

Aspectos bioéticos da telemedicina no Brasil: análise abrangente

Juracy Barbosa dos Santos¹, Guilhermina Rego¹, Rui Nunes¹

1. Faculdade de Medicina da Universidade do Porto, Porto, Portugal.

Resumo

A telemedicina tem ganhado destaque no Brasil, especialmente em contextos de pandemia e áreas remotas. Este artigo explora os aspectos bioéticos e legais dessa prática, especialmente a necessidade de diretrizes claras para garantir uma prática ética e segura. Trata-se de revisão de literatura focada em publicações relevantes sobre ética, bioética, tecnologias da informação e comunicação, proteção de dados e responsabilidades legais associadas à telemedicina. Foram identificados e analisados diversos desafios e benefícios da telemedicina, com ênfase em questões éticas, proteção de dados e responsabilidades legais. A legislação brasileira foi comparada com regulamentações internacionais. Os resultados reforçam que a consolidação da telemedicina como prática segura e socialmente legítima depende da integração entre regulamentação, princípios bioéticos e compromisso ético permanente com os direitos e o bem-estar dos pacientes.

Palavras-chave: Telemedicina. Bioética. Segurança computacional. Ética médica. Legislação. Brasil.

Resumen

Aspectos bioéticos de la telemedicina en Brasil: análisis integral

La telemedicina ha ganado protagonismo en Brasil, especialmente en contextos de pandemia y en áreas remotas. Este artículo explora los aspectos bioéticos y legales de esta práctica, destacando la necesidad de directrices claras para garantizar una práctica ética y segura. Se trata de una revisión de la literatura centrada en publicaciones relevantes sobre ética, bioética, tecnologías de la información y la comunicación, protección de datos y responsabilidades legales asociadas a la telemedicina. Se identificaron y analizaron diversos desafíos y beneficios de la telemedicina, con énfasis en cuestiones éticas, protección de datos y responsabilidades legales. La legislación brasileña fue comparada con regulaciones internacionales. Los resultados refuerzan que la consolidación de la telemedicina como una práctica segura y socialmente legítima depende de la integración entre regulación, principios bioéticos y un compromiso ético permanente con los derechos y el bienestar de los pacientes.

Palabras clave: Telemedicina. Bioética. Seguridad computacional. Ética médica. Legislación. Brasil.

Abstract

Bioethical aspects of telemedicine in Brazil: comprehensive analysis

Telemedicine has gained prominence in Brazil, especially in pandemic contexts and in remote areas. This article explores the bioethical and legal aspects of this practice, emphasizing the need for clear guidelines to ensure ethical and safe practice. This is a literature review focused on relevant publications addressing ethics, bioethics, information and communication technologies, data protection, and legal responsibilities associated with telemedicine. Various challenges and benefits of telemedicine were identified and analyzed, with emphasis on ethical issues, data protection, and legal responsibilities. Brazilian legislation was compared with international regulations. The results reinforce that the consolidation of telemedicine as a safe and socially legitimate practice depends on the integration of regulation, bioethical principles, and a continuous ethical commitment to patients' rights and well-being.

Keywords: Telemedicine. Bioethics. Computer security. Ethics, medical. Legislation. Brazil.

Declararam não haver conflito de interesse.

Telemedicina, definida como o uso de tecnologias de informação e comunicação (TIC) para a prestação de serviços de saúde a distância, tem sido amplamente adotada nos últimos anos como solução inovadora para diversos desafios no setor de saúde. No Brasil, destaca-se como ferramenta essencial para melhorar o acesso a serviços de saúde, especialmente em áreas remotas, e para aumentar a eficiência no atendimento médico. No entanto, essa prática levanta importantes questões éticas que precisam ser cuidadosamente consideradas para garantir que a telemedicina beneficie verdadeiramente os pacientes e respeite os princípios fundamentais da bioética.

A rápida adoção da telemedicina no Brasil trouxe consigo uma série de preocupações bioéticas, relacionadas a privacidade dos dados dos pacientes, qualidade do atendimento médico a distância e equidade no acesso aos serviços de saúde. Autores como Corrêa, Zaganelli e Gonçalves¹ destacam que, apesar dos avanços tecnológicos, é fundamental garantir que a telemedicina não comprometa a qualidade do cuidado médico e que seja utilizada de maneira ética e responsável. O foco da telemedicina deve sempre estar alinhado a princípios bioéticos, priorizando o bem-estar do paciente e a justiça no acesso a serviços de saúde².

Este estudo utiliza uma abordagem bibliográfica exploratória e descritiva para analisar questões bioéticas associadas à telemedicina no Brasil. A pesquisa se baseia em revisão de literatura existente, com o objetivo de fornecer uma visão abrangente sobre os desafios e as melhores práticas para implementação ética da telemedicina, assim como refletir sobre os efeitos das TIC e da globalização na saúde sob uma perspectiva ética, contribuindo para o desenvolvimento de práticas mais seguras e equitativas na telemedicina.

