REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

# ÉTICA E SEGURANÇA DE DADOS EM REDE: IMPLICAÇÕES PARA A SAÚDE DIGITAL

**ETHICS AND NETWORK DATA SECURITY: IMPLICATIONS FOR DIGITAL HEALTH**

Engenharias, Ciências Sociais Aplicadas, Ciências da Saúde •

25/11/2026

REGISTRO DOI: 10.70773/revistatopicos/795532731

Alciene Pereira da Silva
Marcelo Ossamu Honda
Solana Marina Bonfim Lemos
Maria Eduarda Sousa Fontinele
Lorena Poliana Gonçalves Goes
Maria Lúcia Farias Neta
Ramon Pereira Ribeiro
Sara Raquel Pinto Brandão Silva
Rita de Cássia de Almeida
Bethânia Millena Martins Silva

**RESUMO**

Este artigo analisa a articulação entre ética e segurança de dados em rede no contexto da saúde digital, com ênfase no ordenamento jurídico brasileiro. O problema central consiste em verificar como os princípios éticos e as exigências técnicas de proteção de dados podem ser integrados de modo a garantir dignidade, transparência e confiança aos titulares de dados sensíveis. Metodologicamente, adota-se revisão narrativa da literatura, complementada por análise documental da Lei Geral de Proteção de Dados (LGPD) e de referenciais internacionais. Os resultados indicam que a conformidade legal, embora necessária, é insuficiente para responder aos riscos contemporâneos, tais como *function creep*, vigilância algorítmica e uso comercial indevido de informações de saúde. Conclui-se que a incorporação de princípios éticos desde a concepção dos sistemas tipo *ethics by design*, aliada a mecanismos de consentimento granular, interoperabilidade segura e educação digital, constitui condição para que a saúde digital se desenvolva sem comprometer direitos fundamentais.

**Palavras-chave:** Ética de dados; Segurança da informação; LGPD; Saúde digital; Interoperabilidade.

**ABSTRACT**

This article examines the relationship between ethics and network data security in the context of digital health, with emphasis on the Brazilian legal framework. The central problem is to verify how ethical principles and technical data protection requirements can be integrated to ensure dignity, transparency, and trust for data subjects handling sensitive information. Methodologically, it adopts a narrative literature review complemented by documentary analysis of the Brazilian General Data Protection Law (LGPD) and international references. Results indicate that legal compliance,

while necessary, is insufficient to address contemporary risks such as function creep, algorithmic surveillance, and improper commercial use of health information. It concludes that embedding ethical principles from system design onward—ethics by design—alongside granular consent, secure interoperability, and digital education, is a condition for digital health development without compromising fundamental rights.
**Keywords:** Data ethics; Information security; LGPD; Digital health; Interoperability.

## INTRODUÇÃO

A digitalização dos serviços de saúde ampliou de modo significativo a circulação de informações pessoais sensíveis, colocando em evidência tensões entre inovação tecnológica e proteção de direitos fundamentais. Prontuários eletrônicos, plataformas de telemedicina, aplicações de monitoramento remoto e sistemas de inteligência artificial aplicados ao cuidado passaram a demandar não apenas infraestrutura técnica robusta, mas também parâmetros éticos claros para o tratamento de dados (Farias; Almeida, 2026; Brasil, 2018).

O problema que orienta este estudo pode ser formulado nos seguintes termos: *em que medida a conformidade com a Lei Geral de Proteção de Dados (LGPD) é suficiente para assegurar práticas éticas e seguras na saúde digital?* A hipótese sustentada é que a dimensão legal, embora indispensável, não esgota as exigências de proteção, sendo necessária a incorporação de uma perspectiva ética proativa ao ciclo de vida da informação em saúde.

O objetivo geral consiste em analisar as implicações éticas e de segurança de dados para a saúde digital no Brasil. Como objetivos específicos, pretende-se: (i) discutir os conceitos fundamentais de ética e segurança de dados aplicados à saúde; (ii) situar historicamente a proteção de dados e a LGPD; (iii) examinar os direitos dos titulares e os princípios aplicáveis ao tratamento de dados sensíveis; e (iv) comparar abordagens legalistas e centradas no humano na engenharia de sistemas de saúde digital.

Justifica-se o estudo pela crescente relevância do tema no debate regulatório e pela necessidade de orientar práticas institucionais que conciliem inovação, eficiência e respeito à autodeterminação informativa dos pacientes.

