ATA DA SESSÃO PÚBLICA DE DEFESA DO TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO EM DIREITO DA UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL, CAMPUS DE TRÊS LAGOAS

Aos 18 dias do mês de novembro de 2025, às 14h00min, na sala de reuniões Google Meet – com link: https://meet.google.com/nsv-scnk-aqr, realizou-se a sessão pública de defesa do Trabalho de Conclusão de Curso de Graduação em Direito, do(a) acadêmico(a)**IASMIN NATÁLIA DIAS CANHETTI**, intitulado: "DIREITOS HUMANOS E SAÚDE DIGITAL: PROTEÇÃO DE DADOS DE SAÚDE", na presença da banca examinadora composta pelos professores: presidente da sessão, Prof. Dr. Michel Ernesto Flumian, primeiro(a) avaliador(a) Profª. Drª. Carolina Ellwanger (Dir-CPTL/UFMS), segunda avaliadora: Profª. Me. Larissa Mascaro Gomes da Silva (Dir-CPTL/UFMS). Após os procedimentos de apresentação, arguição e defesa, o presidente suspendeu a sessão para deliberação. Retomados os trabalhos, foi divulgado o resultado, sendo considerado(a) o(a) acadêmico(a) APROVADA. Terminadas as considerações, o(a) acadêmico(a) foi cientificado(a) sobre os trâmites devidos para o depósito definitivo do trabalho no Sistema Acadêmico (SISCAD). Nada mais havendo a tratar, foi encerrada a sessão, sendo lavrada a presente ata, que segue assinada por todos os membros da banca.

Prof. Dr. Michel Ernesto Flumian

Profª. Drª. Carolina Ellwanger

Profª. Me. Larissa Mascaro Gomes da Silva

Documento assinado eletronicamente por **Michel Ernesto Flumian**, **Professor do Magisterio Superior**, em 18/11/2025, às 14:50, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Larissa Mascaro Gomes da Silva de Castro**, **Professora do Magistério Superior**, em 19/11/2025, às 09:33, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Carolina Ellwanger**, **Professora do Magistério Superior**, em 24/11/2025, às 21:52, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

CÂMPUS DE TRÊS LAGOAS

Av. Ranulpho Marques Leal, 3484

Fone: (67)3509-3700

CEP 79613-000 - Três Lagoas - MS

República Federativa do Brasil
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Termo de Depósito e Composição da Banca Examinadora

Eu, professor **MICHEL ERNESTO FLUMIAN,** orientador da acadêmica **IASMIN NATÁLIA DIAS CANHETTE,** autorizo o depósito do Trabalho de Conclusão de Curso intitulado **"DIREITOS HUMANOS E SAÚDE DIGITAL: PROTEÇÃO DE DADOS DE SAÚDE"**.

Informo, também, a composição da banca examinadora e a data da defesa do TCC:

Presidente: MICHEL ERNESTO FLUMIAN

lº avaliador(a): CAROLINA ELLWANGER

2º avaliador(a): LARISSA MASCARO GOMES DA SILVA

Data: 18 de novembro.

Horário: 14hrs MS.

Três Lagoas/MS, Dia 29 de Outubro de 2025.

Digitally signed by MICHEL ERNESTO FLUMIAN
DN: C=BR, O=ICP-Brasil, OU=AC OAB, OU=43419613000170, OU=Presencial, OU=Assinatura Tipo A3, OU=ADVOGADO, CN=MICHEL ERNESTO FLUMIAN
Reason: I am the author of this document
Location: Três Lagoas/MS
Date: 2025.10.30 11:55:04-04'00'
Foxit PDF Reader Version: 2025.1.0

Assinatura do(a) orientador(a)

Orientações: O acadêmico ou acadêmica deverá preencher e assinar este documento e, após, uni-lo ao TCC e ao Termo Autenticidade em um único arquivo PDF. O acadêmico ou acadêmica deverá, então, proceder ao depósito desse arquivo PDF único, observando a data limite estipulada pelo Colegiado de Curso.

Termo de Autenticidade

Eu, **IASMIN NATÁLIA DIAS CANHETTE**, acadêmico(a) regularmente apto(a) a proceder ao depósito do Trabalho de Conclusão de Curso intitulado **"DIREITOS HUMANOS E SAÚDE DIGITAL: PROTEÇÃO DE DADOS DE SAÚDE"**, declaro, sob as penas da lei e das normas acadêmicas da UFMS, que o Trabalho de Conclusão de Curso ora depositado é de minha autoria e que fui instruído(a) pelo(a) meu(minha) orientador(a) acerca da ilegalidade do plágio, de como não o cometer e das consequências advindas de tal prática, sendo, portanto, de minha inteira e exclusiva responsabilidade, qualquer ato que possa configurar plágio.

Três Lagoas/MS, 29 de Outubro de 2025.

gov.br
Documento assinado digitalmente
IASMIN NATALIA DIAS CANHETTE
Data: 04/12/2025 01:25:06-0300
Verifique em https://validar.iti.gov.br

_____

Assinatura do(a) acadêmico(a)

Orientações: O acadêmico ou acadêmica deverá preencher e assinar este documento e, após, uni-lo ao TCC e ao Termo de Depósito e Composição da Banca Examinadora em um único arquivo PDF. O acadêmico ou acadêmica deverá, então, proceder ao depósito desse arquivo PDF único, observando a data limite estipulada pelo Colegiado de Curso.

UNIVERSIDADE FEDERAL DO MATO GROSSO DO SUL

IASMIN NATÁLIA DIAS CANHETTE

DIREITOS HUMANOS E SAÚDE DIGITAL: PROTEÇÃO DE DADOS DE SAÚDE

TRÊS LAGOAS

2025

UNIVERSIDADE FEDERAL DO MATO GROSSO DO SUL

DIREITOS HUMANOS E SAÚDE DIGITAL: PROTEÇÃO DE DADOS DE SAÚDE

Trabalho de Conclusão de curso apresentado como requisito parcial para a obtenção do título de bacharelado em Direito pela Universidade Federal do Mato Grosso do Sul.

Orientador: Professor Doutor Michel Ernesto Flumian

TRÊS LAGOAS

2025

AGRADECIMENTOS

Agradeço, antes de tudo, a Deus e a Nossa Senhora, pela presença constante em cada passo desta caminhada. Foram eles quem me concederam a força necessária para seguir, mesmo diante das incertezas, me guiaram com luz e propósito. À minha família, por me apoiar em todos os momentos, compreender minhas ausências e acreditar nos meus sonhos. Cada gesto de amor e incentivo foi o alicerce que sustentou minha trajetória acadêmica. Ao meu orientador, Professor Michel, por sua paciência, dedicação e orientação cuidadosa. Sua confiança e insistência em mim, me mostraram um potencial que eu não imaginava ter. Aos professores da Universidade Federal de Mato Grosso do Sul, que, com compromisso e generosidade, contribuíram para minha formação ética, crítica e humana. Aos amigos e colegas de curso, que tornaram tudo mais leve. Levo comigo o aprendizado e as lembranças de cada um. Por fim, agradeço a todos que, de forma direta ou indireta, participaram deste percurso. Este trabalho é o reflexo de muitas mãos, corações e orações — e a cada um que fez parte disso, deixo aqui minha sincera gratidão.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

CCPA –Lei de Privacidade do Consumidor da Califórnia

CF/88 – Constituição Federal de 1988

GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados da União Europeia)

HIPAA – Health Insurance Portability and Accountability Act (Lei de Portabilidade e Responsabilidade de Seguros de Saúde dos EUA)

IA – Inteligência Artificial

IoT – Internet of Things (Internet das Coisas)

LAI – Lei de Acesso à Informação (Lei nº 12.527/2011)

LGPD – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

MCI – Marco Civil da Internet (Lei nº 12.965/2014)

