

Lílian Natália Ferreira de Lima¹;
Bruno Costa Silva²;
Ivone Pereira da Silva Moura³;
karyne Gleyce Zemf Oliveira⁴;
Janira Martins Silva Sampaio⁵;
Ana Ita Reis Santos⁶;
Nilcelete dos Santos Vieira⁷;
Orquideia Silva Fernandes⁸;
Onayane dos Santos Oliveira⁹.

1.INTRODUÇÃO

A contemporaneidade tem sido marcada por um processo inexorável de digitalização dos sistemas de saúde, catalisado pelo avanço acelerado das tecnologias da informação e comunicação. Essa revolução tecnológica, conhecida como saúde digital, redefine paradigmas tradicionais do cuidado à saúde, promovendo a integração de ferramentas digitais complexas — tais como registros eletrônicos de saúde, inteligência artificial, telemedicina e dispositivos conectados — que ampliam significativamente o potencial diagnóstico, terapêutico e de gestão dos serviços (Santos; Almeida, 2023). No entanto, essa inserção disruptiva da tecnologia no campo da saúde traz à tona uma série de desafios epistemológicos e práticos, sobretudo no que tange à ética e à segurança da informação, que demandam uma reflexão crítica e multidisciplinar para assegurar que os avanços tecnológicos não se sobreponham aos direitos fundamentais dos sujeitos envolvidos.

No âmbito dessa discussão, encontra-se a problemática da proteção de dados sensíveis, cujo manejo inadequado pode ocasionar violação da privacidade, comprometimento da confidencialidade e possíveis danos à dignidade dos pacientes. A operacionalização da saúde digital exige, portanto, a implementação rigorosa de diretrizes éticas que norteiem as práticas clínicas e administrativas, conciliando inovação tecnológica com o respeito à autonomia, à beneficência e à justiça distributiva (Cunha; Mendes; Oliveira, 2021). Ademais, a emergência de novas modalidades de interação entre pacientes, profissionais de saúde e sistemas digitais impõe a necessidade de um arcabouço regulatório robusto, capaz de equilibrar o potencial transformador da tecnologia com a salvaguarda dos direitos humanos e da integridade dos dados pessoais (Mittelstadt, 2019).

A segurança da informação, enquanto componente estrutural da governança em saúde digital, deve abarcar não apenas a proteção contra ameaças cibernéticas, mas também assegurar a conformidade normativa com marcos legais, como a Lei Geral de Proteção de

Dados (LGPD). A efetividade dessas medidas é imprescindível para consolidar a confiança social no ecossistema digital da saúde, assegurando que os benefícios tecnológicos se materializem de forma ética, transparente e equitativa (Ribeiro; Silva; Freitas, 2023).

Diante desse cenário multifacetado, este capítulo propõe-se a aprofundar a análise crítica dos principais dilemas éticos e das exigências de segurança de dados inerentes à saúde digital, destacando as práticas e normativas que podem legitimar o uso responsável e humanizado das tecnologias digitais em saúde.

2.DESENVOLVIMENTO

2.1 Políticas para ética e segurança de dados na saúde digital no SUS

A transformação digital no Sistema Único de Saúde (SUS) tem se consolidado como uma estratégia imprescindível para a melhoria da gestão, do acesso e da qualidade dos serviços de saúde no Brasil. A criação de plataformas digitais integradas, como o Conecte SUS, o Prontuário Eletrônico do Paciente (PEP) e o e-SUS Atenção Básica, promove a centralização de dados clínicos e administrativos, favorecendo a continuidade do cuidado e o planejamento assistencial em âmbito nacional (BRASIL, 2020). Entretanto, essa revolução tecnológica traz consigo a urgente necessidade de assegurar princípios éticos e legais que regem o tratamento dos dados sensíveis, de modo a preservar a privacidade e a segurança dos usuários do SUS.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) estabelece um marco regulatório fundamental, definindo diretrizes rigorosas para a coleta, armazenamento, processamento e compartilhamento dos dados pessoais e sensíveis, entre eles os de saúde. A LGPD impõe o consentimento explícito do titular, transparência na finalidade do uso dos dados, além da responsabilidade e segurança na sua proteção, o que fortalece a confiança dos cidadãos no sistema (Cunha; Mendes; Oliveira, 2021). Ademais, a Resolução nº 466/2012 do Conselho Nacional de Saúde orienta que a pesquisa em saúde deve respeitar a dignidade, a autonomia e o sigilo dos dados dos pacientes, reforçando o compromisso ético do SUS (Brasil, 2012).

Do ponto de vista tecnológico, o SUS investe em sistemas que adotam padrões internacionais de segurança da informação, como criptografia, autenticação multifatorial e protocolos de interoperabilidade HL7 FHIR, para garantir o fluxo seguro e eficaz dos dados entre os diversos níveis de atenção (Santos et al., 2023; Oliveira; Gomes, 2023). A capacitação de profissionais de saúde e gestores é outro vetor crucial, pois a segurança da informação depende tanto da infraestrutura tecnológica quanto da cultura organizacional e da formação ética dos usuários do sistema (Ribeiro; Silva; Freitas, 2023).

Além disso, o SUS tem se empenhado em manter o controle social e a transparência, garantindo que a população possa acompanhar o uso dos seus dados e participar ativamente dos debates sobre as políticas de saúde digital, consolidando assim os princípios

democráticos e participativos que sustentam o sistema (Brasil, 2020).