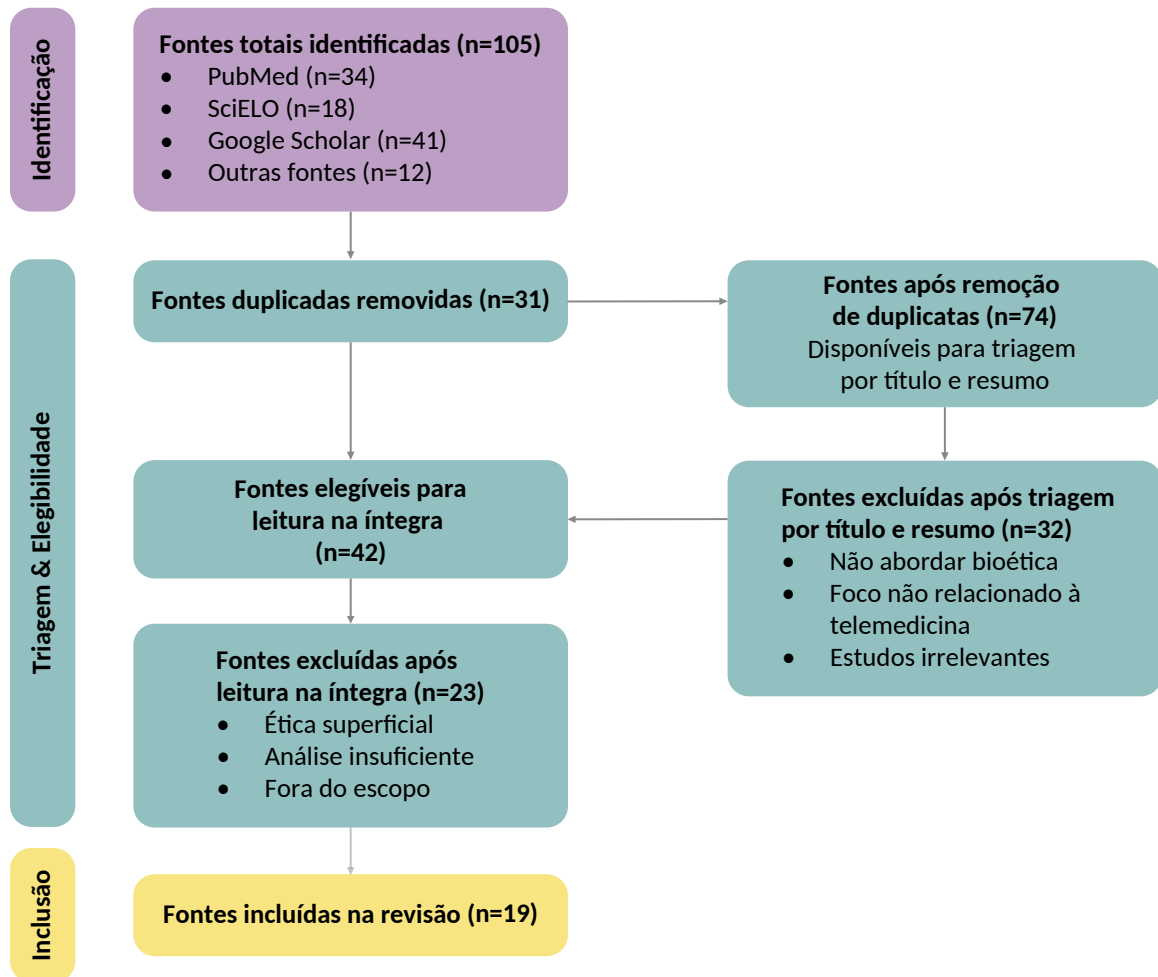
Método

Os procedimentos metodológicos seguiram as diretrizes propostas por Köche³ e por Prodanov e Freitas⁴ para abordagem de revisão bibliográfica de caráter exploratório e descritivo. A condução da revisão seguiu, de forma orientadora e dedutiva, as recomendações do PRISMA 2020⁵, com vistas à transparência e à organização lógica do processo de seleção das fontes, sem pretensão de sistematicidade estrita.

A etapa de identificação resultou em 105 registros, provenientes das bases PubMed, SciELO e Google Scholar, além de outras fontes documentais relevantes, como legislações nacionais e internacionais e documentos normativos institucionais. Após a remoção de duplicatas, 74 registros foram triados por título e resumo, e 32 foram excluídos por não abordarem aspectos éticos ou bioéticos, por apresentarem enfoque exclusivamente técnico ou por não se relacionarem à telemedicina.

Na fase de elegibilidade, 42 documentos foram avaliados na íntegra, dos quais 23 foram excluídos em razão de abordagem ética superficial, ausência de análise bioética estruturada, redundância conceitual ou inadequação ao escopo brasileiro ou comparado internacionalmente. Ao final, 19 estudos compuseram o corpo analítico da revisão, incluindo artigos científicos, legislações, teses, dissertações e documentos institucionais, usualmente disponíveis em diários oficiais e repositórios normativos. A análise e a síntese dos dados foram realizadas de forma crítica e interpretativa, permitindo a construção de uma compreensão sistematizada e fundamentada dos principais aspectos bioéticos que permeiam a telemedicina no contexto brasileiro.

A Figura 1 apresenta o fluxograma do processo de identificação, triagem, elegibilidade e inclusão dos estudos, elaborado conforme as recomendações do PRISMA 2020.

Figura 1. Fluxograma de busca

Discussão

Definição de ética e bioética

Ética é o ramo da filosofia que estuda os valores morais e princípios que regem o comportamento humano em sociedade. Conforme Araújo⁶, trata-se de julgamentos relativos ao bem e ao mal que orientam as condutas humanas, promovendo bem-estar pessoal e social. Envolve reflexões sobre o que é moralmente correto ou incorreto, justo ou injusto, em diferentes contextos.

Já bioética é uma extensão da ética voltada para questões morais ligadas à vida e à saúde. É o estudo das dimensões éticas das ciências da vida, englobando visões, decisões, condutas e políticas nesses campos, buscando guiar práticas que respeitem a dignidade e os direitos humanos⁷.

Na prática médica tradicional, ética e bioética orientam as ações de profissionais de saúde. Ética médica, subcampo da ética profissional, avalia risco, méritos e impactos sociais das atividades médicas, assegurando atuação responsável e respeito aos direitos e à dignidade dos pacientes⁸.

Os princípios éticos fundamentais que guiam a prática médica incluem beneficência, não maleficência, autonomia e justiça. Beneficência exige ações que promovam saúde e bem-estar. Não maleficência visa evitar danos. Autonomia respeita o direito de pacientes a decisões informadas, enquanto justiça demanda equidade na distribuição de recursos e tratamento⁸.

A aplicação desses princípios na prática médica envolve várias responsabilidades. Médicos devem informar claramente os pacientes, assegurar decisões informadas, preservar a confidencialidade e

tratar todos de forma justa, independentemente de fatores pessoais ou socioeconômicos⁸.