OMS – Organização Mundial da Saúde

ONU – Organização das Nações Unidas

PEP – Prontuário Eletrônico do Paciente

SUS – Sistema Único de Saúde

RESUMO

A rápida transformação digital trouxe impactos significativos para o setor da saúde, exigindo reflexão sobre os benefícios e os riscos da utilização de tecnologias que lidam diretamente com dados sensíveis da população. Nesse contexto, torna-se indispensável compreender a relação entre os direitos humanos, o direito fundamental à saúde e a proteção da privacidade, principalmente diante do uso crescente de prontuários eletrônicos, telemedicina, aplicativos móveis e inteligência artificial. O objetivo deste trabalho é analisar como a saúde digital pode contribuir para a efetivação do direito à saúde no Brasil, ao mesmo tempo em que discute os desafios relacionados à proteção de dados pessoais, com ênfase na aplicação da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e em legislações complementares, como a Lei de Acesso à Informação e o Marco Civil da Internet. O presente estudo foi desenvolvido sob uma abordagem qualitativa, caracterizando-se como uma pesquisa bibliográfica exploratório-descritiva. O processo de levantamento de dados incluiu a consulta sistemática a fontes primárias, tal como a Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018 e a Lei de Acesso à Informação – Lei nº 12.527/2011; e legislação internacional, notadamente o Regulamento Geral de Proteção de Dados – GDPR da União Europeia, e o Health Insurance Portability and Accountability Act – HIPAA dos EUA) e a fontes secundárias (doutrina jurídica especializada, artigos científicos e documentos oficiais de organizações internacionais como a OMS). Os resultados evidenciaram que a digitalização em saúde trouxe ganhos importantes na gestão e no acesso aos serviços, mas também revelou riscos de exclusão digital, falhas de interoperabilidade e vulnerabilidades que podem comprometer a privacidade do paciente. Conclui-se que a saúde digital só poderá consolidar-se como instrumento de fortalecimento do direito à saúde se estiver associada a políticas públicas inclusivas, a práticas de ética digital e a sistemas robustos de segurança da informação, assegurando o equilíbrio entre inovação tecnológica e proteção dos direitos fundamentais.

Palavras-chave: Saúde digital; Direitos humanos; LGPD; Proteção de dados; Privacidade.

ABSTRACT

The rapid digital transformation has had significant impacts on the healthcare sector, requiring reflection on the benefits and risks of using technologies that directly handle sensitive population data. In this context, understanding the relationship between human rights, the fundamental right to health, and privacy protection is essential, especially given the growing use of electronic health records, telemedicine, mobile applications, and artificial intelligence. The objective of this work is to analyze how digital health can contribute to the realization of the right to health in Brazil, while also discussing the challenges related to personal data protection, with an emphasis on the application of the General Data Protection Law (LGPD – Law No. 13,709/2018) and complementary legislation, such as the Access to Information Law and the Brazilian Civil Rights Framework for the Internet. This study was developed using a qualitative approach, characterized as exploratory-descriptive bibliographic research. The data collection process included systematic consultation of primary sources, such as the General Personal Data Protection Law (Law No. 13,709/2018) and the Access to Information Law (Law No. 12,527/2011); and international legislation, notably the European Union's General Data Protection Regulation (GDPR) and the US Health Insurance Portability and Accountability Act (HIPAA), as well as secondary sources (specialized legal doctrine, scientific articles, and official documents from international organizations such as the WHO). The results showed that digitalization in healthcare has brought significant gains in management and access to services, but also revealed risks of digital exclusion, interoperability failures, and vulnerabilities that can compromise patient privacy. It is concluded that digital health can only consolidate itself as an instrument for strengthening the right to health if it is associated with inclusive public policies, digital ethics practices, and robust information security systems, ensuring a balance between technological innovation and the protection of fundamental rights.

Keywords: Digital health; Human rights; LGPD; Data protection; Privacy.

1 INTRODUÇÃO

A saúde digital transformou de forma profunda a prestação de serviços no campo da saúde, incorporando prontuários eletrônicos, sistemas de telemedicina, aplicativos de monitoramento e ferramentas de inteligência artificial aplicadas à prática clínica. Esse processo ampliou o acesso, favoreceu a continuidade do cuidado e otimizou a gestão de serviços, sobretudo no Sistema Único de Saúde (SUS), que desde a Estratégia de Saúde Digital 2020-2028 vem apostando na informatização como recurso estratégico para a promoção da integralidade e da universalização da atenção (HADDAD; LIMA, 2024). Ao mesmo tempo em que proporciona avanços, a digitalização expõe cidadãos a riscos crescentes de violações da intimidade, da vida privada e da dignidade, sobretudo no que se refere ao tratamento de dados sensíveis, como os de saúde.

O problema central que emerge nesse cenário reside na seguinte questão: como garantir a proteção de dados de saúde, considerados sensíveis pela legislação, sem comprometer o avanço tecnológico e a democratização do acesso aos serviços digitais? Essa problemática evidencia-se pela interoperabilidade crescente das bases de dados, pela circulação massiva de informações pessoais e pela dificuldade em assegurar que os mecanismos de proteção acompanhem a velocidade das inovações. A saúde digital coloca em debate a efetividade dos direitos humanos no século XXI, especialmente no que se refere à privacidade e à autonomia dos pacientes.

A justificativa para esta investigação assenta-se no fato de que a proteção de dados de saúde não é apenas uma questão técnica, mas uma dimensão essencial da cidadania e dos direitos fundamentais. A Constituição Federal de 1988 garante, em seu artigo 5º, inciso X, o direito à intimidade e à vida privada, e, no artigo 196, estabelece a saúde como direito de todos e dever do Estado. Em complemento, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – classificou informações relacionadas à saúde como dados sensíveis, exigindo tratamento específico e maior rigor em sua utilização. Em âmbito internacional, tanto a Declaração

Universal dos Direitos Humanos (1948) quanto o Regulamento Geral de Proteção de Dados (GDPR), da União Europeia, reforçam a necessidade de assegurar que a inovação digital não seja acompanhada por retrocessos em direitos fundamentais (SIQUEIRA; HOCH, 2019).

Estudos acadêmicos também alertam para os riscos de discriminação, exclusão e estigmatização decorrentes do uso inadequado dessas informações, ressaltando que a perda de controle sobre dados de saúde compromete a autonomia dos indivíduos e a confiança nas instituições (DONEDA; MONTEIRO, 2015). Nesse sentido, torna-se urgente debater mecanismos de regulação, fiscalização e ética que sustentem a saúde digital em consonância com os valores democráticos e os princípios do Estado de Direito.

Diante do exposto esse estudo tem como objetivo geral analisar a relação entre direitos humanos, saúde digital e proteção de dados de saúde, identificando os principais desafios éticos, jurídicos e sociais envolvidos nesse processo e tem como objetivos específicos: examinar as legislações nacionais e internacionais aplicáveis à proteção de dados de saúde; discutir os riscos e consequências da má gestão dessas informações; e apontar boas práticas e recomendações para garantir que a inovação tecnológica na saúde ocorra em consonância com os direitos fundamentais.

O presente estudo foi desenvolvido sob uma abordagem qualitativa, caracterizando-se como uma pesquisa bibliográfica exploratório-descritiva. O processo de levantamento de dados incluiu a consulta sistemática a fontes primárias, tal como a Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018 e a Lei de Acesso à Informação – Lei nº 12.527/2011; e legislação internacional, notadamente o Regulamento Geral de Proteção de Dados – GDPR da União Europeia, e o Health Insurance Portability and Accountability Act – HIPAA dos EUA) e a fontes secundárias (doutrina jurídica especializada, artigos científicos e documentos oficiais de organizações internacionais como a OMS). A seleção do material bibliográfico priorizou publicações com reconhecida relevância acadêmica e pertinência temática, a fim de garantir a atualização e o debate mais recente sobre os desafios da saúde digital. A análise dos dados ocorreu por meio de uma abordagem hermenêutica e interpretativa, buscando compreender os conceitos, princípios e normas jurídicas, identificar as relações entre os direitos humanos e as inovações tecnológicas na saúde, e analisar criticamente os desafios éticos e jurídicos da proteção de dados nesse contexto.

A discussão proposta pretende não apenas situar os avanços tecnológicos no campo da saúde, mas também refletir sobre os limites e responsabilidades inerentes ao seu uso, reafirmando a centralidade da dignidade humana e da proteção da privacidade como condições indispensáveis para a construção de uma saúde digital ética, segura e inclusiva.

2. DIREITOS HUMANOS E O DIREITO À SAÚDE

2.1. CONCEITO DE SAÚDE DIGITAL E E-SAÚDE

O avanço das tecnologias de informação e comunicação (TICs) na área da saúde trouxe novos paradigmas para a organização dos serviços e para o cuidado ao paciente. Nesse cenário, surgem os conceitos de saúde digital e e-Saúde, que apesar de próximos, não são sinônimos. A literatura destaca que ambos os termos se referem à utilização de recursos tecnológicos para ampliar a efetividade dos serviços de saúde, mas diferem em abrangência e finalidade.

