Centro de Documentação e Pesquisa | OABRJ

A GOVERNABILIDADE ALGORÍTMICA NA SAÚDE: MAPEAMENTO DE RISCOS JURÍDICOS E ESTRATÉGIAS DE DEFESA NA ERA DA INTELIGÊNCIA ARTIFICIAL

ALGORITHMIC GOVERNANCE IN HEALTHCARE: MAPPING LEGAL RISKS AND DEFENSE STRATEGIES IN THE AGE OF ARTIFICIAL INTELLIGENCE

Gabriela Alves Guimarães[1] e Juliana Villaça[2]

---

[1] **Gabriela Alves Guimarães** é advogada, sócia da FourEthics Consultoria e *Outsourced CCO & Advisor* da World Post, com dual MBA pela FGV-BR e Ohio University/ USA, especialista em Regulação de Dados London School of Economics and Political Science, certificada pela SCCE/ USA como CCEP/ I – *Certified Compliance and Ethics Professional – International.* Atuou como *Compliance Officer* de multinacionais de ponta, tendo implementado ações corretivas e remediativas para adequação a acordos firmados com o governo norte-americano, além de ter trabalhado para a ONU (PNUD) como auditora de conformidade na Rio+20, evento do qual resultou a Agenda 2030. Como consultora, coordenou investigações corporativas para casos emblemáticos, além de ter concebido e implementado Programas de *Compliance* no Brasil e no exterior. Gabriela é também membro do Comitê Técnico que criou a DSC: 10.000, Auditora Líder Sistema de Gestão Antissuborno, Palestrante e autora de diversos artigos, dentre eles para os livros ESG: O Cisne Verde e o Capitalismo de Stakeholder e Doze Leis de Combate à Corrupção- Hércules em terras brasileiras.

[2] Juliana Villaça é advogada, formada na Universidade Católica de Minas Gerais e pós-graduada em Direito do Trabalho e Processual do Trabalho pela Faculdade Arnaldo. Com mais de 12 anos de experiência como advogada *in house* e consultora jurídica, compliance e governança, Juliana tem larga experiência nas indústrias da construção civil e química, também no atendimento de holdings não financeiras, particularmente nas diligências pré-investimento. Como consultora da FourEthics Consultoria, Juliana tem assistido diversas empresas em investigações corporativas e no aprimoramento das práticas de governança e compliance. Membro da Comissão de Direito Digital, Empresarial, Tributário e Compliance do Instituto dos Advogados Brasileiros (IAB) e da Comissão de Direito Digital da OAB/MG. Autora de artigos publicados em revistas jurídicas nacionais e internacionais nas áreas de compliance, ESG e direito digital.

RESUMO

A crescente inserção da Inteligência Artificial (IA) no setor de saúde inaugura uma nova fronteira de desafios para o Direito. O presente artigo tem por objetivo analisar, sob uma perspectiva crítica e multidisciplinar, os principais riscos jurídicos decorrentes dessa transformação digital. A partir da avaliação de vetores como a qualidade e o viés das bases de dados, a opacidade dos investimentos do setor privado, as ameaças à privacidade e a possível precarização da relação médico-paciente, o estudo examina a adequação do arcabouço normativo brasileiro — incluindo a Lei Geral de Proteção de Dados (LGPD), o Código de Defesa do Consumidor (CDC), o Código Civil,o Projeto de Lei n° 2.338/2023 e a Resolução CFM nº 2.454/2026, que normatiza o uso de IA na medicina — a essas novas realidades. Propõe-se, ao final, um mapeamento das estratégias de atuação para os operadores do Direito na defesa dos diferentes agentes da cadeia de saúde: pacientes, profissionais, instituições e desenvolvedores de tecnologia, contribuindo para o debate sobre a necessária governança ética e legal dos sistemas autônomos na medicina.

Palavras-chave: Inteligência Artificial. Direito da Saúde. Responsabilidade Civil. Proteção de Dados. LGPD. Governança Algorítmica.

ABSTRACT

The increasing integration of Artificial Intelligence (AI) in the healthcare sector introduces a new frontier of challenges for Law. This article aims to analyze, from a critical and multidisciplinary perspective, the main legal risks arising from this digital transformation. By evaluating factors such as the quality and bias of databases, the opacity of private sector investments, threats to privacy, and the potential deterioration of the doctor-patient relationship, the study examines the adequacy of the Brazilian legal framework — including the General Data Protection Law (LGPD), the Consumer Defense Code (CDC), the Civil Code, Bill No. 2,338/2023 and CFM Resolution No. 2,454/2026, which sets ethical-professional rules for the use of AI in medical practice—

to these new realities. Finally, it proposes a mapping of strategies for legal practitioners in defending the different agents in the healthcare chain: patients, professionals, institutions, and technology developers, contributing to the debate on the necessary ethical and legal governance of autonomous systems in medicine.

Keywords: Artificial Intelligence. Health Law. Civil Liability. Data Protection. LGPD. Algorithmic Governance.

