la responsabilidad de los influencers en la era digital. Cienc Latin. 2025;9(3):6631-47.
12. Organización Mundial de la Salud. Gestión de la infodemia: una guía práctica de salud. Geneva: WHO.

2022. Disponible en: https://www.who.int/health-topics/infodemic.

13. Burki T. El movimiento antivacunas en la era del COVID-19. Lancet Digital Health 2020;2(10):e504-e505.
14. Roldán J, Sánchez-Torres J. Marketing de influencers en redes sociales. FACE. 2021;2(2):46–67.
15. Jamison AM, Broniatowski DA, Quinn SC. Malicious Actors on Twitter: A Guide for Public Health Researchers. Am J Public Health. 2019;109(5):688-692.
16. Zawati MH, Lang M. Does an App a Day Keep the Doctor Away? AI Symptom Checker Applications, Entrenched Bias, and Professional Responsibility. J Med Internet Res. 2024;26(1):e50344.
17. Organización Panamericana de la Salud, Organización Mundial de la Salud. La inteligencia artificial en la salud pública. Washington (DC): PAHO. 2021. Disponible en: https://iris.paho.org/handle/10665.2/53887.
18. Mescher T, Hacker RL, Martinez La, Morris CD, Mishkind M, Garver-Apgar CE. Mobile Health Apps: Guidance for Evaluation and Implementation by Healthcare Workers. J Technol Behav Sci. 2025;10(1):224-235.
19. Sánchez B, Naime M. Venezuela en tiempos de pandemia de COVID-19: representaciones sociales y estrategia de mitigación multinivel. Espacio Abierto. 2022;31(4):45-68.
20. Roussiau N, Valence A. Interdependencia y transformación de las representaciones sociales en redes. Rev CES Psicol. 2013;6(I):60-76.
21. Centro Internacional de Políticas para el Crecimiento Inclusivo, Fondo de las Naciones Unidas para la Infancia, Programa Mundial de Alimentos. Protección social y migración venezolana en América Latina y el Caribe en el contexto de la COVID-19. Research Report Nº 58. Brasília, Brasil: UNICEF. 2021. Disponible en: https://www.unicef.org/lac/media/22526/file/Proteccion-social-y-la-migracion-venezolana-OP.pdf
22. Canas-Galvis M. The Rise of "Eco-Influencers" and Misinformation on Child Health. Abstract. Proceedings of the AAP National Conference. 2025:26-30; Denver (CO). Itasca (IL): AAP. 2025. Disponible en: https://medicalxpress.com/news/2025-09-majority-eco-tiktoks-contradictory-medical.html.
23. Cachero-Martínez S. Influencers en Instagram: nuevas formas de conectar con los consumidores. En: Trespalacios-Gutiérrez JA, Estrada-Alonso E, González-Mieres C, editores. Innovación y estrategias en el comercio y en los servicios en general: de lo físico a lo digital. Oviedo, España: Cátedra Fundación Ramón Areces de Distribución Comercial. 2021. Disponible en: https://www.catedrafundacionarecesdcuniovi.es/fotos/si237dhfnc/CFRA-innovacionyestrategias.pdf.
24. Floridi L. La ética de la información. Oxford: Oxford University Press. 2013. Disponible en: https://www.researchgate.net/publication/50223435_Etica_de_la_informacion_su_naturaleza_y_alcance.
25. López-Jara CA, Holguín-Lew JC. Autonomía, confianza y ética médica en la obra de Onora O'Neill. Rev Colomb Psiquiatr. 2013;42(1):120-135.
26. Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Nº 36860 (30 de diciembre de 1999). Caracas: Asamblea Nacional de Venezuela. 1999. Disponible en: https://www.asambleanacional.gob.ve/storage/documentos/botones/constitucion-nacional-20191205135853.PDF.
27. Ley de Reforma Parcial del Código Penal. Gaceta Oficial Nº 5.768 Extraordinario (13 de abril de 2005). Caracas: Asamblea Nacional de Venezuela. 2005. Disponible en: https://www.refworld.org/es/leg/legis/pleg/2005/es/125865.
28. Ley de ejercicio de la Medicina. Gaceta Oficial Nº 41.984 (13 de octubre de 2020). Caracas: Asamblea Nacional de Venezuela. 2020. Disponible en: https://www.ghm.com.ve/wp-content/uploads/2020/12/41984.pdf.
29. Código de Deontología Médica. LXXVI Reunión Extraordinaria de la Asamblea de la Federación Médica Venezolana (20 de marzo de 1985). Caracas: Academia Nacional de Medicina. 2026. Disponible en: https://academianacionaldemedicina.org/publicaciones/libros/codigo-de-deontologia-medica-venezolano/.
30. Código de Ética para el desarrollo y aplicación responsable de la inteligencia artificial. Publicado por el Ministerio del Poder Popular para Ciencia y Tecnología (19 de febrero de 2026). Caracas: MPPCYT. 2026. Disponible en: https://mincyt.gob.ve/wp-content/uploads/2026/02/Codigo_de_Etica_de_Inteligencia_Artificial_de_la_Republica_Bolivariana-1.pdf.
31. Ley Especial contra los Delitos Informáticos. Gaceta Oficial N° 37.313 (30 de octubre de 2001). Caracas: Asamblea Nacional de Venezuela. 2026. Disponible en: https://www.asambleanacional.gob.ve/storage/documentos/leyes/ley-especi-20220309131245.pdf.
32. Creación del Consejo Nacional de Ciberseguridad. Decreto N° 4.975. Gaceta Oficial N° 42.939 (12 de agosto de 2024). Caracas: Gaceta Oficial de la República Bolivariana de Venezuela. 2026. Disponible en: https://assets.kpmg.com/content/dam/kpmg/ve/pdf/2024/08/gaceta-oficial-42939.pdf
33. Reforma de la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos. Gaceta Oficial Nº 39.610 (07 de febrero de 2011). Caracas: Asamblea Nacional. 2016. Disponible en: https://pandectasdigital.blogspot.com/2016/10/ley-de-reforma-de-la-ley-de.html.
34. Ley Orgánica contra la Delincuencia Organizada y el Financiamiento al Terrorismo. Gaceta Oficial Nº

39.912 (30 de abril de 2012). Caracas: Asamblea Nacional. 2026. Disponible en: https://www.asambleanacional.gob.ve/leyes/sancionadas/ley-organica-contra-la-delincuencia-organizada-y-financiamiento-al-terrorismo.

35. Organización Mundial de la Salud. Estrategia Global y Salud Digital 2020-2025. Ginebra, Suiza: WHO. 2021. Disponible en: https://www.who.int/es/publications/i/item/9789240020924.
36. Unión Europea. Reglamento General de Protección de Datos (GDPR). Bruselas, Bélgica: EU. 2016. Disponible en: https://www.privacy-regulation.eu/es/35.htm.
37. Congreso de los Estados Unidos. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Washington (DC): CDC. 1996. en: https://www.cdc.gov/phlp/ php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html.
38. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Recomendación de la UNESCO sobre la ética de la inteligencia artificial. París, Francia: UNESCO. 2022. Disponible en: https://unesdoc.unesco.org/ ark:/48223/pf0000381137_spa.