De acordo com Soares et al. (2022), a saúde digital pode ser entendida como o conjunto de práticas, técnicas e soluções tecnológicas que promovem maior integração entre profissionais, gestores e pacientes, com o objetivo de melhorar a qualidade da assistência. Esse conceito engloba desde a informatização de prontuários eletrônicos até o uso de inteligência artificial, big data, dispositivos móveis e aplicativos que auxiliam na prevenção e no tratamento de doenças.

Já a e-Saúde (ou e-Health, em inglês) surgiu inicialmente como um termo mais restrito, associado ao uso de tecnologias digitais em plataformas eletrônicas voltadas à comunicação e ao gerenciamento de dados em saúde. Para Passos (2019), a e-Saúde está relacionada ao desenvolvimento de ferramentas informatizadas que possibilitam a troca de informações médicas, o suporte à decisão clínica e a comunicação entre os diferentes níveis de atenção à saúde.

A Organização Mundial da Saúde (OMS) conceitua a e-Saúde como “o uso seguro e econômico das tecnologias de informação e comunicação em apoio à saúde e às áreas relacionadas, incluindo serviços, vigilância, educação, conhecimento e pesquisa”. Essa definição evidencia a importância da e-Saúde como base estruturante para a transição rumo à saúde digital, pois representa a etapa inicial de informatização e de comunicação digital no campo da saúde pública.

Silva et al. (2024) identificam que o conceito de saúde digital, especialmente na Atenção Primária à Saúde, é dinâmico e ainda em construção, possuindo múltiplos sinônimos como telessaúde e telemedicina. Para os autores, a saúde digital não deve ser reduzida a um conjunto de ferramentas tecnológicas, mas sim compreendida como um meio para promover o cuidado remoto, fortalecer a comunicação entre profissionais e pacientes e qualificar a gestão do sistema de saúde. Essa perspectiva amplia o alcance da saúde digital, posicionando-a como parte de uma transformação estrutural nos modelos de atenção.

A relação entre saúde digital e inclusão social. De acordo com Francesconi et al. (2025), a saúde digital deve ser pensada como oportunidade de inovação no SUS, possibilitando maior eficiência e qualidade nos serviços, mas também precisa enfrentar barreiras como a exclusão digital e a falta de infraestrutura tecnológica em regiões remotas. Assim, o conceito não pode ser dissociado das políticas públicas, já que a democratização do acesso às tecnologias de saúde é condição para a efetivação de sua função social.

No campo acadêmico, Santos (2025) aponta que a saúde digital se diferencia da e-Saúde pela sua abrangência, uma vez que incorpora elementos mais recentes, como o uso de dispositivos vestíveis, aplicativos de monitoramento em tempo real e plataformas de inteligência artificial. Enquanto a e-Saúde refere-se a uma etapa anterior, voltada para a informatização e integração de sistemas, a saúde digital está ligada à personalização do cuidado, ao engajamento do paciente e à análise preditiva de dados em larga escala.

De Sousa (2023) reforça esse entendimento ao destacar que a saúde digital deve ser compreendida como um avanço do direito à saúde na era tecnológica. Para a autora, a incorporação de novas tecnologias cria oportunidades para ampliar a eficiência e o acesso, mas também gera desafios relacionados à privacidade, segurança da informação e regulação. Assim, o conceito de saúde digital está intimamente vinculado não apenas à inovação, mas também à responsabilidade ética e jurídica.

Além disso, Sun, Guimarães e Araujo (2022) destacam que a transformação digital nos sistemas de saúde, representada pela saúde digital, deve ser analisada como parte de um processo global. Nos países em desenvolvimento, a saúde digital ainda enfrenta obstáculos de infraestrutura e capacitação, enquanto em países desenvolvidos já se consolida como estratégia de gestão integrada dos serviços. Os

autores afirmam que compreender o conceito de saúde digital é reconhecer sua natureza multidimensional, que abrange tanto aspectos técnicos quanto sociais e políticos.

Almeida Filho (2024) argumenta que a saúde digital deve ser compreendida como um conjunto de saberes e práticas que superam a visão reducionista das tecnologias como simples ferramentas. O autor introduz o conceito de metapresencialidade, no qual o cuidado em saúde é mediado pela presença digital, criando novas formas de interação e ampliando as possibilidades de promoção da saúde coletiva. Esse entendimento amplia o debate conceitual e reforça que a saúde digital não é apenas uma modernização de processos, mas sim um novo paradigma de cuidado, que exige reconfigurações epistemológicas e práticas.

Pode-se afirmar que a e-Saúde representa o estágio inicial da digitalização dos serviços de saúde, focado na informatização e comunicação eletrônica, enquanto a saúde digital constitui uma etapa mais abrangente e inovadora, que incorpora tecnologias disruptivas, promove maior protagonismo do paciente e redefine a lógica do cuidado. Mais do que uma mudança técnica, trata-se de uma transformação cultural e organizacional, cujo objetivo é integrar o direito à saúde aos avanços da era digital, garantindo que inovação e inclusão caminhem lado a lado.

2.2. AVANÇOS TECNOLÓGICOS NO SUS (PRONTUÁRIO ELETRÔNICO, TELESSAÚDE, APLICATIVOS, IA)

A transformação digital na saúde brasileira tem se materializado em diversas iniciativas no âmbito do Sistema Único de Saúde (SUS), buscando alinhar os princípios de universalidade, integralidade e equidade aos avanços das tecnologias da informação. Entre essas iniciativas, destacam-se a implantação dos prontuários eletrônicos, o fortalecimento da telessaúde, o uso de aplicativos móveis voltados ao cuidado e a crescente incorporação de ferramentas de inteligência artificial (IA) na prática clínica e na gestão dos serviços.

O prontuário eletrônico do paciente (PEP) constitui uma das inovações mais significativas, pois permite reunir em uma única plataforma os dados clínicos, diagnósticos, exames e tratamentos realizados. Lima et al. (2025) apontam que a informatização desse processo trouxe maior agilidade, padronização e segurança na gestão das informações, reduzindo falhas decorrentes de registros em papel e

facilitando a comunicação entre os diferentes níveis de atenção. Além disso, a Portaria nº 2.073/2011 do Ministério da Saúde regulamentou a certificação de sistemas de registro eletrônico em saúde, exigindo padrões mínimos de segurança e interoperabilidade. Esse movimento fortaleceu a possibilidade de acompanhamento longitudinal do paciente, permitindo maior efetividade no cuidado e integração entre as unidades de saúde.

Outro marco importante é o programa Telessaúde Brasil Redes, criado em 2007 e expandido nos anos seguintes, que utiliza tecnologias de comunicação para apoiar a atenção básica e reduzir desigualdades regionais. Maldonado e Cruz (2021) destacam que a telemedicina e a telessaúde ganharam centralidade durante a pandemia da Covid-19, especialmente após a publicação da Portaria nº 467/2020, que regulamentou as consultas médicas a distância em caráter emergencial. Essa medida representou não apenas uma alternativa temporária, mas também um avanço para consolidar a telemedicina como ferramenta permanente de cuidado, sobretudo em localidades remotas e de difícil acesso.

Os aplicativos móveis e plataformas digitais também passaram a integrar o cotidiano dos usuários do SUS, com destaque para o Conecte SUS, que possibilita o acesso a resultados de exames, histórico de vacinas, receitas digitais e informações sobre atendimentos. Para Francesconi et al. (2025), a integração desses aplicativos à rede de saúde representa uma oportunidade para ampliar a autonomia do paciente e promover maior transparência, aproximando a população dos serviços públicos. No entanto, os autores também ressaltam a importância de políticas que garantam a inclusão digital, a fim de que o acesso às ferramentas não seja limitado a parcelas da população com maior nível de escolaridade ou acesso à internet.

Mais recentemente, a utilização de inteligência artificial (IA**)** e análise de grandes bases de dados tem sido incorporada ao SUS como instrumento de apoio ao diagnóstico e à gestão. Silva et al. (2025) destacam que algoritmos de aprendizado de máquina têm sido aplicados na detecção precoce de doenças, no monitoramento de surtos epidemiológicos e na organização de fluxos de atendimento. Esses recursos possibilitam maior precisão em diagnósticos, previsão de riscos e personalização de condutas clínicas. Contudo, De Sousa (2023) alerta que a incorporação dessas ferramentas levanta desafios éticos e jurídicos relacionados à privacidade, à transparência dos algoritmos e à responsabilidade em caso de erros.