## METODOLOGIA

Trata-se de revisão narrativa da literatura, realizada a partir de consulta a bases indexadas e periódicos da área de saúde coletiva, direito sanitário e tecnologia da informação.

Complementarmente, procedeu-se à análise documental da Lei nº 13.709/2018 (LGPD) e de referenciais internacionais sobre proteção de dados, notadamente o Regulamento Geral de Proteção de Dados da União Europeia (GDPR). A seleção das fontes priorizou publicações recentes que abordassem a interface entre ética, segurança da informação e saúde digital, bem como estudos de revisão sobre a implementação da LGPD no setor saúde. Os resultados são apresentados de forma descritiva e analítica, organizados em torno dos eixos conceituais, históricos, normativos e aplicados.

## CONCEITOS FUNDAMENTAIS

A ética de dados designa o conjunto de princípios morais que orientam o tratamento da informação, assegurando que seu uso respeite valores como dignidade, justiça e transparência (Floridi; Taddeo, 2016) Na saúde digital, essa dimensão define não apenas o quê, mas o porquê e o como da coleta e utilização de dados pessoais, vinculando o tratamento a finalidades legítimas e previamente informadas aos titulares) (OMS, 2021; Brasil, 2018).

Estudos recentes evidenciam que a incorporação de tecnologias como inteligência artificial e big data exige governança regulatória robusta para prevenir vieses discriminatórios e proteger a privacidade dos pacientes. A ética de dados, nesse sentido, não se reduz ao cumprimento legal: envolve postura proativa de responsabilidade social e compromisso com direitos fundamentais (Araújo; Campos, 2025).

A segurança de dados, por sua vez, compreende o conjunto de práticas e tecnologias voltadas à proteção da informação, com vistas a assegurar confidencialidade, integridade e disponibilidade. No setor saúde, isso implica implementar controles que previnam acessos não autorizados, vazamentos e usos indevidos de dados sensíveis.

A literatura aponta que a rápida evolução tecnológica amplia os riscos de exposição em sistemas interoperáveis, como prontuários eletrônicos e plataformas de telemedicina. A segurança deve, portanto, ser compreendida como processo contínuo, envolvendo criptografia, autenticação, monitoramento e descarte seguro de informações. Regulamentos como a LGPD e o GDPR reforçam a necessidade de alinhar práticas técnicas a princípios éticos,

garantindo tratamento transparente e proporcional às finalidades declaradas (Gonçalo *et al.*, 2025).

## MARCOS HISTÓRICOS DA PROTEÇÃO DE DADOS

A discussão sobre privacidade ganhou marco teórico no final do século XIX com o artigo The Right to Privacy, de Warren e Brandeis (1890), que defendia o direito de ser deixado sozinho muito antes da era digital. Na década de 1970, com o avanço da computação, surgiram as primeiras preocupações regulatórias: a Lei do Estado alemão de Hesse, de 1970, é considerada o primeiro texto legal de proteção de dados do mundo, motivada pela necessidade de proteger cidadãos contra abusos informacionais, em parte como reação ao período nazista.

Na década seguinte, a popularização dos computadores pessoais e o surgimento dos primeiros vírus levaram ao desenvolvimento de soluções de segurança digital, como antivírus e firewalls. A chegada da internet intensificou a comunicação e o compartilhamento de dados em escala global, criando novos desafios éticos e de segurança. A partir dos anos 2000, a explosão da coleta de dados por empresas, redes sociais e sistemas de inteligência artificial trouxe à tona dilemas mais complexos, como perfilamento comportamental, disseminação de desinformação e proteção em sistemas imprevisíveis.

No Brasil, a Lei nº 13.709/2018 representa marco regulatório ao estabelecer princípios fundamentais para o tratamento de dados pessoais. Inspirada no GDPR, a LGPD busca proteger os direitos fundamentais de liberdade e privacidade, garantindo que o uso de

dados ocorra de forma ética, transparente e proporcional às finalidades declaradas.