1.2 Desafios contemporâneos na ética e segurança de dados no SUS

Apesar dos avanços, a implementação plena das políticas de ética e segurança na saúde digital enfrenta desafios complexos no âmbito do SUS. Primeiramente, a heterogeneidade dos sistemas e a fragmentação dos dados dificultam a interoperabilidade plena e segura, expondo vulnerabilidades a ataques cibernéticos e riscos de vazamentos que podem comprometer informações sensíveis (Santos et al., 2023; Oliveira; Gomes, 2023). O aumento exponencial do volume de dados gerados pela expansão da telemedicina, da inteligência artificial e dos dispositivos conectados intensifica ainda mais a complexidade da governança e da proteção desses dados.

Outro desafio relevante reside na escassez de profissionais capacitados para lidar com a gestão ética e técnica dos dados em saúde no contexto público. A insuficiência de treinamentos específicos em segurança da informação, governança de dados e ética digital nas equipes do SUS potencializa o risco de falhas humanas, que frequentemente são a principal causa de incidentes de segurança (Ribeiro; Silva; Freitas, 2023). A resistência cultural à adoção de práticas robustas de proteção, combinada com limitações orçamentárias e infraestrutura desigual, dificulta a implementação de soluções efetivas em todo o território nacional.

Adicionalmente, o dilema ético de equilibrar a utilidade dos dados para pesquisa, vigilância epidemiológica e gestão com a garantia da privacidade individual é objeto de intensos debates. A transparência quanto ao uso dos dados e o consentimento informado são desafios práticos, especialmente para populações vulneráveis ou com menor acesso à informação, o que pode comprometer os direitos fundamentais dos cidadãos e aumentar desigualdades (Cunha; Mendes; Oliveira, 2021; Mendes; Costa, 2022).

A rápida evolução tecnológica demanda atualização constante das normas, políticas e práticas do SUS, o que exige articulação interinstitucional, recursos financeiros e comprometimento político. O avanço na regulação da ética digital, a incorporação de auditorias independentes, e o fortalecimento de órgãos de controle social são imperativos para garantir que a saúde digital no SUS seja segura, ética e inclusiva (Brasil, 2020; Ribeiro; Silva; Freitas, 2023).

2 CONSIDERAÇÕES FINAIS

A incorporação das tecnologias digitais no âmbito do Sistema Único de Saúde representa uma transformação estrutural que pode ampliar significativamente o acesso, a qualidade e a eficiência dos serviços de saúde no Brasil. Contudo, esse avanço tecnológico impõe a necessidade imperiosa de consolidar práticas éticas e robustos mecanismos de segurança da informação para a proteção dos dados pessoais e sensíveis dos usuários.

A consolidação de uma política pública que harmonize inovação, proteção da privacidade e transparência é essencial para garantir a legitimidade e a confiança do SUS perante a sociedade.

Embora o SUS tenha avançado na implementação de instrumentos legais, normativos e tecnológicos, os desafios permanecem complexos e multifacetados, demandando esforços contínuos de capacitação, atualização normativa e articulação intersetorial. O equilíbrio entre o uso responsável dos dados para fins assistenciais, gerenciais e de pesquisa e a salvaguarda dos direitos fundamentais dos cidadãos constitui um imperativo ético e jurídico. Nesse cenário, o fortalecimento da governança em saúde digital e a ampliação do controle social são fundamentais para promover uma saúde pública inclusiva, segura e ética, alinhada às diretrizes da universalidade, integralidade e equidade que norteiam o SUS.

REFERÊNCIAS

CUNHA, C. M.; MENDES, E. V.; OLIVEIRA, R. A. **A LGPD e a proteção de dados no SUS: entre desafios e oportunidades**. Revista Brasileira de Saúde Digital, v. 1, n. 1, p. 45-60, 2021. Disponível em: <https://www.scielo.br/rbrsd/a/56MHDpw9hrMKXYzCWyB77Cp/>. Acesso em: 16 maio 2025.

MITTELSTADT, B. D. **Ethics of artificial intelligence: Mapping the debate**. Big Data & Society, v. 6, n. 2, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2909885. Acesso em: 16 maio 2025.

RIBEIRO, R. S.; SILVA, M. R.; FREITAS, C. A. **Challenges and opportunities in AI application in health data governance**. Health Policy and Technology, v. 12, p. 100618, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2405844024023284>. Acesso em: 16 maio 2025.

BRASIL. Ministério da Saúde. **Portaria nº 1.996, de 17 de agosto de 2020**. Institui a Estratégia e-SUS Atenção Primária à Saúde (e-SUS APS). Diário Oficial da União, Brasília, 2020. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2020/prt1996_17_08_2020.html. Acesso em: 16 maio 2025.

BRASIL. Conselho Nacional de Saúde. **Resolução nº 466, de 12 de dezembro de 2012**. Diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Diário Oficial da União, Brasília, 2012. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/2013/res0466_12_12_2012.html. Acesso em: 16 maio 2025.

MENDES, D. F.; COSTA, E. R. **Aspectos éticos e legais da inteligência artificial na saúde**. Revista de Bioética e Direito em Saúde, v. 8, n. 3, p. 75-88, 2022.

OLIVEIRA, R. S.; GOMES, L. F. **Desafios na adoção dos sistemas de informação em**

saúde no contexto da Atenção Primária no Brasil. Cadernos de Saúde Coletiva, v. 31, n. 1, p. 13–23, 2023.

SANTOS, L. F.; ALMEIDA, C. R. **Tecnologias digitais e transformação da saúde: análise crítica.** Saúde Digital, v. 2, n. 1, p. 12-27, 2023.