O uso de IA e big data na saúde pública permite avançar na construção de

políticas baseadas em evidências. Penteado et al. (2023) destacam que a Estratégia de Saúde Digital 2020-2028 estabeleceu diretrizes para a integração das novas tecnologias, incluindo a criação de sistemas interoperáveis que favoreçam a tomada de decisões em tempo real. A expectativa é que, ao longo dos próximos anos, a inteligência artificial contribua não apenas para diagnósticos individuais, mas também para estratégias coletivas de prevenção, planejamento de recursos e gestão hospitalar.

Apesar dos avanços, os desafios são expressivos. Sun, Guimarães e Araujo (2022) ressaltam que a transformação digital nos sistemas de saúde depende de investimentos contínuos em infraestrutura, capacitação dos profissionais e criação de mecanismos de regulação capazes de acompanhar a velocidade da inovação. Nesse sentido, é necessário que o Estado atue de forma estratégica, garantindo que o uso dessas tecnologias esteja alinhado ao direito à saúde e à proteção dos dados sensíveis da população.

Os avanços tecnológicos no SUS – representados pelo prontuário eletrônico, pela telessaúde, pelos aplicativos digitais e pela inteligência artificial – configuram uma verdadeira revolução nos serviços públicos de saúde. Tais inovações ampliam a eficiência, favorecem o acesso e qualificam a assistência, mas também exigem reflexão crítica sobre inclusão, privacidade e equidade. O desafio consiste em assegurar que essas ferramentas não se tornem um fator de desigualdade, mas sim um instrumento de fortalecimento do direito universal à saúde.

2.3. BENEFÍCIOS E RISCOS DA DIGITALIZAÇÃO: GESTÃO, INCLUSÃO E DESAFIOS DE INTEROPERABILIDADE

A digitalização da saúde trouxe benefícios incontestáveis tanto para a gestão dos serviços quanto para a experiência dos pacientes. A informatização dos processos administrativos e clínicos permite maior controle sobre os fluxos assistenciais, otimiza a alocação de recursos e fortalece o planejamento em saúde. Segundo Lima et al. (2025), a modernização proporcionada pelos prontuários eletrônicos e sistemas informatizados de registro reduziu erros manuais e garantiu maior precisão nas informações, criando condições para diagnósticos mais assertivos e tratamentos personalizados. Do ponto de vista da gestão pública, Francesconi et al. (2025) ressaltam que o uso de big data e inteligência artificial possibilita a análise de

grandes volumes de dados, o que favorece a formulação de políticas baseadas em evidências e a previsão de surtos epidemiológicos. Esses ganhos traduzem-se em maior eficiência e efetividade na tomada de decisões dentro do Sistema Único de Saúde (SUS).

No campo da inclusão, a saúde digital ampliou o alcance dos serviços, especialmente em contextos de desigualdade social e territorial. A expansão da telemedicina, intensificada durante a pandemia da Covid-19, tornou possível atender populações em áreas remotas ou com escassez de profissionais de saúde. Maldonado e Cruz (2021) destacam que a chamada Telemedicina 4.0 conectou pacientes e médicos em tempo real, reduzindo barreiras geográficas e garantindo continuidade ao cuidado mesmo em cenários de crise. Além disso, aplicativos móveis e plataformas digitais, como o Conecte SUS, aproximaram os cidadãos dos serviços públicos, permitindo maior autonomia no acompanhamento de consultas, exames e vacinação (FRANCESCONI et al., 2025). Para Santos (2025), essa experiência fortaleceu a percepção de protagonismo do paciente, que passou a ter maior controle sobre sua saúde e sobre o próprio histórico clínico.

Apesar dos benefícios, a digitalização também apresenta riscos importantes. Um dos principais é a exclusão digital, que afeta comunidades sem acesso adequado à internet ou com baixa alfabetização tecnológica. Sun, Guimarães e Araujo (2022) apontam que, enquanto países desenvolvidos avançam rapidamente na incorporação de tecnologias de ponta, em nações em desenvolvimento persistem barreiras estruturais que limitam a universalização da saúde digital. No Brasil, essa realidade se reflete nas disparidades regionais: áreas urbanas concentram maior oferta de serviços digitais, enquanto localidades rurais e comunidades vulneráveis ainda enfrentam dificuldades de conectividade e infraestrutura.

Outro desafio é a interoperabilidade dos sistemas, isto é, a capacidade de diferentes plataformas digitais de saúde se comunicarem de maneira eficiente. Passos (2019) observa que, sem padrões técnicos unificados, os prontuários eletrônicos e outros sistemas de gestão acabam funcionando de forma isolada, o que compromete a continuidade do cuidado e gera retrabalho para os profissionais. Essa fragmentação também eleva os riscos de inconsistências nos registros e fragiliza a proteção de dados, já que informações podem ser duplicadas ou armazenadas em ambientes pouco seguros.

A questão da segurança da informação é um risco diretamente ligado à

digitalização. Sousa (2023) alerta que a intensificação do uso de inteligência artificial e big data abre novas possibilidades de inovação, mas também amplia a vulnerabilidade a vazamentos de dados sensíveis, que podem ser utilizados para fins discriminatórios ou comerciais. Para mitigar esses riscos, torna-se fundamental o cumprimento da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que classifica informações de saúde como categoria sensível e estabelece regras mais rígidas para seu tratamento.

A digitalização da saúde oferece benefícios expressivos em termos de gestão, inclusão e eficiência, mas exige atenção constante aos riscos de exclusão social, falhas de interoperabilidade e ameaças à privacidade. O desafio central consiste em equilibrar inovação e proteção de direitos, garantindo que a modernização tecnológica no SUS ocorra em consonância com os princípios de universalidade, integralidade e equidade que orientam o sistema.

3. PROTEÇÃO DE DADOS DE SAÚDE: ASPECTOS LEGAIS E ÉTICOS

3.1. A LGPD E A REGULAÇÃO BRASILEIRA DA PROTEÇÃO DE DADOS DE SAÚDE

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) representa um marco jurídico no Brasil ao estabelecer princípios e regras para o tratamento de dados pessoais, inclusive no setor da saúde. Inspirada em legislações internacionais como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD busca assegurar direitos fundamentais como a privacidade, a liberdade e a dignidade da pessoa humana, ao mesmo tempo em que regula a atuação de organizações públicas e privadas no uso de informações sensíveis. No âmbito da saúde, sua relevância é ainda mais significativa, uma vez que dados clínicos, genéticos e biométricos são considerados altamente sensíveis e demandam tratamento específico, sob pena de gerar discriminação e violação da intimidade dos indivíduos (SARLET; RUARO, 2021).

A LGPD estabelece que dados de saúde, por integrarem a categoria de dados pessoais sensíveis, devem receber um nível elevado de proteção, exigindo base legal específica para seu tratamento. Isso significa que hospitais, clínicas, laboratórios e até mesmo aplicativos de monitoramento precisam justificar juridicamente a coleta, o

armazenamento e o compartilhamento dessas informações. Para Aragão e Schiocchet (2020), o impacto da LGPD no Sistema Único de Saúde (SUS) é profundo, pois exige que a maior rede pública de saúde da América Latina adote medidas rápidas e eficazes de adequação, implementando padrões de segurança da informação e treinamento contínuo dos profissionais que lidam com dados clínicos.

Um dos princípios centrais da lei é o da finalidade, que determina que o tratamento de dados só pode ocorrer para propósitos legítimos e previamente informados ao titular. Associado a isso, o princípio da transparência garante ao paciente o direito de ser informado sobre como seus dados estão sendo utilizados e a possibilidade de solicitar correções ou exclusões. Sousa et al. (2024) destacam que a aplicação da LGPD no setor da saúde também fortaleceu a noção de autodeterminação informativa, assegurando ao paciente maior controle sobre suas informações pessoais. Esse direito torna-se essencial em um cenário de crescente digitalização, no qual o cidadão deve ser protagonista do processo de proteção de sua privacidade.