A trajetória histórica da proteção de dados não constitui uma linha evolutiva linear, mas um processo cumulativo de respostas a crises e a transformações tecnológicas que reconfiguraram as relações de poder entre indivíduos, Estados e corporações. A formulação seminal de Warren e Brandeis (1890), embora situada no contexto da imprensa sensacionalista do final do século XIX, estabeleceu o alicerce conceitual do "direito de ser deixado sozinho" que, posteriormente, seria ressignificado diante da computação de larga escala. Contudo, é preciso reconhecer que essa matriz anglo-americana de privacidade como não interferência mostrou-se insuficiente para capturar a complexidade da vigilância contemporânea, na qual o poder não se exerce apenas pela exposição, mas pela modulação algorítmica de comportamentos e pela mercantilização de perfis.

A Lei do Estado alemão de Hesse, de 1970, surge precisamente como uma resposta à necessidade de proteger o cidadão não apenas contra a intrusão estatal, mas contra os abusos informacionais de um Estado que, no período nazista, utilizara registos populacionais para fins de perseguição sistemática.

Esse marco é frequentemente citado como o primeiro texto legal de proteção de dados do mundo, mas sua importância reside menos na inovação técnica do que na introdução de um princípio fundamental: o tratamento de dados pessoais exige uma base legal e finalidades legítimas, não podendo ser exercido de forma arbitrária . A partir dessa experiência, a década de 1970 assistiu à proliferação de legislações nacionais na Europa, muitas delas influenciadas pela

necessidade de harmonizar a proteção de dados com o fluxo transfronteiriço de informações, especialmente após o desenvolvimento dos primeiros sistemas de computação em rede.

A popularização dos computadores pessoais nos anos 1980 e a subsequente expansão da internet nos anos 1990 deslocaram o foco da proteção de dados do âmbito estatal para o setor privado. O surgimento de vírus, *malware* e a crescente dependência de infraestruturas digitais para serviços essenciais evidenciaram que a segurança da informação não era apenas uma questão de confidencialidade, mas de integridade e disponibilidade dos sistemas. Nesse período, a Diretiva 95/46/CE da União Europeia representou um esforço pioneiro de harmonização regulatória, estabelecendo princípios como finalidade, proporcionalidade e direitos de acesso e retificação que, décadas depois, influenciariam diretamente a LGPD brasileira.

A partir dos anos 2000, a explosão da coleta de dados por plataformas digitais, redes sociais e sistemas de inteligência artificial introduziu dilemas qualitativamente distintos. O *function creep* com o uso de dados para finalidades não declaradas originalmente, tornou-se prática corrente em modelos de negócio baseados em vigilância e publicidade comportamental.

A disseminação de desinformação e a opacidade dos algoritmos de recomendação revelaram que a proteção de dados não podia mais ser concebida apenas como um direito de controle individual sobre informações já coletadas, mas exigia uma abordagem proativa que incidisse sobre a arquitetura dos sistemas. É nesse contexto que o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), de 2016, e a LGPD brasileira, de 2018, emergem não apenas

como instrumentos de conformidade, mas como tentativas de reequilibrar as relações de poder entre titulares e agentes de tratamento.

No Brasil, a trajetória até a LGPD foi marcada por uma pluralidade de fontes normativas setoriais — como o Código de Defesa do Consumidor, o Marco Civil da Internet e normas do setor de saúde — que, embora relevantes, careciam de um framework unificado para a proteção de dados pessoais. A aprovação da Lei nº 13.709/2018, inspirada no GDPR mas adaptada às especificidades do ordenamento jurídico brasileiro, representou um avanço ao estabelecer fundamentos autônomos como a autodeterminação informativa e a dignidade da pessoa humana que transcendem a mera tutela da privacidade . Contudo, a efetividade da LGPD depende não apenas de sua arquitetura normativa, mas da capacidade institucional da Autoridade Nacional de Proteção de Dados (ANPD) e da maturidade das organizações em incorporar seus princípios em práticas cotidianas, especialmente em setores de alta sensibilidade, como a saúde.

## LGPD E O TRATAMENTO DE DADOS NA SAÚDE DIGITAL

A LGPD estabelece conceitos estruturantes para a construção de direitos e deveres entre titulares e agentes de tratamento. O titular é a pessoa natural a quem se referem os dados pessoais; o controlador é a pessoa natural ou jurídica a quem competem as decisões sobre o tratamento; o operador realiza o tratamento em nome do controlador; e o encarregado é a pessoa indicada para atuar como canal de comunicação entre controlador, titulares e a Autoridade Nacional de Proteção de Dados.