SUMÁRIO

1 INTRODUÇÃO; 2 O ECOSSISTEMA DIGITAL DA SAÚDE: ENTRE A PROMESSA DE EFICIÊNCIA E A REALIDADE DOS RISCOS; 2.1 A Falibilidade dos Algoritmos: Vieses, Opacidade e a Questão da Responsabilidade Civil; 2.2 Assimetria de Informação e Conflitos de Interesse: As Parcerias Estratégicas das *Big Pharmas*; 2.3 O SUS na Encruzilhada Digital: Terceirização, Agendas Ocultas e o Direito Fundamental à Saúde; 2.4 Dados como Ativo: A Mercantilização da Informação e a Precificação de Riscos; 3 OS SUJEITOS DA RELAÇÃO JURÍDICA NA ERA DOS SISTEMAS AUTÔNOMOS; 3.1 O Paciente-Usuário: Da Hipervulnerabilidade ao Direito à Explicação; 3.2 O Profissional de Saúde (HCP): Autonomia, Viés de Automação e Dever de Vigilância; 3.3 O Estabelecimento Assistencial e o Adquirente da Tecnologia: Compliance e Responsabilidade Solidária; 3.4 O Desenvolvedor e o Fornecedor de IA: Dever de Segurança e Alocação de Riscos; 4 O ARCABOUÇO NORMATIVO E A REGULAÇÃO EM CONSTRUÇÃO; 4.1 A LGPD e a Tutela dos Dados Sensíveis de Saúde; 4.2 O CDC e a Tutela do Paciente-Consumidor na Saúde Suplementar; 4.3 O PL n° 2.338/2023 e a Classificação de Risco dos Sistemas de IA na Saúde; 4.4. A Resolução CFM nº 2.454/2026 como marco setorial ético-profissional; 5 O PAPEL DO ADVOGADO NA GOVERNANÇA DA SAÚDE DIGITAL: PREVENÇÃO, LITIGIO E ESTRATÉGIA; 6 CONCLUSÃO: POR UMA SAÚDE DIGITAL CENTRADA NA PESSOA HUMANA; REFERÊNCIAS.

1. INTRODUÇÃO

A intersecção entre a inteligência artificial (IA) e o setor de saúde tem sido apresentada como uma das mais promissoras fronteiras da inovação. De algoritmos capazes de diagnosticar doenças com precisão sobre-humana a sistemas preditivos que personalizam tratamentos, a promessa é de uma medicina mais eficiente, precisa e acessível. Paralelamente, no entanto, essa revolução silenciosa carrega consigo um espectro de riscos jurídicos, éticos e sociais que desafiam as estruturas tradicionais do Direito.

No Brasil, a incorporação tecnológica avança em um cenário de relativa vacuidade legislativa específica, onde normas setoriais, resoluções de conselhos de classe e a interpretação analógica de diplomas gerais, como o Código Civil, o Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados (LGPD),tentam dar conta de conflitos para os quais não foram originalmente concebidos. Assim, questões fundamentais emergem: a quem imputar responsabilidade quando um diagnóstico algorítmico falha? Como assegurar que os dados de saúde, agora transformados em ativo valioso, não sejam utilizados para discriminação ou precificação abusiva? Qual o limite ético da interação homem-máquina em um campo historicamente ancorado no humanismo e na confiança?

Este artigo se propõe a investigar essas questões e a mapear os riscos jurídicos inerentes à aplicação da IA na saúde, analisando-os à luz do ordenamento jurídico pátrio e dos projetos de lei em tramitação. Mais do que uma análise diagnóstica, busca-se oferecer um guia para a atuação estratégica do advogado, considerando os distintos polos da relação: o paciente (hiper)vulnerável, o profissional de saúde diante do viés de automação, o estabelecimento hospitalar adquirente de tecnologia e o desenvolvedor do sistema.

Para tanto, a pesquisa estrutura-se em uma abordagem dedutiva, partindo da contextualização do ecossistema digital da saúde e seus riscos inerentes, passando pela análise dos sujeitos envolvidos e do arcabouço normativo aplicável, para, ao final, delinear o papel do advogado na governança dessa nova realidade. A conclusão, longe de pretender esgotar o debate, almeja ser um convite à reflexão sobre a necessidade

premente de uma governança algorítmica centrada na pessoa humana, que coloque a tecnologia a serviço da vida e da dignidade, e não o contrário.

2. O ECOSSISTEMA DIGITAL DA SAÚDE: ENTRE A PROMESSA DE EFICIÊNCIA E A REALIDADE DOS RISCOS

A transformação digital na saúde é um fenômeno multifacetado que transcende a mera digitalização de prontuários. Envolve a criação de um ecossistema complexo onde interagem dispositivos vestíveis (gadgets), plataformas de telemedicina, sistemas de apoio à decisão clínica baseados em aprendizado de máquina e robustas redes de interoperabilidade de dados. No epicentro dessa revolução, a IA desponta como a grande protagonista, mas também como a fonte de novos e complexos riscos.