Outro aspecto importante é a relação entre a LGPD e o desenvolvimento de novas tecnologias. Dourado e Aith (2022) apontam que a lei brasileira se consolidou como o ponto de partida para a regulação da inteligência artificial na saúde, principalmente por reconhecer o direito à explicação e à revisão de decisões automatizadas. Isso significa que algoritmos usados para apoiar diagnósticos ou indicar tratamentos devem ser transparentes e auditáveis, evitando que decisões médicas fiquem restritas a sistemas opacos, também conhecidos como “caixas-pretas”. Assim, a LGPD não apenas protege dados, mas também cria parâmetros éticos e regulatórios para a incorporação da inteligência artificial no setor de saúde.

Apesar de seus avanços, a implementação da LGPD enfrenta desafios práticos. Gonçalo et al. (2025) ressaltam que a rápida evolução tecnológica exige regulamentações complementares e governança eficiente, pois a lei, embora abrangente, precisa ser constantemente atualizada para lidar com novas demandas, como a interoperabilidade de sistemas de saúde, o compartilhamento internacional de dados e o uso crescente de big data. No caso do SUS, essas dificuldades são ampliadas pelo porte da rede e pela desigualdade regional, que dificulta a padronização de medidas de segurança em todo o território nacional.

A LGPD funciona como um instrumento de equilíbrio entre inovação e proteção de direitos fundamentais. Ao mesmo tempo em que permite o avanço da saúde digital,

por meio da informatização de prontuários eletrônicos, telemedicina e plataformas digitais, a lei impõe limites claros para evitar abusos, como o uso discriminatório de informações médicas ou sua exploração para fins comerciais. Como argumenta Sarlet e Ruaro (2021), a efetiva aplicação da LGPD é condição indispensável para garantir que a transformação digital na saúde ocorra em consonância com a dignidade da pessoa humana.

A LGPD representa um marco regulatório estruturante para a saúde digital no Brasil**.** Sua importância vai além da proteção jurídica de dados, pois está diretamente vinculada à garantia do direito à saúde em um ambiente digital seguro e ético. No entanto, a plena eficácia da lei dependerá da atuação conjunta do Estado, das instituições de saúde e da sociedade civil, de modo a assegurar que o avanço tecnológico seja compatível com os direitos fundamentais e com a universalidade que norteia o sistema de saúde brasileiro.

3.2. MARCOS LEGAIS COMPLEMENTARES: LEI DE ACESSO À INFORMAÇÃO E MARCO CIVIL DA INTERNET

A proteção de dados em saúde e a garantia da privacidade digital não podem ser analisadas de forma isolada, estando necessariamente relacionadas a um conjunto de legislações complementares que regulam o ambiente digital no Brasil. Entre essas normas, destacam-se a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014)**,** ambos fundamentais para estabelecer parâmetros de transparência, responsabilidade e direitos no uso da informação.

A Lei de Acesso à Informação (LAI) representou um passo decisivo para a consolidação da democracia e da participação social no país, garantindo ao cidadão o direito de solicitar e receber informações públicas, inclusive em relação às políticas de saúde. De acordo com De Miranda e Zaganelli (2017), a LAI se conecta ao conceito de compliance público, pois cria mecanismos para coibir a má gestão e a corrupção, ao mesmo tempo em que fortalece a transparência administrativa. No contexto da saúde digital, essa legislação contribui para que usuários e instituições possam fiscalizar a utilização de dados sensíveis, garantindo maior confiança no sistema.

Já o Marco Civil da Internet (MCI)**,** sancionado em 2014, é reconhecido como uma espécie de “Constituição da Internet” no Brasil. Sua construção foi fruto de um amplo processo participativo, que incluiu consultas públicas virtuais e contribuições

da sociedade civil, como destaca Cruz (2015), ao analisar a experiência inovadora de elaboração legislativa. Esse processo democrático conferiu legitimidade à norma, que se tornou referência internacional ao estabelecer princípios como a neutralidade da rede, a proteção da privacidade e a liberdade de expressão**.**

Entre seus dispositivos, o MCI reforça o direito à privacidade e à proteção dos dados pessoais, prevendo que a coleta, uso e armazenamento de informações devem respeitar princípios de necessidade, finalidade e consentimento. Kopstein e Zanella (2023) apontam que o MCI foi decisivo para balizar juridicamente a liberdade de expressão na internet, mas reconhecem que tal direito não é absoluto, devendo ser ponderado em relação a outros, como a honra e a privacidade. Essa perspectiva é essencial quando se trata de dados de saúde, que constituem informações sensíveis e podem gerar discriminação se não forem devidamente protegidos.

Apesar de seus avanços, o Marco Civil também apresenta limitações práticas. Silva et al. (2024) observam que, diante do crescimento das redes sociais e do aumento dos conflitos relacionados à desinformação, discurso de ódio e responsabilidade das plataformas, a legislação mostra-se insuficiente para responder aos novos desafios. Ainda que tenha estabelecido diretrizes importantes, há lacunas regulatórias, sobretudo no que tange à responsabilização civil de intermediários digitais e à proteção contra o uso abusivo de dados.

Assim, tanto a LAI quanto o MCI se apresentam como marcos complementares à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), pois, ao mesmo tempo em que asseguram transparência e participação social, estabelecem limites e deveres no uso da informação em ambiente digital. Enquanto a LAI garante o direito de acesso a dados públicos, o MCI define os contornos da privacidade e da liberdade na internet, criando um equilíbrio entre transparência e proteção. No campo da saúde digital, essa complementaridade é indispensável para que a regulação seja efetiva, conciliando inovação tecnológica, proteção dos direitos fundamentais e segurança da informação.

3.3 COMPARAÇÕES INTERNACIONAIS: GDPR EUROPEU, HIPAA NOS EUA E VULNERABILIDADES DOS DADOS SENSÍVEIS.

A regulação da proteção de dados pessoais apresenta diferentes configurações ao redor do mundo, refletindo as particularidades políticas, jurídicas e culturais de

cada região. No contexto europeu, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR – General Data Protection Regulation), aprovado em 2016 e em vigor desde 2018, como o marco mais robusto e abrangente em termos de tutela de dados. No cenário norte-americano, embora não exista uma lei federal única, a HIPAA (Health Insurance Portability and Accountability Act), criada em 1996, cumpre papel essencial no campo da saúde ao regular o uso e compartilhamento de informações médicas. Comparar esses modelos evidencia não apenas convergências, mas também fragilidades e vulnerabilidades que precisam ser enfrentadas em escala global.

O GDPR tem como base a concepção de que a proteção de dados é um direito fundamental, estabelecendo princípios como a licitude, a finalidade, a transparência e a minimização dos dados. Ele impõe regras estritas para o tratamento de informações sensíveis, como dados de saúde, genéticos e biométricos, exigindo consentimento explícito e garantindo direitos ao titular, como acesso, portabilidade e exclusão. Para Oliveira et al. (2024), esse regulamento tornou-se referência mundial, influenciando legislações como a LGPD no Brasil e o CCPA na Califórnia, justamente por adotar um padrão elevado de proteção e prever sanções rigorosas em caso de descumprimento.

Nos Estados Unidos, a regulação é fragmentada, com leis estaduais e setoriais. No caso da saúde, a HIPAA assegura a confidencialidade e integridade de dados clínicos, mas é considerada restrita quando comparada ao GDPR, pois seu foco está na proteção de informações médicas em transações eletrônicas, não alcançando todo o espectro de dados digitais. Conforme Gomes et al. (2025), essa limitação gera vulnerabilidades significativas, uma vez que outras categorias de dados sensíveis, como hábitos de consumo digital ou informações coletadas por aplicativos de saúde, podem ficar desprotegidas. Além disso, os recentes escândalos de vazamento de dados, como o caso Cambridge Analytica, revelaram a fragilidade do modelo estadunidense frente ao uso indiscriminado de informações pessoais.

Outro ponto importante diz respeito às novas tecnologias, como a Blockchain, que apresentam desafios de conformidade regulatória. Farias Júnior (2024) observa que a natureza descentralizada e imutável dessa tecnologia dificulta a aplicação de normas como o GDPR e a LGPD, especialmente no que se refere ao direito ao esquecimento e à exclusão de dados. Isso evidencia que, mesmo regulamentos avançados, enfrentam limitações quando aplicados a ambientes digitais disruptivos.