A bioética, como disciplina mais ampla, estende esses princípios para incluir preocupações com justiça social e equidade no acesso a cuidados de saúde. Preocupa-se com condições sociais e ambientais que impactam a saúde, defendendo abordagens integradas. Isso inclui avaliar determinantes sociais da saúde e defender políticas que garantam acesso igualitário a serviços para todos⁷.

Ética médica em telemedicina

Os princípios éticos que fundamentam a prática médica tradicional garantem uma relação baseada em confiança, respeito e justiça. A beneficência exige que os médicos priorizem o bem-estar do paciente tratando e prevenindo doenças, assim como oferecendo aconselhamento para melhorar sua qualidade de vida². Complementando a beneficência, a não maleficência impõe que os médicos evitem causar danos avaliando rigorosamente os riscos e benefícios das intervenções, assegurando, assim, que os benefícios superem os riscos².

A autonomia reconhece o direito dos pacientes de decidir sobre seu cuidado. Os médicos devem fornecer informações claras e completas, permitindo escolhas conscientes. O respeito à autonomia é essencial para uma prática ética e humanizada². A justiça exige equidade na distribuição de recursos e igualdade no tratamento dos pacientes, independentemente de fatores socioeconômicos ou pessoais. Essa abordagem promove um acesso justo a cuidados de saúde para todos².

Esses princípios fortalecem a confiança entre médicos e pacientes, essencial para a adesão ao tratamento. A prática médica ética também envolve a manutenção da confidencialidade dos pacientes. Isso significa que todas as informações pessoais e de saúde dos pacientes devem ser mantidas em sigilo, exceto quando o paciente consente com a divulgação ou quando ela for exigida por lei. A confidencialidade é fundamental para a construção da confiança entre médicos e pacientes².

Por fim, a prática ética requer profissionalismo e integridade. Os médicos devem tratar todos com dignidade, comunicar-se com honestidade e evitar discriminações ou preconceitos, promovendo cuidado respeitoso e inclusivo².

Contudo, a telemedicina traz novos desafios éticos, especialmente quanto à confidencialidade dos dados dos pacientes. A transmissão eletrônica aumenta o risco de violações de privacidade, exigindo que as plataformas adotem medidas robustas de segurança para proteger essas informações¹.

O consentimento informado também é um desafio, pois é essencial que pacientes compreendam os riscos e benefícios dos tratamentos, o que pode ser mais difícil virtualmente. Médicos devem explicar detalhadamente os tratamentos e garantir espaço para dúvidas e preocupações⁹.

A relação médico-paciente, fundamental na prática médica, pode ser prejudicada pela mediação tecnológica. A distância dificulta a conexão empática e a confiança, tornando necessário o esforço dos profissionais para manter comunicação clara e humanizada, usando recursos que favoreçam a interação visual e auditiva².

Outro desafio é a equidade no acesso à telemedicina, pois nem todos têm acesso a tecnologias ou internet de qualidade, fato que cria desigualdades. Políticas públicas devem assegurar que todos, independentemente da localização ou condição socioeconômica, possam utilizar esses serviços⁹.

A segurança dos dados permanece prioritária, com plataformas obrigadas a seguir padrões rigorosos como criptografia e autenticação multifator¹. Por fim, a aceitação dos pacientes varia, e médicos devem respeitar suas preferências, assim como oferecer suporte para tornar a telemedicina uma opção viável e confortável⁹.

Para enfrentar os desafios éticos da telemedicina e assegurar a manutenção dos princípios éticos tradicionais, são necessárias diretrizes específicas que orientem a prática médica a distância. Em primeiro lugar, plataformas de telemedicina devem implementar medidas de segurança cibernética avançadas, como usar criptografia, *firewalls* e autenticação multifator, além de auditorias regulares, para garantir a segurança e confidencialidade dos dados dos pacientes, identificando e corrigindo vulnerabilidades¹.

As diretrizes devem garantir acesso equitativo à telemedicina, com atendimento de qualidade a todos, independentemente da localização ou condição socioeconômica, incluindo suporte técnico e equipamentos para quem precisar¹. Consequentemente, a telemedicina deve ser

continuamente monitorada para garantir padrões éticos e qualidade, incluindo revisão de segurança, avaliação da satisfação dos pacientes e análise de resultados, com sistemas de feedback para melhorias constantes².

A adoção de tecnologias avançadas pode ajudar a melhorar a segurança e a eficácia da telemedicina. Isso inclui o uso de inteligência artificial para apoio a diagnóstico, a telemonitorização para acompanhamento contínuo de pacientes e a integração de dispositivos de saúde conectados. As diretrizes devem encorajar a inovação tecnológica, ao mesmo tempo que garantem que essas tecnologias sejam implementadas de maneira ética e segura¹.

Profissionais de saúde também precisam de treinamento contínuo em telemedicina que abranja aspectos técnicos, éticos e comunicacionais, para garantir atendimento ético e de qualidade. Instituições devem oferecer programas regulares de atualização sobre tecnologias e diretrizes². Ademais, devem humanizar o atendimento na telemedicina usando comunicação clara e empática; videochamadas ajudam a manter conexão visual e emocional, aproximando a experiência da presencial⁹.

Transparência é fundamental para a prática ética da telemedicina. Pacientes devem ser informados sobre como seus dados serão utilizados e protegidos, e quaisquer incidentes de segurança devem ser comunicados de maneira clara e oportuna. A comunicação aberta ajuda a construir confiança e assegurar que os pacientes estejam cientes de seus direitos e das medidas de proteção implementadas⁹.

Os pacientes devem ser envolvidos ativamente no desenvolvimento e na implementação de serviços de telemedicina. Isso inclui a consulta sobre suas necessidades e preferências, a inclusão de suas perspectivas no design dos serviços e a provisão de suporte adequado para ajudá-los a utilizar as tecnologias de telemedicina. O envolvimento dos pacientes ajuda a garantir que os serviços sejam acessíveis, compreensíveis e adequados às suas necessidades².