2.1 A Falibilidade dos Algoritmos: Vieses, Opacidade e a Questão da Responsabilidade Civil

O primeiro e talvez mais fundamental risco reside na própria arquitetura da IA. Sistemas inteligentes são treinados a partir de grandes volumes de dados (*big data*). A assertividade de um diagnóstico ou recomendação, portanto, está diretamente condicionada à qualidade, representatividade e imparcialidade da base de dados que os alimenta. Como alertam especialistas, a utilização de bases de dados enviesadas, por exemplo, sub-representando grupos raciais, de gênero ou socioeconômicos,pode perpetuar e até amplificar desigualdades históricas, gerando o que se convencionou chamar de "discriminação algorítmica". Um algoritmo treinado majoritariamente com dados de pacientes de um determinado perfil pode ser significativamente menos preciso ao diagnosticar doenças em populações não representadas, criando uma medicina de duas velocidades e violando o princípio constitucional da equidade no acesso à saúde (art. 196, CF/88).

A essa problemática soma-se a opacidade característica de muitos modelos de IA, especialmente os de aprendizado profundo (*deep learning*). O fenômeno conhecido

como "caixa-preta" algorítmica torna praticamente impossível, até mesmo para seus criadores, rastrear o iter lógico que levou a uma determinada conclusão [Santaella, 2023]. Essa falta de transparência ou "explicabilidade" coloca em xeque institutos jurídicos basilares, como o dever de informação e o consentimento informado. Como pode um médico validar ou contestar uma recomendação cujo fundamento ele não consegue compreender? Como pode um paciente consentir de forma livre e esclarecida se não lhe são apresentados, de forma inteligível, os riscos e limites da tecnologia empregada?

Diante de um erro diagnóstico ou terapêutico mediado por IA, a questão da responsabilidade civil se impõe com especial dramaticidade. O Código Civil, em seu art. 927, caput, e parágrafo único, estabelece a obrigação de reparar o dano, fundada na culpa (responsabilidade subjetiva) ou, nos casos especificados em lei ou quando a atividade normalmente implicar risco, independentemente de culpa (responsabilidade objetiva). No campo da saúde, tradicionalmente se entende que a responsabilidade do médico é subjetiva, baseada na culpa provada (negligência, imprudência ou imperícia), enquanto a dos hospitais e planos de saúde tende a ser objetiva, na qualidade de fornecedores de serviços, nos termos do art. 14 do CDC [Bonna; Sá, 2021].

No entanto, a cadeia de agentes se alonga com a introdução da IA. A quem imputar o dano: ao desenvolvedor do *software*, que pode ter criado um algoritmo “defeituoso”? Ao estabelecimento de saúde que adquiriu e implementou a tecnologia? Ao médico que, confiando no sistema (viés de automação), deixou de realizar uma checagem crítica que detectaria o erro? Ou a todos de forma solidária?

A doutrina tem se debruçado sobre o tema. Nagaroli (2023) argumenta que a mera utilização da IA não altera, por si só, a natureza da obrigação médica, que permanece sendo de meio. O médico não se obriga a curar, mas a empregar todos os conhecimentos e técnicas disponíveis em prol do paciente. Contudo, o dever de conduta do profissional é alargado, passando a incluir a necessidade de compreender as limitações da ferramenta que utiliza, de supervisionar seus *outputs* e de agir como um "filtro crítico" entre a recomendação algorítmica e a decisão clínica final [Marinangelo, 2025]. Com a publicação da Resolução CFM nº 2.454/2026 (DOU 27 fev. 2026; vigência após 180 dias), o Conselho Federal de Medicina positivou que a IA deve ser empregada exclusivamente como ferramenta de apoio, mantendo o médico como responsável final pelas decisões clínicas, diagnósticas, terapêuticas e prognósticas (art. 4º, I), e vedou a

delegação à IA da comunicação de diagnósticos, prognósticos ou decisões terapêuticas ao paciente sem a devida mediação humana (art. 5º, §2º). A norma ainda impõe o registro do uso de IA no prontuário (art. 4º, V) e assegura o direito do paciente à informação clara e acessível quando a IA for utilizada como apoio relevante (art. 5º, §1º; art. 11), reforçando o dever de vigilância crítica e a centralidade da relação médico- paciente.

Paralelamente, os desenvolvedores e fornecedores de sistemas de IA, como fabricantes de produtos ou fornecedores de serviços, podem ser enquadrados na responsabilidade objetiva do CDC (art. 12 e 14) pelo defeito no produto ou serviço que oferecem Legale Educacional, 2025]. A grande dificuldade reside, contudo, na prova do defeito e do nexo causal em sistemas complexos e autorreguláveis. É nesse contexto que se insere a discussão sobre a necessidade de um regime específico de responsabilidade para sistemas de IA, como o que se desenha no Projeto de Lei n° 2.338/2023.

2.2 Assimetria de Informação e Conflitos de Interesse: As Parcerias Estratégicas das *Big Pharmas*

Um segundo vetor de risco, menos discutido, mas igualmente crucial, diz respeito à assimetria de informação e aos potenciais conflitos de interesse que permeiam as parcerias estratégicas no setor. As grandes farmacêuticas têm realizado vultosos investimentos na aquisição ou no desenvolvimento de plataformas de IA, como ilustram os casos da AstraZeneca adquirindo a Modella AI e da parceria entre Nvidia e Eli Lilly [Terra, 2024; Times Brasil, 2025].