No que tange à categoria de dados sensíveis, Gimenez (2025) ressalta que o

rol estabelecido pela LGPD e pelo GDPR não deve ser interpretado de forma taxativa, já que o avanço tecnológico constantemente cria novas formas de coleta e uso de informações pessoais. Essa compreensão é essencial para lidar com vulnerabilidades emergentes, como o uso de dados de geolocalização, de dispositivos vestíveis (wearables) e de algoritmos de inteligência artificial aplicados à saúde.

O GDPR europeu representa um padrão de excelência em proteção de dados, enquanto a HIPAA norte-americana mantém-se como uma legislação específica, porém limitada. As vulnerabilidades apontadas pelos especialistas reforçam a necessidade de harmonização internacional, capaz de estabelecer parâmetros mínimos globais para assegurar a privacidade, a dignidade e a segurança das informações pessoais em um mundo cada vez mais digitalizado e interconectado.

4. DIREITOS HUMANOS E A PROTEÇÃO DA PRIVACIDADE EM SAÚDE DIGITAL

4.1 A AUTODETERMINAÇÃO INFORMATIVA E O PAPEL DO ESTADO NA REGULAÇÃO

O conceito de autodeterminação informativa refere-se ao direito do indivíduo de controlar a coleta, o tratamento e a utilização de seus dados pessoais, assegurando que apenas ele possa decidir, de forma consciente e informada, sobre o destino dessas informações. Trata-se de um desdobramento do direito fundamental à privacidade, reconhecido como essencial na sociedade da informação. Para Sousa e Silva (2020), a autodeterminação informativa constitui um instrumento de empoderamento do titular dos dados, conferindo-lhe maior capacidade de defesa frente às práticas abusivas de instituições públicas e privadas, especialmente em contextos de intensa digitalização.

Esse princípio surgiu com força no cenário europeu, a partir da jurisprudência do Tribunal Constitucional Alemão, em 1983, no julgamento da chamada “Lei do Censo”, quando se consolidou a ideia de que o cidadão deve ter meios de controlar quem pode acessar suas informações e para quais finalidades. No Brasil, essa concepção foi incorporada na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que estabelece a autodeterminação informativa como fundamento central para a proteção dos dados pessoais. Como explicam Lugati e Almeida (2020),

o consentimento do titular, embora seja uma das principais ferramentas de proteção, não é suficiente por si só para garantir a autodeterminação, sendo necessária a atuação efetiva do Estado para equilibrar a relação entre indivíduos e grandes corporações.

A doutrina também enfatiza que a autodeterminação informativa deve ser compreendida como um direito de natureza constitucional, intimamente ligado à dignidade da pessoa humana. Batista, Cesar e Cesar (2024) destacam que, diante da massificação dos fluxos de dados e dos constantes vazamentos de informações, esse direito passa a ser um espaço de disputa democrática, no qual o Estado deve assumir a função de regulador e fiscalizador, garantindo que as tecnologias não sejam utilizadas para reduzir a autonomia dos indivíduos. Nesse sentido, a autodeterminação informativa não é apenas um direito individual, mas também uma garantia coletiva de que o tratamento de dados respeitará valores constitucionais como a liberdade, a igualdade e a não discriminação.

Teixeira (2018) complementa essa perspectiva ao afirmar que, na era da sociedade de risco, marcada pela vigilância digital e pela coleta massiva de dados, o papel do Estado torna-se indispensável para impor limites claros às práticas tanto de entes privados quanto de órgãos públicos. Ele defende que o Estado não pode delegar integralmente a proteção de dados ao mercado, sob pena de enfraquecer a efetividade do direito fundamental, sendo necessário estruturar mecanismos de supervisão, transparência e responsabilização.

Assim, a autodeterminação informativa deve ser vista como um princípio norteador da proteção de dados, mas que só se concretiza plenamente com a presença ativa do Estado. Cabe ao poder público estabelecer normas, criar autoridades independentes, fiscalizar condutas e punir abusos, de forma a equilibrar o avanço tecnológico com a garantia dos direitos fundamentais. Em síntese, a proteção dos dados pessoais, especialmente na área da saúde digital, só se efetiva quando a autodeterminação informativa é combinada com políticas regulatórias eficazes e com a responsabilidade estatal em assegurar a dignidade da pessoa humana.

4.2 O PAPEL DAS INSTITUIÇÕES E PROFISSIONAIS DE SAÚDE NA PRESERVAÇÃO DA PRIVACIDADE

A preservação da privacidade no contexto da saúde digital constitui um dos maiores desafios da contemporaneidade, visto que envolve informações consideradas altamente sensíveis e diretamente ligadas à dignidade da pessoa humana. Nesse cenário, tanto as instituições de saúde quanto os profissionais que nelas atuam assumem responsabilidade central no tratamento ético e seguro dessas informações. Keinert e Cortizo (2018) explicam que a privacidade em saúde possui dimensões normativas, tecnológicas e culturais, o que exige não apenas legislações robustas, mas também uma mudança de postura institucional e profissional frente ao manuseio de dados sensíveis.

As instituições de saúde, públicas ou privadas, devem adotar políticas de governança de dados, alinhadas à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que incluam desde a implementação de sistemas de prontuário eletrônico seguros até protocolos de criptografia e acesso restrito. Moraes (2020) destaca que a gestão das informações em saúde precisa ocorrer em nível de excelência, pois a confidencialidade dos registros clínicos é indispensável para a continuidade do cuidado e para a preservação da confiança entre pacientes e serviços. Além disso, a responsabilidade institucional inclui a promoção de treinamentos contínuos de suas equipes, garantindo que todos os profissionais compreendam as implicações éticas e jurídicas do tratamento inadequado de informações.

No âmbito individual, os profissionais de saúde têm o dever ético e legal de resguardar o sigilo profissional, já previsto nos códigos de ética das diferentes categorias. Contudo, a digitalização dos processos amplia os riscos de exposição indevida. Casos como o da atriz Klara Castanho, analisado por Matheus (2025), demonstram como falhas no cumprimento do dever de confidencialidade podem gerar graves violações de direitos fundamentais, expondo a vulnerabilidade dos pacientes e a necessidade de fortalecimento das práticas de compliance institucional. Esse episódio reforça a obrigação dos profissionais em adotar condutas responsáveis, que vão além do atendimento clínico, incluindo o zelo pela proteção dos dados que acessam.

A crescente utilização da telemedicina e de plataformas digitais de atendimento impõe novos desafios. Lopes et al. (2025) apontam que a implementação da LGPD nesses serviços ainda enfrenta obstáculos práticos, como a padronização do consentimento informado e a adaptação dos sistemas de informação às exigências

legais. Esses entraves evidenciam que a preservação da privacidade não depende apenas da lei, mas de uma atuação integrada entre tecnologia, processos de gestão e consciência profissional.

Assim, a atuação responsável de instituições e profissionais deve ser vista como um compromisso ético coletivo, voltado não apenas à obediência normativa, mas à proteção efetiva da dignidade do paciente. Ao garantir a confidencialidade e a segurança das informações, fortalecem-se a confiança no sistema de saúde e a legitimidade do cuidado, consolidando a privacidade como um direito inalienável que deve ser preservado em todas as práticas de saúde.

4.3 PERSPECTIVAS FUTURAS: ÉTICA DIGITAL, POLÍTICAS PÚBLICAS E SEGURANÇA DA INFORMAÇÃO

Ao pensar o futuro da saúde digital, torna-se evidente a necessidade de articular políticas públicas consistentes, uma ética digital fortalecida e práticas de segurança da informação que acompanhem os avanços tecnológicos. A inclusão digital é um dos principais eixos desse processo, uma vez que a expansão de serviços digitais em saúde só será efetiva se alcançar populações historicamente excluídas. Sousa et al. (2023) ressaltam que a inclusão não deve se restringir ao acesso físico às tecnologias, mas deve contemplar também competências digitais, infraestrutura sustentável e sensibilização cultural, de modo a evitar que a digitalização aprofunde desigualdades sociais.

Nesse cenário, a formulação de políticas públicas deve ir além da modernização tecnológica, incorporando estratégias de educação digital e cidadania informacional. Guidi et al. (2025) explicam que a cidadania digital emerge como um direito fundamental, exigindo que governos invistam em sistemas de proteção cibernética, mas também em campanhas de conscientização que capacitem cidadãos a utilizarem de forma segura e ética as ferramentas digitais. Isso implica em integrar legislações já existentes, como a Lei Geral de Proteção de Dados, a estratégias mais amplas de governança digital, garantindo que princípios como universalidade e equidade, próprios do SUS, sejam preservados.