Por sua vez, o consentimento informado deve ser claro, documentado e garantir que pacientes compreendam o tratamento, riscos, direitos e uso dos dados. Médicos devem explicar opções e responder a todas as dúvidas⁹.

Tecnologias da informação e impactos na medicina

A evolução das TIC tem transformado profundamente a medicina, oferecendo novas ferramentas e métodos para diagnosticar, tratar e gerir a saúde. Desde os anos 1960, as TIC avançaram da eficiência administrativa para sistemas de apoio à decisão clínica, registros eletrônicos de saúde e telemedicina⁸.

A digitalização dos registros facilitou o acesso e a troca de informações entre profissionais, melhorando a continuidade e qualidade do cuidado⁷. Sistemas de telemetria e monitoramento remoto permitiram acompanhamento a distância, com intervenções mais rápidas e personalizadas⁷.

A pandemia de covid-19 acelerou o uso das TIC na medicina, mostrando a importância das soluções digitais para manter o atendimento durante o distanciamento social. Consultas e tratamentos remotos reduziram riscos de infecção e garantiram o cuidado necessário⁶.

Entre as principais tecnologias utilizadas na telemedicina estão videoconferências, plataformas digitais e dispositivos móveis. Videoconferências são ferramentas que permitem consultas, diagnósticos e tratamentos a distância em tempo real. Promovem interação visual e auditiva, fundamentais para construir confiança entre médico e paciente¹⁰. Plataformas como Zoom, Microsoft Teams e Google Meet são adaptadas para garantir privacidade e atender às demandas específicas da área de saúde.

Plataformas digitais de saúde oferecem funcionalidades como agendamento, registros eletrônicos, comunicação segura e acesso a informações médicas. Essas ferramentas otimizam a gestão dos cuidados pois facilitam a troca de informações e melhoram a coordenação entre profissionais de saúde⁸.

Já dispositivos como *smartphones* e *tablets* são essenciais na telemedicina, por permitirem que pacientes monitorem sua saúde em tempo real. Aplicativos e dispositivos conectados, como medidores de glicose e monitores de pressão, auxiliam no monitoramento contínuo e na coleta de dados, possibilitando que o acompanhamento médico seja mais preciso e personalizado⁷.

As TIC oferecem diversos benefícios à área médica, como maior acessibilidade a cuidados

de saúde, especialmente para pacientes com mobilidade reduzida ou residentes em áreas remotas. A telemedicina elimina a necessidade de deslocamentos, proporcionando economia de tempo e recursos para pacientes e profissionais¹⁰. Além disso, essas tecnologias facilitam a comunicação entre profissionais de saúde, promovendo cuidado mais integrado e eficiente⁸.

Apesar dos benefícios, as TIC apresentam desafios, como em relação à segurança e privacidade dos dados dos pacientes. A transmissão digital de informações aumenta o risco de ciberataques e violações, comprometendo a confidencialidade⁸. Também há preocupações sobre desigualdades no acesso, já que pacientes sem recursos tecnológicos podem ser excluídos⁶.

A adaptação a tecnologias digitais é outra barreira. Muitos profissionais de saúde não estão familiarizados com essas ferramentas, o que pode afetar a eficácia do atendimento⁷. Consultas remotas, embora úteis, enfrentam limitações, como a impossibilidade de realizar exames físicos, o que pode impactar diagnósticos e tratamentos.

Dados em ambientes virtuais de saúde

A proteção dos dados de saúde dos pacientes é crucial para a confiança no sistema de saúde digital e o cumprimento de regulamentações como a Lei Geral de Proteção de Dados (LGPD), no Brasil, e o Health Insurance Portability and Accountability Act (HIPAA), nos Estados Unidos (EUA)⁸. Para prevenir acessos não autorizados e ciberataques, são indispensáveis medidas como criptografia, autenticação multifator, *firewalls* e monitoramento contínuo¹⁰.

As plataformas de telemedicina devem obedecer rigorosamente às normas legais de segurança e privacidade. Paralelamente, é essencial cultivar uma cultura de segurança entre os profissionais de saúde por meio de treinamentos regulares e conscientização sobre a proteção dos dados⁷. A transparência com pacientes sobre como seus dados serão utilizados e protegidos também é essencial para manter a confiança no sistema de saúde digital.

A responsabilidade pela segurança dos dados deve ser compartilhada entre desenvolvedores de tecnologia, instituições de saúde e médicos, com esforços conjuntos para garantir práticas seguras e eficazes¹.

Aspectos da Lei Geral de Proteção de Dados

A LGPD estabelece um marco legal para o tratamento de dados pessoais no Brasil, aplicando-se tanto a pessoas físicas quanto jurídicas, públicas ou privadas. Na telemedicina, em que dados sensíveis de saúde são tratados, a LGPD desempenha papel essencial, exigindo proteção rigorosa e segurança¹¹.

O tratamento de dados pessoais na telemedicina deve seguir os princípios da LGPD, como finalidade, transparência, segurança e responsabilização (art. 6º)¹¹. Esses princípios guiam práticas éticas e seguras de coleta, armazenamento e uso de dados, promovendo a confiança dos pacientes e a conformidade legal¹. O consentimento informado é central, devendo ser livre, explícito e detalhado, informando a finalidade do uso dos dados, formas de compartilhamento e medidas de segurança (art. 7º)¹¹. Esse processo educa os pacientes sobre seus direitos e a importância da proteção de dados¹.

A LGPD exige proteção adicional para dados sensíveis, como informações de saúde, devido ao risco de discriminação em caso de uso inadequado. O tratamento desses dados é permitido apenas com consentimento explícito ou para proteger a vida ou integridade física do titular ou de terceiros (art. 11º)¹¹.