Se, por um lado, tais alianças prometem acelerar a pesquisa e o desenvolvimento de novos fármacos, por outro, levantam sérias questões sobre a privacidade dos dados e a lisura das futuras recomendações médicas. Os dados de saúde, especialmente aqueles em larga escala, são o "petróleo" da economia digital. Ao firmarem parcerias com gigantes da tecnologia, as farmacêuticas obtêm acesso a um vasto repositório de informações clínicas que podem ser utilizadas para treinar seus algoritmos, não apenas para a descoberta de medicamentos, mas também para direcionar estratégias de marketing e vendas de forma (hiper)personalizada e potencialmente manipuladora.

O histórico do setor farmacêutico, marcado por escândalos de corrupção de médicos e campanhas de promoção conflituosas, acende um alerta vermelho. Um sistema de IA treinado para recomendar tratamentos pode, deliberadamente ou não, privilegiar os medicamentos de seu parceiro comercial, em detrimento de opções mais baratas, eficazes ou adequadas ao perfil do paciente. Trata-se de uma forma sofisticada e de difícil detecção de conflito de interesses, que opera na camada profunda do código, longe do olhar fiscalizatório do paciente ou mesmo do médico prescritor.

Exemplo paradigmático dessa tendência é a recente parceria firmada no estado de Utah (EUA) com a empresa Doctronic, permitindo que pacientes solicitem a renovação de prescrições médicas por meio de um agente de IA, sem a intervenção humana direta [Utah, 2026]. Ainda que a iniciativa alegue aumentar o acesso e a eficiência, ela inaugura um precedente perigoso ao delegar a uma máquina um ato privativo do médico, com potenciais repercussões sobre a segurança do paciente e a relação de confiança que permeia a prescrição. No Brasil, nos termos da recente Resolução CFM nº 2.454/2026, referida delegação integral a sistemas automatizados contrasta com a diretriz de supervisão humana obrigatória (art. 15, parágrafo único) e com a regra de que a decisão sobre prescrição e demais atos médicos cabe sempre ao médico (art. 18, §2º), preservando-se a mediação humana na comunicação clínica (art. 5º, §2º).

2.3 O SUS na Encruzilhada Digital: Terceirização, Agendas Ocultas e o Direito Fundamental à Saúde

O Sistema Único de Saúde (SUS), pilar do direito fundamental à saúde no Brasil (art. 196, CF/88), não está imune a essa onda de transformação digital. Iniciativas como a implantação de quiosques médicos com IA na China, que prometem diagnósticos rápidos com alta precisão, acendem o debate sobre a potencial adoção de modelos semelhantes no país como forma de desafogar o sistema e reduzir custos [Click Petróleo e Gás, 2026].

No entanto, essa possibilidade esconde riscos substanciais. O primeiro é o da "terceirização" disfarçada da saúde pública. A aquisição de soluções privadas de IA pode, na prática, transferir para empresas particulares o controle sobre decisões clínicas

essenciais, fragilizando a gestão pública e criando uma dependência tecnológica de difícil reversão. O Estado, ao invés de prover diretamente a saúde, converter-se-ia em mero comprador de serviços diagnósticos de conglomerados de tecnologia, o que levanta questões sobre a efetividade do comando constitucional que impõe ao Poder Público o dever de organizar e executar diretamente as ações e serviços de saúde (art. 197, CF/88).

Um segundo risco, ainda mais sombrio, é o do uso dos dados de saúde dos cidadãos para "agendas governamentais ocultas". A recente operação da Polícia Federal que investiga a venda ilegal de dados de pacientes do SUS demonstra, na prática, a vulnerabilidade dessas informações e seu valor comercial [G1, 2026]. A integração de sistemas de IA ao SUS, por meio da Rede Nacional de Dados em Saúde (RNDS), amplia exponencialmente a capacidade de coleta, processamento e compartilhamento dessas informações [Decreto nº 12.560/ 2025].

Em um contexto de retrocessos democráticos e tentativas de controle populacional, como revelam documentos sobre políticas de controle de natalidade [Brasil Paralelo, 2026], a existência de uma base de dados de saúde unificada e analisada por IA pode se tornar um instrumento de biopoder nas mãos do Estado. A tecnologia, que deveria servir para qualificar a gestão e melhorar o atendimento, pode ser desvirtuada para finalidades escusas de vigilância, discriminação ou engenharia social, em clara afronta aos direitos fundamentais e à dignidade da pessoa humana.

2.4 Dados como Ativo: A Mercantilização da Informação e a Precificação de Riscos

A centralidade dos dados na nova economia da saúde transformou-os no ativo mais valioso do setor. O aumento do comércio, inclusive clandestino, de informações de saúde já é uma realidade preocupante [AMB, 2023; MedicinaSA, 2023]. Esse mercado, alimentado pelo crescimento da telemedicina e pela multiplicação de *gadgets* de saúde, opera frequentemente à margem da legalidade e da transparência.