Outro aspecto essencial é a construção de uma sólida ética digital. Narciso et al. (2024) destacam que a simples adoção de plataformas digitais não é suficiente: é necessário refletir sobre as implicações éticas do uso massivo de dados, prevenindo

abusos e reforçando práticas de transparência. No campo da saúde, essa preocupação é ainda mais urgente, já que informações clínicas possuem caráter sensível e sua utilização inadequada pode comprometer direitos fundamentais.

A segurança da informação aparece como condição inegociável para a confiança do usuário nos serviços digitais. Isso envolve tanto a implementação de soluções tecnológicas como criptografia, autenticação em múltiplos fatores e sistemas de monitoramento contra ataques cibernéticos quanto o desenvolvimento de uma cultura organizacional que valorize a privacidade. A convergência entre políticas públicas, ética digital e segurança informacional aponta para um futuro no qual a saúde digital poderá consolidar-se como ferramenta inclusiva, democrática e comprometida com os direitos humanos.

5. CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste trabalho evidenciou que a transformação digital no campo da saúde representa um avanço incontornável, capaz de ampliar o acesso, melhorar a gestão de informações e qualificar o atendimento oferecido aos cidadãos. Contudo, ao mesmo tempo em que traz benefícios significativos, esse processo também suscita dilemas éticos, jurídicos e sociais que precisam ser enfrentados para que a inovação tecnológica esteja alinhada aos direitos humanos e constitucionais.

Constatou-se que a saúde, enquanto direito fundamental previsto na Constituição Federal de 1988, deve ser compreendida em articulação com a proteção da privacidade e da dignidade da pessoa humana. Nesse sentido, a digitalização da saúde exige atenção especial ao tratamento dos dados pessoais, especialmente os considerados sensíveis, como os registros clínicos e genéticos. A preservação da confidencialidade dessas informações é condição essencial para a manutenção da confiança entre paciente e profissional, bem como para a efetividade das políticas públicas de saúde.

A pesquisa demonstrou ainda que marcos normativos como a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014) desempenham papéis complementares na construção de um ambiente regulatório capaz de equilibrar inovação tecnológica e proteção de direitos. Esses instrumentos, somados às

experiências internacionais como o GDPR europeu e a HIPAA norte-americana, apontam caminhos para fortalecer a regulação e minimizar vulnerabilidades.

A atuação estatal se mostra indispensável para garantir fiscalização e políticas públicas consistentes, mas não é suficiente sem o compromisso ético das instituições e dos profissionais de saúde na adoção de práticas seguras e respeitosas no tratamento das informações. A proteção de dados deve ser incorporada como parte da cultura organizacional e da qualidade assistencial.

As perspectivas futuras indicam que a saúde digital tende a se expandir com a incorporação de novas tecnologias, como inteligência artificial, big data e dispositivos vestíveis. Para que esse processo ocorra de maneira inclusiva e sustentável, será imprescindível investir em políticas de inclusão digital, ética digital e segurança da informação, garantindo que a modernização tecnológica não amplie desigualdades, mas contribua para a efetivação dos princípios de universalidade, integralidade e equidade do SUS.

A proteção dos dados de saúde não é apenas uma exigência legal, mas sobretudo uma questão de respeito à dignidade humana e de fortalecimento da cidadania. A saúde digital, se conduzida de forma responsável, pode se consolidar como um instrumento poderoso para a promoção da saúde coletiva, desde que os avanços tecnológicos caminhem lado a lado com a defesa dos direitos fundamentais.

REFERÊNCIAS

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do sistema único de saúde. **Reciis**, v. 14, n. 3, 2020. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2012. Acesso em: 2 jul. 2025.

BATISTA, Waleska Miguel; CESAR, Camila Torres; CESAR, Daniel. Autodeterminação informativa e sua importância na sociedade da informação sobre o prisma constitucional. **Revista Direitos Culturais**, v. 19, n. 47, p. 75-91, 2024. Disponível em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/1631. Acesso em: 25 jun. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 jun. 2025.

CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet**. 2015. Tese (Doutorado) — Universidade de São Paulo, São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/en.php. Acesso em: 22 jun. 2025.

DONEDA, Danilo; DE AGUIAR MONTEIRO, Marília. Proteção de dados pessoais enquanto direito fundamental e o direito fundamental à saúde–privacidade e e-Health. **Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética**, p. 147, 2015. Disponível em:https://www.saude.sp.gov.br/resources/instituto-de-saude/homepage/temas-saude-coletiva/pdfs/14470instsaude.pdf. Acesso em: 18 jul. 2025.

DOURADO, Daniel de Araujo; AITH, Fernando Mussa Abujamra. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais. **Revista de Saúde Pública**, v. 56, p. 80, 2022. Disponível em: https://www.scielo.br/j/rsp/a/k38jGvJdbQSYN4MpzGZpfXw/?lang=pt. Acesso em: 25 ago. 2025.

FARIAS JÚNIOR, Tácito Augusto. **Privacidade de dados em Blockchain: um estudo sobre a conformidade regulatória com as regulamentações de proteção de dados do Brasil e da Europa**. 2024. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal de Sergipe, São Cristóvão, 2024. Disponível em: https://ri.ufs.br/jspui/handle/riufs/19550. Acesso em: 3 jul. 2025.

FRANCESCONI, Laura Rosa et al. Saúde coletiva na era digital: desafios e oportunidades para a inovação no SUS. **Lumen et Virtus**, v. 16, n. 47, p. 3805-3813, 2025. Disponível em: https://periodicos.newsciencepubl.com/LEV/article/view/4551. Acesso em: 2 ago. 2025.

GIMENEZ, Carina Magda de Souza. **Dados pessoais sensíveis: rol exemplificativo ou taxativo? Uma análise da categoria especial à luz da LGPD**. 2025. Dissertação (Mestrado Profissional em Direito) — Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, São Paulo, 2025. Disponível em: https://repositorio.idp.edu.br/handle/123456789/5422. Acesso em: 11 ago. 2025.

GONÇALO, Wemerson et al. Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023. **Physis: Revista de Saúde Coletiva**, v. 35, p. e350113, 2025. Disponível em: https://www.scielo.br/j/physis/a/56MHDpw9hrMKXYzCWyB77Cp/. Acesso em: 17 ago. 2025

GUEDES GOMIDE NASCIMENTO GOMES, Patrícia et al. Vulnerabilidades: panorama das legislações de proteção de dados pessoais GDPR, CCPA, LGPD e

PIPL. Direito UNIFACS – **Debate Virtual**, n. 297, 2025. Disponível em: https://revistas.unifacs.br/index.php/redu/article/download/9520/5363. Acesso em: 7 jun. 2025.

GUIDI, Zulma Nascimento et al. A IMPORTÂNCIA DA SEGURANÇA E DA CIDADANIA DIGITAL NA ERA DA INFORMAÇÃO. **Revista Tópicos**, v. 3, n. 24, p. 1-15, 2025. Disponível em:https://interface.org.br/publicacoes/saude-digital-no-sistema-unico-de-saude-sus/ Revista Interface Acesso em: 9 ago. 2025.

HADDAD, Ana Estela; LIMA, Nísia Trindade. Saúde Digital no Sistema Único de Saúde (SUS). **Interface-Comunicação, Saúde, Educação**, v. 28, p. e230597, 2024. Disponível em: https://www.scielo.br/j/icse/a/nZkyh3JK8dNkZMkxcPjg9gm/?format=html&lang=p. Acesso em: 14 ago. 2025.

KEINERT, Tania Margarete Mezzomo; CORTIZO, Carlos Tato. Dimensões da privacidade das informações em saúde. **Cadernos de Saúde Pública**, v. 34, n. 7, p. e00039417, 2018. Disponível em: https://www.scielo.br/j/csp/a/VQbX3mB7hz4rZvrYwHqG9Lx/. Acesso em: 18 jun. 2025.

KOPSTEIN, Marcos Antunes; ZANELLA, Diego Carlos. Compreensões legais acerca da liberdade de expressão na Internet**. Meritum, Revista de Direito da Universidade FUMEC**, v. 18, n. 2, 2023. Disponível em: https://revista.fumec.br/index.php/meritum/article/view/9030. Acesso em: 30 ago. 2025.