A transparência é outro princípio-chave da LGPD, que exige que os responsáveis pelo tratamento de dados forneçam informações claras e acessíveis aos titulares dos dados sobre como estes estão sendo utilizados (art. 9º)¹¹. Na telemedicina, isso implica que pacientes sejam informados também sobre os direitos que têm, como o de acesso, retificação, exclusão e portabilidade dos dados. Corrêa, Zaganelli e Gonçalves¹ enfatizam que transparência fortalece a relação de confiança entre pacientes e prestadores de serviços de saúde.

O tratamento de dados pessoais na telemedicina também deve incluir medidas adequadas de segurança para proteger os dados contra acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (art. 46)¹¹. Essas medidas incluem a implementação de controles de acesso, criptografia de dados e a realização de auditorias de segurança regulares. A responsabilidade

é compartilhada entre empresas, profissionais e desenvolvedores de tecnologia¹.

A nomeação de um encarregado pela proteção de dados (*data protection officer*, DPO) é obrigatória, para garantir a conformidade com a LGPD e atender pacientes e organizações quanto a dúvidas e preocupações (art. 41)¹¹.

Por fim, a LGPD prevê penalidades rigorosas para descumprimento, como multas e exclusão de dados (art. 52), incentivando práticas de conformidade e reforçando a confiança pública¹¹. Na telemedicina, aderir à LGPD é vital para evitar sanções e proteger os pacientes.

Segurança da informação em plataformas de telemedicina

A segurança da informação é essencial para proteger os dados de pacientes e garantir a confiabilidade dos serviços de telemedicina. As plataformas devem implementar medidas robustas para prevenir acessos não autorizados, perda, alteração ou divulgação indevida de dados, assegurando a conformidade legal e a confiança dos usuários no sistema².

Criptografia é medida essencial para proteger dados em trânsito e repouso, já que os torna inacessíveis a terceiros sem a chave de descryptografia. Essa prática é fundamental para a proteção de informações sensíveis, como dados de saúde, durante a transmissão e o armazenamento².

Controles de acesso também são indispensáveis, por limitarem o acesso apenas a profissionais autorizados. A autenticação multifator, que combina métodos como senhas e códigos enviados a dispositivos móveis, é crucial para prevenir acessos indevidos e ciberataques, protegendo a integridade dos dados dos pacientes⁹.

Auditorias regulares de segurança identificam e corrigem vulnerabilidades, garantindo conformidade com regulamentações como a LGPD. Essas auditorias mantêm as plataformas atualizadas e eficazes, reforçando a segurança e a confiabilidade dos serviços². Ademais, treinamento contínuo dos profissionais de saúde é vital para promover uma cultura de segurança. Eles devem ser capacitados para reconhecer ameaças e proteger dados, assegurando práticas consistentes com políticas organizacionais e regulamentações⁷.

A gestão de incidentes é outro pilar da segurança. Procedimentos claros para detecção, resposta e recuperação de incidentes minimizam danos e garantem a notificação de violação conforme exigido pela LGPD. Um plano de resposta bem elaborado reforça a confiança dos pacientes².

Políticas de segurança abrangentes devem ser implementadas para regular todas as etapas do tratamento de dados, desde a coleta até a eliminação. Revisões periódicas dessas políticas garantem sua eficácia diante de mudanças nas ameaças ou regulamentações¹.

A colaboração entre desenvolvedores, prestadores de serviços e profissionais médicos é essencial para integrar práticas de segurança em todos os níveis. A proteção de dados é responsabilidade compartilhada que exige o compromisso de todos os envolvidos⁹.

Por fim, transparência com pacientes sobre as medidas de segurança adotadas fortalece a confiança no sistema de telemedicina. Informá-los sobre a proteção de seus dados e direitos é aspecto central para uma prática segura e ética².

Consentimento informado e proteção da privacidade dos pacientes

O consentimento informado é princípio central da LGPD e da ética na telemedicina. Deve ser livre, informado e inequívoco, de modo a permitir que pacientes compreendam como seus dados serão usados, armazenados e compartilhados. A LGPD garante o direito a informações claras sobre o tratamento de dados pessoais (art. 7º, §1º)¹¹, exigindo que pacientes sejam informados sobre a finalidade específica, entidades envolvidas e medidas de segurança adotadas.

Obter consentimento informado é desafiador, mas essencial para educar pacientes sobre seus direitos e a proteção de dados. Profissionais de saúde devem explicar opções de tratamento e riscos, permitindo decisões informadas. Além disso, pacientes podem revogar o consentimento a qualquer momento, sem prejuízo ao atendimento¹.

A privacidade dos pacientes é fundamental na telemedicina. Apenas profissionais autorizados devem acessar os dados, exclusivamente para fins médicos. Qualquer violação de privacidade deve ser tratada com transparência, reforçando a ética e a confiança no sistema⁹. As plataformas

de telemedicina precisam adotar políticas claras de privacidade, detalhando como os dados são protegidos, os direitos dos pacientes e os procedimentos para relatar violações. A transparência fortalece a confiança entre pacientes e prestadores de serviços². Medidas técnicas, como criptografia e controles de acesso rigorosos, são essenciais para proteger dados sensíveis. Essas práticas asseguram que pacientes compartilhem informações com confiança².

Treinamentos regulares sobre consentimento informado e proteção de privacidade são cruciais para profissionais de saúde. A proteção de dados é questão técnica e ética, que exige o comprometimento de toda a equipe⁷.

A gestão eficaz de consentimentos e privacidade inclui um plano de resposta a incidentes, detalhando ações para violações de dados, como notificação imediata a autoridades e pacientes, conforme a LGPD (art. 48)¹¹. A gestão eficaz de incidentes é crucial para manter a confiança dos pacientes e a integridade dos serviços de telemedicina².

A privacidade deve ser priorizada em todas as etapas das plataformas de telemedicina, da concepção à operação. Desenvolvedores, prestadores de serviços e profissionais médicos devem adotar práticas alinhadas às melhores diretrizes internacionais e à LGPD. A proteção da privacidade é responsabilidade compartilhada e essencial para a confiança nos serviços¹.