Os princípios da finalidade, necessidade e transparência orientam o tratamento, assegurando que informações pessoais sejam coletadas apenas quando estritamente necessárias, utilizadas de forma objetiva e comunicadas de maneira clara ao usuário. Na saúde digital, tais princípios assumem relevância ampliada, pois envolvem dados sensíveis que exigem rigor adicional na proteção e no consentimento informado.

O tratamento de dados pessoais em saúde deve observar as hipóteses legais previstas na LGPD, como consentimento explícito, tutela da saúde ou cumprimento de obrigação legal. Esses fundamentos garantem que o uso da informação seja legítimo e proporcional às finalidades declaradas (Brasil, 2018; Voigt; Von dem Bussche, 2017).

Os direitos dos titulares constituem eixo central da proteção de dados e asseguram maior autonomia e transparência no uso da informação. Entre eles, destacam-se: a confirmação da existência de tratamento, que permite ao titular solicitar às instituições de saúde informações sobre o uso de seus dados, evitando práticas ocultas (Tavares; Oliveira, 2023); o acesso e a correção de dados, que garantem a atualização de informações incorretas ou desatualizadas, preservando a integridade clínica (Araújo; Campos, 2025); e a revogação do consentimento, que assegura ao titular retirar sua autorização a qualquer momento, reforçando o princípio da autodeterminação informativa (Gonçalo *et al.*, 2025).

No que se refere à portabilidade e à eliminação, verifica-se a possibilidade de transferência segura de informações entre sistemas interoperáveis e a exclusão definitiva quando não houver mais justificativa legal para o tratamento (Voigt; Von dem Bussche, 2017).

Além disso, a informação sobre compartilhamento e sobre as consequências da negativa garante transparência quanto a quem acessa os dados e quais impactos podem decorrer da recusa em fornecê-los, especialmente em contextos de saúde pública e pesquisa (Alshawii *et al.*, 2022). A efetividade desses direitos, contudo, depende da implementação prática de mecanismos de consentimento granular, interoperabilidade segura e educação digital, que ampliem a compreensão dos usuários sobre seus próprios direitos.

A aplicação da LGPD ao setor saúde exige uma leitura que transcenda a literalidade dos dispositivos legais e considere as especificidades do ecossistema assistencial. Em primeiro lugar, é fundamental reconhecer que o conceito de "titular" não se restringe ao paciente: acompanhantes, familiares, profissionais de saúde e terceirizados também têm seus dados tratados nas operações cotidianas de hospitais, clínicas e plataformas de telemedicina . Essa amplitude impõe às instituições a necessidade de mapear fluxos informacionais que muitas vezes escapam à percepção dos gestores, especialmente em ambientes onde o prontuário eletrônico se tornou o centro nevrálgico da assistência (De Paula, 2026)

Os dados de saúde são classificados pela LGPD como dados pessoais sensíveis, o que implica um regime jurídico mais restritivo e a exigência de bases legais específicas para o tratamento . Entre as hipóteses autorizativas, destacam-se a tutela da saúde que permite o compartilhamento de informações entre profissionais envolvidos no cuidado, o cumprimento de obrigação legal ou regulatória como a notificação compulsória de doenças e a guarda de prontuários por prazos determinados e o exercício regular de direitos, especialmente em contextos de defesa em processos judiciais ou administrativos. A

coexistência dessas bases legais exige do controlador uma análise cuidadosa da finalidade específica de cada operação, sob pena de configurar tratamento incompatível com os princípios da finalidade e da necessidade (Araujo, 2025; Alshawii, 2022;)

Os direitos dos titulares, embora formalmente assegurados pela LGPD, enfrentam desafios práticos significativos no ambiente digital de saúde. O direito de acesso, por exemplo, é frequentemente dificultado pela fragmentação dos sistemas de prontuário eletrônico e pela ausência de interfaces que permitam ao paciente compreender, em linguagem acessível, quais dados foram coletados e como são utilizados (Brasil, 2018).

A portabilidade, por sua vez, esbarra em barreiras técnicas de interoperabilidade e em resistências institucionais à transferência de informações entre prestadores concorrentes (Brasil, 2018a). A revogação do consentimento, quando aplicável, suscita questões complexas sobre a possibilidade de exclusão de dados já integrados a registos clínicos cuja retenção é obrigatória por normas sanitárias (BRASIL, 2018b; CFM, 2007). Essas tensões revelam que a efetividade dos direitos depende não apenas de sua previsão legal, mas da implementação de mecanismos concretos de consentimento granular, painéis de transparência e APIs seguras que viabilizem seu exercício (Brasil, 2020; Cavoukian, 2011).