LOPES, Eloísa Karine Braga et al. Desafios da implementação da Lei Geral de Proteção de Dados em serviços de saúde que fazem uso da telemedicina: uma revisão integrativa. **Cadernos Ibero-Americanos de Direito Sanitário**, v. 14, n. 1, 2025. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/1238. Acesso em: 12 jun. 2025.

LUGATI, Lys Nunes; de Almeida, Juliana Evangelista. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, v. 12, n. 2, p. 1-33, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 3 ago. 2025.

MALDONADO, José; CRUZ, Antonio. Telemedicina 4.0: desafios e oportunidades para o SUS. **Relatório de Pesquisa**. **Projeto Desafios para o Sistema Único de Saúde no contexto nacional e global de transformações sociais, econômicas e tecnológicas (CEIS 4.0)**. Rio de Janeiro: CEE/Fiocruz, 2021. Disponível em:

https://cee.fiocruz.br/sites/default/files/Relatorio%20Final%20-%20Fiocruz%20-%20Maldonado%20e%20Cruz.pdf. Acesso em: 6 ago. 2025.

MATHEUS, Ana Carolina Couto. Privacidade e proteção de dados na saúde suplementar: uma análise crítica do caso Klara Castanho à luz do ordenamento jurídico brasileiro e do compliance. **Virtuajus**, Belo Horizonte, v. 10, n. 18, p. 125-140, 2025. Disponível em: https://periodicos.pucminas.br/virtuajus/article/view/35769. Acesso em: 28 jun. 2025.

MIRANDA, Wallace Vieira de; ZAGANELLI, Juliana Costa. Marco civil da internet e política pública de transparência: uma análise da e-democracia e do compliance público. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 633-646, 2017. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/4921. Acesso em: 6 jul. 2025.

MORAES, Margarete Farias de. Segurança, privacidade e confidencialidade dos registros em saúde. **Informação em Pauta**, v. 5, n. 1, p. 23-35, 2020. Disponível em: https://periodicos.ufc.br/informacaoempauta/article/view/43510. Acesso em: 12 jul. 2025.

NARCISO, Rodi et al. Ética e privacidade na educação digital: os desafios éticos e de privacidade no uso de tecnologias digitais. **Revista Foco**, v. 17, n. 1, p. e4123, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/4123. Acesso em: 30 jun. 2025.

OLIVEIRA LIMA, Lucas Alves et al. INFORMATIZAÇÃO EM SAÚDE: AVANÇOS TECNOLÓGICO E A MODERNIZAÇÃO NOS SERVIÇOS DE SAÚDE. **Lumen Et Virtus**, v. 16, n. 48, p. 5102-5111, 2025. Disponível em: https://periodicos.newsciencepubl.com/LEV/article/view/5091. Acesso em: 15 jul. 2025.

OLIVEIRA, Marcos Martins et al. Análise comparada das normas de proteção de dados do Brasil, da União Europeia e do Estado da Califórnia — EUA: LGPD X GDPR X CCPA. **Revista de Direito, Governança e Novas Tecnologias, Florianópolis**, v. 10, n. 2, 2025. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/10923. Acesso em: 23 ago. 2025.

PASSOS, Carlos Nestor. Transformação digital na saúde: desafios e perspectivas. **Revista Científica Hospital Santa Izabel**, v. 3, n. 3, p. 178-184, 2019. Disponível em: https://revistacientifica.hospitalsantaizabel.org.br/index.php/RCHSI/article/view/53 revistacientifica.hospitalsantaizabel.org.br Acesso em: 5 ago. 2025.

PENTEADO, Bruno Elias et al. A digitalização em saúde sob os marcos da Estratégia de Saúde Digital para o Brasil. **Revista Fronteiras**, v. 25, n. 1, 2023. Disponível em: https://revistas.unisinos.br/index.php/fronteiras/article/view/25695/60749509. Acesso em: 16 ago. 2025.

SANTOS, João Victor Secundo. Transformação digital no setor de saúde: tendências, desafios e impactos na experiência do paciente. **Revista Contemporânea**, v. 5, n. 6, p. e8330, 2025. Disponível em: https://ojs.revistacontemporanea.com/ojs/index.php/home/article/view/8330. Acesso em: 8 ago. 2025.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 81-106, maio/ago. 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 31 jul. 2025.

SILVA, Cícera Renata Diniz Vieira et al. Conceito de saúde digital na Atenção Primária à Saúde (2020-2022): um estudo baseado no método evolucionário de Rodgers. **Boletim de Conjuntura (BOCA)**, v. 17, n. 49, p. 432-454, 2024. Disponível em: https://revista.ioles.com.br/boca/index.php/revista/article/view/3156 revista.ioles.com.br Acesso em: 1 ago. 2025.

SILVA, Gleciane Souza et al. Inovação digital na saúde pública: impactos, desafios e perspectivas. **Asclepius International Journal of Scientific Health Science,** v. 4, n. 4, p. 103-109, 2025. Disponível em: https://asclepiushealthjournal.com/index.php/aijshs/article/view/81 asclepiushealthjournal.com Acesso em: 10 jul. 2025.

SILVA, Iris Nathalia da et al. Liberdade de Expressão e Responsabilidade Civil nas Plataformas de Redes Sociais: **As Insuficiências do Marco Civil da Internet**. 2024. Trabalho de Conclusão de Curso (Graduação) — Universidade Federal de Santa Catarina. Disponível em: https://repositorio.ufsc.br/handle/123456789/262804.Acesso em: 13 ago. 2025

SILVA, Marcos Fernandes da et al. A era dos dispositivos digitais na promoção da saúde: conectando o cuidado. **Brazilian Journal of Implantology and Health Sciences**, v. 6, n. 5, p. 1260-1288, 2024. Disponível em: https://bjihs.emnuvens.com.br/bjihs/article/view/2138. Acesso em: 5 jun. 2025.

SIQUEIRA, L.; HOCH, P. Os dados pessoais e a proteção de dados de saúde: análise a partir das iniciativas de e-Saúde. In: **Congresso Internacional de Direito e Contemporaneidade**, Rio Grande do Sul, 2019. Anais… p. 1-18. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.2.pdf. Acesso em: 14 ago. 2025.

SOARES, Alessandra Nascimento et al. O que é saúde digital? Uma revisão integrativa. **Brazilian Journal of Development**, v. 8, n. 5, p. 38954-38972, 2022. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/48290 Brazilian Journals+1 Acesso em: 13 jul. 2025.

SOUSA, Cibele Faustino de. Impactos das inovações tecnológicas na saúde: direito à saúde e tecnologia. **Gestão & Cuidado em Saúde**, v. 1, n. 1, e11462, 2023. Disponível em: https://revistas.uece.br/index.php/gestaoecuidado/article/view/11462.Acesso em: 13 ago. 2025.

SOUSA, Maria Aparecida de Moura Amorim et al. Inclusão digital: perspectivas futuras e desafios em potencial. **Revista Internacional de Estudos Científicos**, v. 1, n. 2, p. 199-219, 2023. Disponível em: https://www.researchgate.net/publication/375871749_Inclusao_Digital_perspectivas_futuras_e_desafios_em_potencial. Acesso em: 26 ago. 2025

SOUSA, Rosilene Paiva Marinho; DA SILVA, Paulo Henrique Tavares. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Informação & Sociedade**, v. 30, n. 2, 2020. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/52483. Acesso em: 7 ago. 2025.

SOUSA, Vanielly Lino et al. Os impactos da Lei Geral de Proteção de Dados (LGPD) no sistema de saúde brasileiro. **Revista JRG de Estudos Acadêmicos**, v. 7, n. 14, p. e141129, 2024. Disponível em: https://revistajrg.com/index.php/jrg/article/view/1129. Acesso em: 13 jul. 2025.

SUN, Violeta; GUIMARÃES, Luisa; ARAÚJO, Marcelo. A transformação digital nos sistemas de saúde. **Panorama Setorial da Internet**, n. 1, p. 1-32, 2022. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/20220428183557/psi-ano-14-n-1-a_transformacao_digital_nos_sistemas_de_saude.pdf. Acesso em: 10 jun. 2025

TEIXEIRA, Guilherme da Fonseca. Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados: a inevitável privatização dos deveres estaduais de proteção. **Católica Law Review**, v. 2, n. 1, p. 11-38, jan. 2018. https://revistas.ucp.pt/index.php/catolicalawreview/article/view/1995/1918. Acesso em: 10 jun. 2025