Teoria do delito e imputação na telemedicina

A teoria do delito na telemedicina aplica princípios do direito penal às práticas médicas digitais. A Lei 14.510/2022¹² e a Resolução do Conselho Federal de Medicina (CFM) 2.314/2022¹³ definem diretrizes para essa prática, incluindo responsabilização penal e civil dos profissionais. A imputação exige verificar conduta delituosa, tipicidade, antijuridicidade e culpabilidade.

A conduta delituosa pode incluir diagnósticos errados, prescrições inadequadas e descumprimento de protocolos. A tipicidade analisa se a conduta se encaixa no tipo penal, como negligência, imperícia e imprudência, puníveis pelo Código Penal brasileiro¹⁴.

A antijuridicidade ocorre quando a conduta é contrária ao direito, sem justificativa legal,

como agir com negligência causando dano. A culpabilidade avalia a capacidade do profissional de entender o caráter ilícito e agir conforme isso, considerando seu preparo em tecnologias digitais e telemedicina.

A imputação objetiva exige que o dano decorra diretamente da ação ou omissão do médico, verificando-se o nexo causal. A Resolução CFM 2.314/2022¹³ exige rigor no cumprimento dos protocolos para garantir segurança e eficácia no atendimento.

A Lei 14.510/2022¹² destaca a responsabilidade dos profissionais na telemedicina, reforçando o consentimento informado e a transparência com os pacientes. Também prevê sanções, incluindo suspensão ou cassação do registro profissional para quem descumprir as normas legais.

Erros médicos na telemedicina podem gerar responsabilidades civil, penal e administrativa. A responsabilidade civil exige indenização por danos causados por negligência, imprudência ou imperícia, com profissionais devendo garantir qualidade e segurança no atendimento remoto, conforme resolução do CFM¹³.

A responsabilidade penal abrange crimes como lesão corporal culposa, homicídio culposo e omissão de socorro, previstos no Código Penal, que requerem comprovação de culpa. A Lei 14.510/2022¹² reforça a necessidade de seguir normas para evitar erros médicos e suas consequências legais.

Na esfera administrativa, conselhos profissionais aplicam sanções como advertências, multas, suspensão e cassação do registro para quem descumprir normas éticas e técnicas da telemedicina, conforme resolução do CFM¹³. O rigor no cumprimento dessas normas é crucial para garantir segurança e eficácia no atendimento remoto.

Profissionais e instituições devem adotar medidas preventivas, como atualização contínua em tecnologias digitais, treinamentos e sistemas de qualidade e segurança, conforme reforçado pelo arcabouço legal^{12,13}, a fim de minimizar os riscos da telemedicina.

Transparência na comunicação com pacientes é essencial. Profissionais devem informar claramente riscos e benefícios do atendimento remoto, assegurando o consentimento informado, conforme Lei 14.510/2022¹² e Resolução CFM 2.314/2022¹³.

A violação do segredo profissional na telemedicina acarreta graves consequências legais, éticas e profissionais para médicos e instituições. O segredo profissional é dever ético e legal que obriga profissionais a manterem sigilo sobre informações confidenciais dos pacientes, conforme enfatizado na resolução do CFM¹³.

Na esfera civil, a violação pode gerar ações indenizatórias por danos morais e materiais, pois pacientes têm direito a reparação por divulgação não autorizada. Profissionais e instituições devem adotar medidas para proteger esses dados, conforme previsto na legislação¹².

Na esfera penal, a violação é crime tipificado no Código Penal (art. 154)¹⁴, com penas de detenção de três meses a um ano ou multa. A Resolução CFM 2.314/2022¹³ determina sanções penais e administrativas para os infratores. Administrativamente, as sanções incluem advertência, censura, suspensão e cassação do registro, ressaltando a necessidade do cumprimento rigoroso dos princípios éticos e legais na telemedicina^{13,14}. Além das sanções, a violação compromete a confiança entre médico e paciente, fundamental para o sucesso terapêutico e a integridade da prática médica, como destacado pelo CFM¹³.

Profissionais e instituições devem implementar medidas rigorosas, como uso de tecnologias seguras, políticas de privacidade e treinamentos regulares, conforme a Lei 14.510/2022¹² e a Resolução CFM 2.314/2022¹³, para evitar violações. A transparência sobre a proteção das informações é vital para a confiança na telemedicina. Pacientes devem ser informados claramente sobre medidas de segurança e seus direitos, garantindo comunicação aberta e proteção da privacidade^{12,13}.

O exercício ilegal da medicina via telemedicina representa risco à saúde pública e segurança dos pacientes. A legislação estabelece diretrizes rigorosas para que apenas profissionais qualificados e registrados possam atuar por meio de tecnologias digitais^{12,13}.

Ocorre exercício ilegal quando pessoa não qualificada ou sem registro realiza consultas, diagnósticos, prescrições ou tratamentos sem autorização. O Código Penal (art. 282)¹⁴ prevê detenção de seis meses a dois anos para esse crime. Profissionais devem estar registrados no CRM de sua jurisdição e cumprir exigências legais e éticas. Instituições

de saúde devem garantir que apenas profissionais qualificados atuem na telemedicina¹³.

As consequências são severas: sanções civis, penais e administrativas. Pacientes podem pedir indenização por danos causados por profissionais ilegais, os quais podem enfrentar prisão. Instituições que permitirem ou facilitarem o exercício ilegal também respondem administrativamente.

As instituições são responsáveis por garantir que suas plataformas sejam usadas só por profissionais qualificados, com verificação constante de registros e medidas de segurança para impedir acessos não autorizados, conforme determina a lei¹².

Regulamentação da telemedicina nos Estados Unidos e na União Europeia

Nos EUA, proteção de dados e telemedicina são reguladas por leis federais e estaduais. A principal legislação federal é o Health Insurance Portability and Accountability Act (HIPAA)¹⁵, promulgado em 1996, que estabelece padrões nacionais para garantir a privacidade e segurança das informações de saúde dos pacientes¹⁵.