Um dos usos mais controversos desses dados é a sua aplicação na precificação de riscos pelas operadoras de planos de saúde. Dados coletados por pulseiras inteligentes,

relógios e outros dispositivos vestíveis, quando compartilhados sem a devida transparência com o usuário, podem ser utilizados para criar perfis de risco detalhados, influenciando não apenas o valor das mensalidades futuras, mas também, a própria possibilidade de contratação ou renovação do plano [Estadão, 2026; UOL, 2026].

Embora a Lei nº 9.656/98 vede a recusa de adesão com base em doenças ou lesões preexistentes, permitindo apenas a imposição de Cobertura Parcial Temporária (CPT), a análise preditiva baseada em IA pode identificar padrões de comportamento (sedentarismo, hábitos alimentares, padrões de sono) que, embora não configurem doenças, são utilizados como proxies para estimar o risco futuro de adoecimento. Isso abre uma perigosa fronteira para a discriminação atuarial, onde o acesso à saúde pode ser condicionado não por aquilo que o paciente é, mas pelo que o algoritmo prevê que ele será.

A ausência de transparência sobre como esses dados são coletados, tratados e compartilhados, especialmente na integração entre diferentes sistemas (hospitais, laboratórios, aplicativos de bem-estar), viola frontalmente os princípios da finalidade, adequação e necessidade previstos na LGPD (arts. 6º e 11), além de comprometer a confiança que deve nortear as relações de consumo e, sobretudo, as relações de cuidado em saúde.

3. OS SUJEITOS DA RELAÇÃO JURÍDICA NA ERA DOS SISTEMAS AUTÔNOMOS

A complexificação do ecossistema de saúde digital impõe uma releitura do papel de cada ator envolvido na cadeia de cuidado. A tradicional relação dual médico-paciente cede espaço a uma teia de interações que inclui hospitais, operadoras de planos de saúde, fornecedores de tecnologia e desenvolvedores de algoritmos. Compreender as novas responsabilidades e vulnerabilidades de cada um desses sujeitos é condição essencial para uma atuação jurídica efetiva.

3.1 O Paciente-Usuário: Da Hipervulnerabilidade ao Direito à Explicação

O paciente, parte historicamente vulnerável na relação de saúde, vê sua posição agravada no ambiente digital. Sobre a vulnerabilidade técnica e informacional inerente ao leigo, soma-se agora a "hipervulnerabilidade algorítmica". O paciente não apenas desconhece a medicina, mas também ignora por completo o funcionamento, os critérios e os vieses do sistema de IA que participa de seu diagnóstico ou tratamento.

Em defesa do paciente, o advogado deve manejar um arsenal jurídico que vai além da tradição reparatória. A atuação preventiva é fundamental, assegurando que o consentimento informado seja, de fato, livre e esclarecido. Isso implica exigir que os termos de consentimento, nos termos do art. 11, I, da LGPD e do art. 6º, III, do CDC, detalhem de forma acessível a participação da IA no ato médico, seus riscos, limitações e, sobretudo, a possibilidade de o paciente optar por uma avaliação exclusivamente humana (direito de oposição).

No contencioso, o advogado deve estar apto a litigar com base na teoria da perda de uma chance, quando a omissão na utilização de uma ferramenta de IA ou a confiança acrítica em seu resultado privar o paciente de uma oportunidade de cura ou melhora [Uscocovich; Santos, 2023]. Além disso, a defesa do direito à explicação (*right to explanation*), ainda que não expresso na lei brasileira, pode ser extraída dos princípios da transparência e da boa-fé objetiva (art. 422 do Código Civil) e do dever de informação qualificada do CDC, impondo aos fornecedores o ônus de demonstrar a lógica subjacente à decisão algorítmica que afetou o paciente.

3.2 O Profissional de Saúde (HCP): Autonomia, Viés de Automação e Dever de Vigilância

O profissional de saúde (em inglês, denominado *HCP- Health Care Professional*) encontra-se na posição mais delicada do novo ecossistema. Ele é, a um só tempo, usuário da tecnologia e seu “fiador” perante o paciente. A autonomia profissional, garantida pelo Código de Ética Médica, é desafiada pela introdução de sistemas que podem sugerir, com alta dose de persuasão, determinados diagnósticos ou condutas.

O principal risco a que está exposto é o chamado "viés de automação" (*automation bias*), uma tendência cognitiva do ser humano a confiar excessivamente nos *outputs* gerados por sistemas automatizados, relaxando seu próprio senso crítico e vigilância [Facchini Neto; Barbosa, 2023]. Um médico que recebe uma sugestão diagnóstica de um *software* "revolucionário" pode se sentir inclinado a aceitá-la sem a devida verificação, especialmente em contextos de sobrecarga de trabalho, ainda que oCFM tenha recentemente reforçado os deveres no plano ético-profissional, quais sejam: (i) a IA é instrumento de apoio, permanecendo o médico como responsável final pelas decisões (art. 4º, I); (ii) é obrigatório exercer julgamento crítico sobre recomendações algorítmicas (art. 4º, II) e manter-se atualizado sobre limitações, riscos e vieses (art. 4º, III); (iii) o uso de IA como apoio à decisão deve ser registrado no prontuário (art. 4º, V); e (iv) o médico pode recusar sistemas sem validação científica adequada ou certificação regulatória pertinente (art. 3º, III), preservando sua autonomia (art. 3º, IV; art. 18, §1º).