A governança em proteção de dados no setor saúde demanda, ainda, uma articulação entre a LGPD e o sigilo profissional, que historicamente rege a relação médico-paciente. O dever de confidencialidade, embora anterior à lei, é por ela reforçado na medida em que estabelece sanções administrativas e mecanismos

de responsabilização que não existiam no regime puramente deontológico (Cavoukian,2011).

Contudo, a conformidade não se esgota na assinatura de termos de consentimento ou na publicação de políticas de privacidade: exige a implementação de controlos de acesso baseados em perfis, o registo de *logs* de auditoria, a segregação de funções e a capacitação continuada de todos os envolvidos no tratamento, desde a recepção até o corpo clínico. A ausência dessas medidas configura risco não apenas jurídico, mas ético, na medida em que expõe os titulares a danos decorrentes de acessos indevidos, vazamentos e usos secundários não autorizados (Cavoukian,2011).

## ABORDAGENS DE ENGENHARIA E CICLO DE VIDA DA INFORMAÇÃO

A engenharia de software aplicada à saúde digital exige abordagem que transcenda a técnica, incorporando valores éticos e sociais. Duas perspectivas destacam-se nesse cenário. A abordagem legalista prioriza normas, compliance e conformidade regulatória, com foco em atender requisitos da LGPD e do GDPR e garantir alinhamento dos sistemas às legislações vigentes (Voigt; Von dem Bussche, 2017).

A abordagem centrada no humano enfatiza a ética por concepção (*ethics by design*), incorporando princípios como dignidade, justiça e transparência desde a fase de projeto, com o objetivo de reduzir vieses algorítmicos e promover confiança social (Araújo; Campos, 2025).

O ciclo de vida da informação em saúde digital deve ser orientado por práticas éticas e seguras em todas as suas etapas. A minimização recomenda a coleta apenas dos dados estritamente

necessários, evitando excessos que ampliem riscos de exposição. A retenção e o descarte exigem políticas claras de armazenamento temporário e eliminação segura após o uso, prevenindo vazamentos e usos indevidos (Tavares; Oliveira, 2023).

A evolução tecnológica traz riscos que precisam ser mitigados. O *function creep* como uso de dados para fins não declarados, amplia a vigilância e compromete a confiança. A discriminação e a vigilância política por algoritmos podem reforçar desigualdades ou viabilizar monitoramento indevido. O uso comercial indevido de dados sensíveis para fins mercadológicos sem consentimento informado constitui risco adicional relevante (Alshawii *et al.*, 2022).

Nesse contexto, a interoperabilidade é essencial à saúde digital, mas deve ser acompanhada de mecanismos éticos: transparência sobre quem acessa os dados e para quais finalidades, consentimento granular para maior controle do usuário e APIs seguras com protocolos que assegurem integridade e confidencialidade (Gonçalo *et al.*, 2025). O Quadro 1 sintetiza a comparação entre as duas abordagens.

**Quadro 1.** Comparativo: abordagem legalista versus abordagem centrada no humano

| **Aspecto** | **Abordagem legalista (normas e *compliance*)** | **Abordagem centrada no humano (ética *by design*)** |
|---|---|---|
| **Foco principal** | Cumprimento estrito das normas legais (LGPD, GDPR). | Respeito à dignidade, justiça e direitos fundamentais desde a concepção do sistema. |
| **Objetivo** | Evitar sanções jurídicas e garantir conformidade | Promover confiança social e reduzir riscos éticos, como |

| | | |
|---|---|---|
| | regulatória. | vieses e discriminação. |
| **Implementação** | Políticas de compliance, auditorias e relatórios de conformidade. | Integração de princípios éticos no ciclo de desenvolvimento (privacy by design, fairness by design). |
| **Benefícios** | Segurança jurídica, previsibilidade e padronização. | Maior aceitação social, transparência e fortalecimento da relação paciente-instituição. |
| **Limitações** | Pode ser burocrática e reativa, focada apenas em evitar penalidades. | Exige mudança cultural e investimento em educação digital e design inclusivo. |
| **Exemplo prático em saúde** | Implementação de consentimento formal em prontuários eletrônicos para atender à LGPD. | Interfaces inclusivas para idosos e leigos, com linguagem clara nas políticas de privacidade. |

**Fonte:** adaptado de Araújo; Campos (2025); Voigt; Von dem Bussche (2017).

A contraposição entre abordagens legalistas e centradas no humano, embora útil para fins analíticos, não deve ser interpretada como uma dicotomia excludente. A conformidade normativa constitui condição necessária, mas não suficiente, para a proteção efetiva em saúde digital.