O HIPAA exige que entidades cobertas, como planos de saúde, provedores e intermediários de dados, implementem medidas rigorosas, incluindo criptografia, controles de acesso, autenticação multifator e auditorias de segurança. Também garante aos pacientes o direito de acessar e corrigir suas informações¹⁵.

Para a telemedicina, o HIPAA impõe requisitos para proteger dados durante atendimentos a distância, exigindo que as plataformas assegurem a segurança das comunicações eletrônicas e dos dados dos pacientes. A conformidade é obrigatória para todos os provedores que usam tecnologia digital¹⁵.

Além do HIPAA, o Health Information Technology for Economic and Clinical Health Act (HITECH)¹⁶ reforça suas disposições e promove o uso de registros eletrônicos de saúde (*electronic health records*, EHR). O HITECH prevê penalidades severas para violações e exige notificação aos pacientes e ao Departamento de Saúde e Serviços Humanos (HHS) em casos de violações significativas¹⁶.

Já a União Europeia (UE) tem uma abordagem harmonizada para a proteção de dados e a regulamentação da telemedicina, baseada na

General Data Protection Regulation (GDPR)¹⁷, que entrou em vigor em maio de 2018. A GDPR estabelece um conjunto abrangente de normas para a proteção de dados pessoais, aplicáveis a todas as organizações que processam dados de cidadãos da UE, independentemente de onde essas organizações estejam localizadas.

A GDPR exige consentimento informado, transparência e minimização de dados, e garante direitos aos titulares, como acesso, retificação, exclusão e portabilidade. As organizações devem adotar medidas técnicas e organizacionais, como pseudonimização, criptografia, avaliações de impacto e notificação de violações em até 72 horas¹⁷.

Em relação à telemedicina, a GDPR exige que provedores de serviços garantam que as informações de saúde dos pacientes sejam tratadas com a máxima confidencialidade e segurança. Isso inclui a adoção de tecnologias seguras para a transmissão e armazenamento de dados, bem como a implementação de políticas e procedimentos claros para a proteção de dados. A conformidade com o GDPR é essencial para qualquer organização que ofereça serviços de telemedicina a cidadãos da UE¹⁷.

Além da GDPR, a UE tem a *NIS Directive*¹⁸, que estabelece requisitos para a segurança das redes e sistemas de informação, incluindo os sistemas utilizados para a prestação de serviços de saúde. A NIS Directive exige que operadores de serviços essenciais, como hospitais e clínicas, implementem medidas de segurança adequadas e notifiquem as autoridades competentes sobre quaisquer incidentes de segurança que possam ter impacto significativo na prestação dos serviços¹⁸.

A Estratégia Europeia para a Saúde Digital¹⁹ também fornece diretrizes para a promoção da telemedicina e da saúde digital na UE. Essa estratégia visa melhorar a interoperabilidade dos sistemas de saúde, promover a inovação em saúde digital e garantir que os serviços de saúde digitais sejam acessíveis e seguros para todos os cidadãos da UE. A estratégia enfatiza a importância da proteção de dados e da privacidade como fundamentos para a confiança dos cidadãos na saúde digital¹⁹.

Comparativo entre Brasil, Estados Unidos e União Europeia

Ao comparar a legislação brasileira com as regulamentações dos EUA e da UE, observa-se que

todos os três sistemas legais têm como objetivo principal a proteção dos dados pessoais e a segurança na prestação de serviços de saúde digital. No entanto, há diferenças significativas nas abordagens e nos requisitos específicos.

No Brasil, a LGPD estabelece diretrizes abrangentes para a proteção de dados pessoais, aplicáveis a todas as organizações que processam dados de cidadãos brasileiros. A LGPD é similar ao GDPR da UE em termos de rigor e abrangência, exigindo consentimento informado, transparência e implementação de medidas de segurança adequadas. No entanto, a LGPD apresenta peculiaridades, como exigência de DPO e sanções específicas para o descumprimento das normas¹¹.

Nos EUA, a regulamentação é mais fragmentada, com o HIPAA estabelecendo padrões federais para a proteção de dados de saúde, complementado por leis estaduais específicas para a telemedicina. A conformidade com o HIPAA é obrigatória para todos os provedores de serviços de saúde, mas a aplicação e os requisitos específicos podem variar de acordo com o estado. A abordagem dos EUA é mais orientada para a prática e menos centralizada que a abordagem harmonizada da UE^{15,16}.

A União Europeia, por meio da GDPR e da NIS Directive, adota abordagem altamente regulada e harmonizada para a proteção de dados e a segurança da telemedicina. A GDPR impõe requisitos rigorosos para o consentimento, a transparência e a segurança dos dados, aplicáveis a todas as organizações que processam dados de cidadãos da UE. A estratégia da UE para a saúde digital também promove interoperabilidade e inovação, assegurando que os serviços de saúde digitais sejam seguros e acessíveis^{17,18}.

Em conclusão, embora existam diferenças nas abordagens e nos requisitos específicos entre Brasil, EUA e UE, todos os três sistemas legais reconhecem a importância da proteção de dados e da segurança na telemedicina. A conformidade com regulamentações locais é essencial para garantir a confiança dos pacientes e a eficácia dos serviços de saúde digitais. As melhores práticas internacionais podem servir como referência para a melhoria contínua das regulamentações e das práticas de proteção de dados na telemedicina.

Considerações finais

Os resultados desta revisão bibliográfica exploratória e descritiva indicam que a telemedicina, no contexto brasileiro, deve ser analisada para além de seus aspectos técnicos e normativos, exigindo reflexão ética e bioética consistente. A literatura evidencia que a incorporação das TIC na prática médica reconfigura a relação médico-paciente, o cuidado em saúde e a gestão de dados sensíveis, demandando a ressignificação dos princípios bioéticos clássicos.