Juridicamente, essa conduta pode configurar imperícia. O dever de cuidado do profissional se expande, passando a incluir a obrigação de conhecer as limitações da ferramenta que utiliza e de exercer um juízo crítico e autônomo sobre suas recomendações. Como bem sintetizam Kfouri Neto e Nagaroli (2025), o médico não pode se eximir de sua responsabilidade delegando a decisão a um algoritmo; sua função é justamente a de ser o "humano no *loop*", o responsável por validar, contextualizar e, se necessário, contestar a "consulta robótica".

Na defesa do profissional, o advogado deve atuar preventivamente na elaboração de protocolos claros que delimitem o uso da IA e na capacitação contínua da equipe para mitigar o viés de automação. No contencioso, a linha de defesa poderá envolver a demonstração de que o erro decorreu de um defeito no sistema (culpa do desenvolvedor) e não de uma falha no dever de vigilância, ou que, mesmo agindo com a diligência esperada, o dano era imprevisível e inevitável (caso fortuito ou força maior), rompendo o nexo causal.

3.3 O Estabelecimento Assistencial e o Adquirente da Tecnologia: Compliance e Responsabilidade Solidária

Hospitais, clínicas, laboratórios e demais estabelecimentos de saúde, ao adquirirem e implementarem sistemas de IA, assumem um papel central na gestão dos riscos. Sendo que, como fornecedores de serviços, respondem objetivamente pelos danos causados aos pacientes, independentemente de culpa, nos termos do art. 14 do CDC, podendo ser responsabilizados de forma solidária com o profissional ou o desenvolvedor.

Para mitigar esse risco, a atuação do advogado na assessoria preventiva é crucial. Isso envolve a elaboração de contratos robustos com os fornecedores de tecnologia, com cláusulas claras de garantia, responsabilidade, sigilo e confidencialidade, além de previsão de auditoria e verificação da segurança e transparência dos algoritmos. A adoção de um Programa de *Compliance* em IA, que inclua a criação de um comitê de ética digital, a realização de *due diligence* tecnológica prévia à aquisição e a implementação de protocolos de uso e supervisão humana, é medida que se impõe para demonstrar a boa-fé e a adoção das cautelas necessárias.

A Resolução CFM nº 2.454/2026 reforça essa agenda ao exigir que instituições que desenvolvam ou utilizem IA realizem avaliação preliminar para definição do grau de risco (art. 12) e informem a categorização (art. 13), além de estabelecer processos internos de governança (art. 14) e, quando houver adoção de sistemas próprios, criar Comissão de IA e Telemedicina sob coordenação médica e subordinada à diretoria técnica (art. 14, parágrafo único). Também prevê a implementação de mecanismos de auditoria especializada e monitoramento contínuos (art. 9º, §2º).

Ainda na esfera preventiva, o advogado deve orientar o estabelecimento sobre a obrigatoriedade de manter um registro detalhado (*data paper trail*) de todas as decisões assistidas por IA, permitindo a rastreabilidade e a futura investigação de eventuais falhas. A transparência com o paciente sobre o uso dessas tecnologias, inclusive por meio de informações claras nos sites e materiais institucionais, é outro pilar da estratégia de mitigação de riscos reputacionais e jurídicos.

3.4 O Desenvolvedor e o Fornecedor de IA: Dever de Segurança e Alocação de Riscos

Os desenvolvedores e fornecedores de sistemas de IA, como criadores da tecnologia, ocupam a base da cadeia de riscos. Sua responsabilidade, enquadrável na órbita do CDC (arts. 12 e 18) por vício do produto ou serviço, é objetiva. Não se trata de discutir se agiram com culpa, mas sim se o sistema que colocaram no mercado apresenta defeito de concepção, de segurança ou de informação.

Na defesa desse polo, o advogado deve atuar intensamente na fase de concepção e treinamento do algoritmo. É fundamental documentar todo o processo, demonstrando a adoção das melhores práticas de engenharia, a busca por bases de dados representativas e não enviesadas e a realização de testes rigorosos de segurança e eficácia. A implementação de mecanismos de explicabilidade, ainda que imperfeitos, é um diferencial competitivo e uma prova de boa-fé.

O PL n° 2.338/2023 (em tramitação na Casa Revisora), ao classificar a saúde como área de alto risco, imporá obrigações adicionais, como a elaboração de relatórios de impacto algorítmico e a adoção de medidas de governança [Abramed, 2025]. O advogado terá um papel-chave na interpretação dessa nova regulação e na adequação dos produtos aos seus ditames. A negociação contratual com os adquirentes também é estratégica, buscando delimitar claramente o escopo da responsabilidade do fornecedor, excluindo, por exemplo, danos decorrentes de usos não previstos, de má utilização por parte do profissional ou de customizações realizadas pelo adquirente que alterem o funcionamento original do sistema.