A abordagem legalista, ao priorizar o cumprimento de requisitos formais, como a obtenção de consentimento documentado ou a elaboração de relatórios de impacto, tende a negligenciar as dimensões culturais e organizacionais que determinam a qualidade real da proteção. Uma instituição pode estar formalmente em conformidade com a LGPD e, ainda assim, manter práticas de

acesso excessivo, interfaces confusas e políticas de retenção inadequadas que comprometem a autodeterminação informativa dos pacientes.

A abordagem centrada no humano, por sua vez, encontra no conceito de *privacy by design* (PbD) seu principal referencial teórico e metodológico. Desenvolvido por Ann Cavoukian na década de 1990, o PbD propõe que a privacidade seja incorporada desde a concepção de sistemas e processos, e não tratada como um ajuste posterior . Seus sete princípios fundamentais: proatividade, privacidade como padrão, privacidade embutida no design, funcionalidade total, segurança de ponta a ponta, visibilidade e transparência, e respeito pela privacidade do usuário que oferecem um roteiro para a engenharia de sistemas de saúde que vai além da mera conformidade . No contexto brasileiro, a adoção do PbD é particularmente relevante porque a LGPD, embora não utilize explicitamente essa terminologia, incorpora seus elementos nos princípios da finalidade, necessidade, transparência e segurança (Brasil,2018)

A transposição do PbD para o ciclo de vida da informação em saúde digital implica decisões concretas em cada etapa. Na fase de conceção, trata-se de definir arquiteturas que limitem a coleta ao mínimo necessário e que estabeleçam, por padrão, os níveis mais elevados de proteção o que corresponde ao princípio da privacidade como padrão (*privacy by default*).

No desenvolvimento, a incorporação de *fairness by design* busca mitigar vieses algorítmicos que possam resultar em discriminação no acesso a cuidados ou na definição de prioridades clínicas. Na operação, a segurança de ponta a ponta exige criptografia em

repouso e em trânsito, autenticação multifator e monitoramento contínuo de acessos. No descarte, políticas de retenção e eliminação segura devem observar não apenas os prazos legais, mas também a minimização de dados residuais que possam ser reidentificados.

A interoperabilidade, condição indispensável para a continuidade do cuidado e para a eficiência dos sistemas de saúde, constitui um dos maiores desafios para a implementação de uma ética *by design*. APIs seguras, padrões abertos como o FHIR (*Fast Healthcare Interoperability Resources*) e mecanismos de consentimento granular são elementos técnicos que viabilizam a troca de informações sem comprometer a confidencialidade (Breda;Garibe, 2026).

Contudo, a interoperabilidade não é apenas um problema técnico: envolve decisões políticas sobre quem tem acesso a quais dados e para quais finalidades, bem como mecanismos de governança que assegurem a prestação de contas (*accountability*) em caso de uso indevido. A ausência de uma cultura de governança colaborativa entre prestadores, operadoras, plataformas tecnológicas e órgãos reguladores tende a produzir soluções fragmentadas que, embora tecnicamente funcionais, carecem de legitimidade ética (De Paula, 2026).

Por fim, a educação digital emerge como condição transversal para a efetividade de qualquer abordagem de engenharia. De pouco adianta projetar sistemas com os mais altos padrões de privacidade se os titulares não compreendem seus direitos ou não dispõem de letramento suficiente para exercê-los.

A literacia em proteção de dados no contexto da saúde não se limita à compreensão de termos de consentimento: envolve a capacidade de avaliar os riscos associados ao compartilhamento de informações, de identificar práticas abusivas e de exigir dos agentes de tratamento a transparência a que estão obrigados. Iniciativas de educação digital devem, portanto, ser concebidas como parte integrante do ciclo de vida da informação, e não como um apêndice comunicacional desvinculado das decisões técnicas e organizacionais.