A proteção de dados pessoais emerge como eixo ético central, diretamente vinculada à dignidade humana e ao princípio da não maleficência. Os estudos analisados indicam que a confidencialidade, no ambiente digital, depende não apenas da conformidade legal, mas do compromisso moral de profissionais e instituições em prevenir riscos e danos decorrentes do uso indevido de informações de

saúde. Nesse sentido, a análise comparativa entre a legislação brasileira e os marcos internacionais revela convergência quanto à centralidade da privacidade, embora destaque que normas, por si só, não asseguram práticas eticamente adequadas.

No que se refere à autonomia, a literatura aponta que o consentimento informado na telemedicina deve ser compreendido como processo contínuo de comunicação ética, abrangendo não apenas aspectos clínicos, mas também riscos tecnológicos e tratamento de dados. A beneficência é associada ao potencial de ampliação do acesso à saúde, enquanto a justiça impõe a necessidade de enfrentar desigualdades digitais que podem comprometer a indicação ética da telemedicina.

Assim, os resultados reforçam que a consolidação da telemedicina como prática segura e socialmente legítima depende da integração entre regulamentação, princípios bioéticos e compromisso ético permanente com os direitos e o bem-estar dos pacientes.

Referências

1. Corrêa JCB, Zaganelli MV, Gonçalves BD. Telemedicina no Brasil: desafios ético-jurídicos em tempos de pandemia da Covid-19. *Humanit Technol (FINOM)* [Internet]. 2020 [acesso 21 maio 2025];25(1):200-18. Disponível: <https://bit.ly/4dHEuLw>
2. Garcia EF, Oliveira SM, Reis JG. Bioética e telemedicina. *Rev Bioética Cremego* [Internet]. 2020 [acesso 10 jun 2025];2(1):61-6. Disponível: <https://bit.ly/48Cxx4r>
3. Köche JC. Fundamentos de metodologia científica. Petrópolis: Vozes; 2015.
4. Prodanov CC, Freitas EC. Metodologia do trabalho científico. 2ª ed. Novo Hamburgo: Feevale; 2013.
5. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* [Internet]. 2021 [acesso 18 maio 2025];372:71. DOI: 10.1136/bmj.n71
6. Araújo RCV. Direito versus bioética em tempos de pandemia: que desafios? *Rev Ang Ciênc Saúde* [Internet]. 2022 [acesso 21 maio 2025];1:1-4. DOI: 10.54283/RACSaude.v3i2edsupl1.2022.p1-4
7. Oliveira EL, Soares A, Lima J, Santos RM. Falhas de comunicação e epistemológicas limitam a abordagem da bioética na formação e na prática em saúde. *Interface (Botucatu)* [Internet]. 2021 [acesso 21 maio 2025];25:e200679. DOI: 10.1590/interface.200679
8. Cohen C, Gobbetti G, Oliveira RA. Breve discurso sobre ética, moral, estética e bioética das relações. *Rev Bras Psicanál* [Internet]. 2021 [acesso 21 maio 2025];55(2):41-57. Disponível: <https://bit.ly/4njFLN1>
9. Sánchez MVC, Costa FG, Bossio P, Fàbrega C, Abejas AG, Vergès AS. Telemedicina y eSalud: reflexiones desde la bioética. Barcelona: Institut Borja de Bioètica; 10 nov 2022. Disponível: <https://bit.ly/4wapuhs>
10. Sganzerla AS, Zanella DC, Paulo Neto A, Good C. A bioética como ética aplicada: a saúde em destaque. *Rev Inst* [Internet]. 2023 [acesso 21 maio 2025];5(2):59-78. Disponível: <https://bit.ly/4cZButq>
11. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União* [Internet]. Brasília, nº 154-A, p. 1, 15 ago 2018 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4w7whs6>

12. Brasil. Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de 1990. Autoriza e disciplina a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. Diário Oficial da União [Internet]. Brasília, nº 244, p. 1, 28 dez 2022 [acesso 21 maio 2025]. Disponível: <https://bit.ly/42eG5mG>
13. Conselho Federal de Medicina. Resolução nº 2.314, de 20 de abril de 2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. Diário Oficial da União [Internet]. Brasília, p. 227, 5 maio 2022 [acesso 21 maio 2025]. Disponível: <https://tinyurl.com/hyrzwr3f>
14. Brasil. Decreto-Lei nº 2 848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União [Internet]. Brasília, p. 23911, 31 dez 1940 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3OJpDI1>
15. United States. Health Insurance Portability and Accountability Act (HIPAA). To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Federal Register [Internet]. Washington, 20 ago 1996 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4w9dEUT>
16. United States. Health Information Technology for Economic and Clinical Health Act (HITECH). Federal Register [Internet]. Washington, v. 74, n. 209, 30 out 2009 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3QQVfMj>
17. European Union. General Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR). Off J Eur Union [Internet]. 2016 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4n6oRBj>
18. European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union. [Internet]. Brussels, 27 abr 2016 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4wbaiRe>
19. eHealth - digital services in health and care [Internet]. Brussels: European Commission; 2025 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3OJpJzn>

Juracy Barbosa dos Santos – Doutorando – drjuracybarbosa@gmail.com

 0009-0009-1729-9778

Guilhermina Rego – Doutora – guilherminarego@med.up.pt

 0000-0002-8590-9832

Rui Nunes – Doutor – ruinunes@med.up.pt

 0000-0002-1377-9899

Correspondência

Juracy Barbosa dos Santos – Faculdade de Medicina da Universidade do Porto. Alameda Prof. Hernâni Monteiro, 4200-319. Porto, Portugal.

Contribuições dos autores

Juracy Barbosa dos Santos foi responsável pela concepção do estudo, análise dos dados e redação do manuscrito. Guilhermina Rego realizou a revisão do manuscrito. Rui Nunes foi responsável pela análise crítica e revisão final do manuscrito.

Disponibilidade de dados: Todos os dados utilizados ou gerados na pesquisa estão integralmente descritos e apresentados no corpo do artigo.

Editora responsável: Dilza Teresinha Ambrós Ribeiro

Recebido: 28.4.2025

Revisado: 5.6.2025

Aprovado: 13.1.2026