4. O ARCABOUÇO NORMATIVO E A REGULAÇÃO EM CONSTRUÇÃO

A resposta do ordenamento jurídico brasileiro aos desafios impostos pela IA na saúde é, até o momento, fragmentária e baseada na aplicação analógica de normas gerais. No entanto, um novo marco regulatório está em gestação e promete alterar significativamente esse cenário.

4.1 A LGPD e a Tutela dos Dados Sensíveis de Saúde

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) é, indubitavelmente, o principal instrumento de tutela dos direitos dos titulares de dados no ambiente digital. Ao classificar os dados de saúde como "dados pessoais sensíveis" (art. 5º, II), a LGPD lhes confere uma proteção qualificada, estabelecendo hipóteses mais restritas para o seu tratamento.

O art. 11 da lei determina que o tratamento de dados sensíveis só pode ocorrer quando o titular ou seu responsável legal consentir de forma específica e destacada, para finalidades determinadas, ou nas hipóteses em que for imprescindível para a tutela da saúde, em procedimento realizado por profissionais da área ou por entidades sanitárias. A "tutela da saúde", contudo, não pode ser interpretada como uma carta branca para o uso indiscriminado de dados. A finalidade deve ser estritamente vinculada ao cuidado assistencial, não se confundindo com pesquisas de mercado, perfilamento comportamental ou precificação de riscos, que exigiriam consentimento específico.

A aplicação da LGPD ao setor de saúde impõe, na prática, a necessidade de revisão de todos os fluxos de informação. A tokenização de dados, técnica que substitui informações sensíveis por um identificador não significativo (*token*), surge como uma ferramenta promissora para viabilizar o compartilhamento seguro e a interoperabilidade sem expor os dados reais [IBM, 2025]. Iniciativas como a Rede Nacional de Dados em Saúde (RNDS) e a parceria InovaHC-B3 para o OpenCare Interop demonstram a relevância da tokenização na construção de um ecossistema de dados mais seguro e centrado no paciente [Gov.br, 2025; B3, 2025].

4.2 O CDC e a Tutela do Paciente-Consumidor na Saúde Suplementar

A aplicação do Código de Defesa do Consumidor às relações entre pacientes e planos de saúde é pacífica na jurisprudência do Superior Tribunal de Justiça (STJ), conforme a Súmula 608. O CDC também se aplica, em regra, às relações entre pacientes e hospitais particulares, configurando uma típica relação de consumo, salvo nas hipóteses de atendimento custeado pelo SUS, onde prevalece o regime de direito público [STJ, 2020].

Isso significa que o paciente-usuário da saúde suplementar é legalmente um consumidor, com todos os direitos daí decorrentes, incluindo a proteção contra publicidade enganosa e abusiva (que pode ser a base para coibir o marketing enganoso de "IA infalíveis"), o direito à informação clara e adequada sobre os serviços contratados e a responsabilidade objetiva dos fornecedores.

A introdução da IA, portanto, deve ser analisada sob as lentes do CDC; assim, uma negativa de cobertura baseada em um parecer emitido por um sistema de IA pode ser contestada com base no dever de fundamentação e transparência, sendo a decisão automatizada e não revisada por humano potencialmente abusiva, por violar o direito à informação e à ampla justificação. Da mesma forma, o uso de dados de saúde para majorar mensalidades ou criar barreiras de acesso, sem o consentimento livre e esclarecido, configura prática abusiva nos termos do art. 39 do CDC.

4.3 O PL n° 2.338/2023 e a Classificação de Risco dos Sistemas de IA na Saúde

Após intensos debates no Senado Federal, o Projeto de Lei n° 2.338/2023, de autoria do Senador Rodrigo Pacheco, foi aprovado e encaminhado à Câmara dos Deputados em março de 2025, onde tramita como apensado a outras proposições [Senado Federal, 2023; Câmara dos Deputados, 2025]. O projeto estabelece o marco legal para o desenvolvimento e uso da inteligência artificial no Brasil, com base na centralidade da pessoa humana e na proteção de direitos fundamentais.

Para o setor de saúde, a classificação dos sistemas de IA como de "alto risco" é um dos pontos mais sensíveis. O projeto original prevê que sistemas utilizados em "serviços essenciais, como saúde, segurança e educação" sejam submetidos a um regime mais rigoroso de avaliação e controle, incluindo a obrigatoriedade de realização de avaliação de impacto algorítmico, documentação detalhada e medidas de transparência e explicabilidade.

A Associação Brasileira de Medicina Diagnóstica (Abramed) tem alertado para o risco de que essa classificação genérica, sem considerar as particularidades de cada aplicação, possa engessar a inovação e inibir investimentos, sem necessariamente aumentar a segurança do paciente [Abramed, 2025]. O setor defende que a regulação seja

proporcional ao risco efetivo, evitando-se a aplicação do mesmo rigor a um sistema de apoio à triagem administrativa e a um algoritmo de diagnóstico oncológico.