## CONSIDERAÇÕES FINAIS

A ética e a segurança de dados constituem pilares indissociáveis da saúde digital. A LGPD representa avanço regulatório significativo no Brasil, mas sua efetividade depende da implementação prática de princípios como minimização, consentimento granular, interoperabilidade segura e educação digital. A análise comparativa entre abordagens legalistas e centradas no humano evidencia que a conformidade normativa, isoladamente, não responde aos riscos contemporâneos de vigilância, discriminação algorítmica e uso indevido de dados sensíveis.

A integração entre tecnologia e ética, desde a concepção dos sistemas até o descarte das informações, é condição para promover confiança, dignidade e equidade no tratamento de dados em saúde. Pesquisas futuras podem aprofundar a avaliação empírica de mecanismos de consentimento granular em prontuários eletrônicos e o impacto de iniciativas de literacia digital sobre a percepção de pacientes quanto à proteção de seus dados.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALSHAWII, A. *et al.* Data privacy during pandemics: a systematic literature review of COVID-19 smartphone applications. **PeerJ Computer Science,** v. 7, e826, 2022. DOI: 10.7717/peerj-cs.826.

ARAÚJO, A. S.; CAMPOS, R. F. Normativas destinadas ao uso ético e seguro da inteligência artificial na saúde. **Revista de Direito Sanitário,** v. 25, n. 1, 2025. DOI: 10.11606/issn.2316-9044.rdisan.2025.232489.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018a.

BRASIL. **Lei nº 13.787 de 27 de dezembro de 2018.** Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília, DF: Presidência da República, 2018b

BRASIL. Ministério da Saúde. **Estratégia de Saúde Digital para o Brasil 2020-2028.** Brasília, DF: Ministério da Saúde, 2020.

BREDA, LO; GARIBE, A. Tratamento de dados em saúde: bases legais, limites e boas práticas. **Migalhas,** 12 fev. 2026. Disponível em: https://www.migalhas.com.br/depeso/449916/tratamento-de-dados-em-saude-bases-legais-limites-e-boas-praticas. Acesso em: [13 novembro 2026].

CAVOUKIAN, A. *Privacy by Design*: The 7 Foundational Principles. **Toronto: Information and Privacy Commissioner of Ontario,** 2011. Disponível em: https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução CFM nº 1.821, de 11 de julho de 2007.** Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes. Brasília, DF: CFM, 2007.

DE PAULA, G. LGPD na saúde: prontuário, sigilo e direitos do paciente. **Migalhas,** 25 maio 2026. Disponível em: https://www.migalhas.com.br/depeso/456531/lgpd-na-saude-prontuario-sigilo-e-direitos-do-paciente. Acesso em: [13 novembro 2026].

FARIAS, Célio Ramos; ALMEIDA, Verônica Scriptore Freire e. Proteção de dados pessoais sensíveis na saúde digital: desafios jurídico-regulatórios da telemedicina e da inteligência artificial. **Cadernos Ibero-Americanos de Direito Sanitário,** Brasília, v. 15, n. 2, 2026.

FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics? **Philosophical Transactions of the Royal Society A,** London, v. 374, n. 2083, p. 20160360, 2016.

GONÇALO, W. *et al.* Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023. **Physics: Revista de Saúde Coletiva,** v. 35, n. 1, 2025. DOI: 10.1590/S0103-73312025350113pt.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Ethics and governance of artificial intelligence for health:** WHO guidance. Geneva: World Health Organization, 2021.

TAVARES, F.; OLIVEIRA, R. Data protection and digital health: challenges of LGPD implementation in Brazil. **Health Policy and**

**Technology,** v. 12, n. 3, 100754, 2023. DOI: 10.1016/j.hlpt.2023.100754.

VOIGT, P.; VON DEM BUSSCHE, A. The EU General Data Protection Regulation (GDPR): a practical guide. **Cham: Springer, 2017.** DOI: 10.1007/978-3-319-57959-7.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. **Harvard Law Review,** v. 4, n. 5, p. 193–220, 1890.

---

*O presente trabalho foi realizado com apoio do Programa de Educação pelo Trabalho para a Saúde (PET-Saúde: Informação e Saúde Digital) - Ministério da Saúde / Ministério da Educação (Brasil).*