Outro ponto crucial do PL é a definição da responsabilidade civil. O setor de saúde, por meio da Abramed, tem alertado para a necessidade de o texto legal diferenciar as responsabilidades dos diversos agentes da cadeia, evitando que o desenvolvedor que tenha agido com transparência e seguido procedimentos adequados seja responsabilizado por usos indevidos ou imprevisíveis de sua tecnologia na ponta. Defende-se, assim, uma responsabilização proporcional, que recaia sobre quem efetivamente exerce controle sobre o sistema.

A definição da autoridade competente para fiscalizar e regular a IA no Brasil também foi objeto de importantes ajustes. Em dezembro de 2025, o governo federal encaminhou projeto que estabelece a ANPD como autoridade responsável por coordenar o sistema e editar normas gerais, mas consolida a competência das autoridades setoriais, como a Anvisa e a ANS, para regular e fiscalizar a IA em seus respectivos segmentos, reconhecendo seu conhecimento técnico específico.

4.4 A Resolução CFM nº 2.454/2026 como marco setorial ético-profissional

A publicação da Resolução CFM nº 2.454/2026 consolida, no plano ético-profissional, um conjunto de deveres e direitos que impacta diretamente a governança algorítmica na saúde. A norma define conceitos (modelos, sistemas e aplicações de IA) e estrutura obrigações ao longo do ciclo de vida das soluções (art. 9º, §1º; Anexo I), além de classificar os sistemas por grau de risco (baixo, médio, alto e inaceitável), condicionando auditoria e monitoramento à proporcionalidade do impacto (art. 1º, §2º; arts. 12–13). No núcleo da disciplina, afirma-se a supervisão humana obrigatória (art. 15, parágrafo único) e a preservação da autonomia do médico para acolher ou rejeitar recomendações (art. 3º, IV; art. 18, §2º), bem como o dever de informar o paciente quando a IA for utilizada como apoio relevante (art. 5º, §1º; art. 11), com vedação de comunicação automatizada de diagnósticos ou decisões terapêuticas (art. 5º, §2º). No tocante a dados, exige-se observância rigorosa da LGPD e padrões mínimos de segurança compatíveis com dados sensíveis (art. 6º, §3º; arts. 16–17), reforçando a interseção entre ética médica e proteção de dados no desenho de sistemas de saúde digital.

5 O PAPEL DO ADVOGADO NA GOVERNANÇA DA SAÚDE DIGITAL: PREVENÇÃO, LITÍGIO E ESTRATÉGIA

A complexidade do cenário descrito impõe ao advogado que atua na área da saúde uma necessária reinvenção. O profissional do Direito não pode mais se limitar à propositura de ações reparatórias ou à defesa em processos ético-profissionais: sua atuação deve ser ampliada para abarcar a consultoria preventiva e a governança estratégica da tecnologia no ambiente de saúde. Na defesa dos pacientes, o advogado deve: Atuar na esfera extrajudicial, exigindo das operadoras e hospitais informações claras sobre o uso de IA nos processos decisórios que afetam o paciente;

· Manejar ações judiciais com pedidos de produção antecipada de provas para desvendar a lógica de algoritmos que embasaram negativas de cobertura ou diagnósticos questionáveis, com fundamento no direito à explicação;

· Pleitear indenizações por danos morais e materiais, explorando a teoria da perda de uma chance e a responsabilidade objetiva dos fornecedores, sempre que o uso da IA estiver na origem do dano.

Na assessoria a desenvolvedores de tecnologia, o advogado deve:

· Orientar sobre a adequação à LGPD desde a fase de concepção do produto (*privacy by design*), assegurando que o tratamento de dados tenha base legal e seja transparente;

· Realizar a *due diligence* jurídica das bases de dados utilizadas no treinamento dos algoritmos, prevenindo riscos de violação de direitos autorais e de uso de dados ilegítimos;

· Elaborar contratos de licenciamento e parceria que delimitem claramente as responsabilidades, transferindo riscos de forma equilibrada e prevendo mecanismos de auditoria e segurança.

Na consultoria a estabelecimentos médicos-hospitalares, o advogado deve:

· Implementar programas de compliance digital, com a criação de comitês de ética em IA e a elaboração de protocolos de uso e supervisão humana das tecnologias;

· Revisar e negociar contratos com fornecedores de tecnologia, assegurando cláusulas de garantia, sigilo, responsabilidade e suporte técnico adequadas;

· Orientar sobre a obrigação de transparência com o paciente, incluindo a elaboração de termos de consentimento específicos para procedimentos que envolvam IA.

Na defesa de profissionais de saúde, o advogado deve:

· Atuar na educação continuada da classe, alertando para os riscos do viés de automação e para o dever legal de supervisão crítica dos *outputs* algorítmicos;

· Em casos de erro, construir a defesa técnica demonstrando que o profissional agiu dentro dos protocolos estabelecidos e com a diligência esperada, buscando, se for o caso, redirecionar a responsabilidade para o desenvolvedor por defeito do sistema ou para a instituição por falha na sua implementação;

· Representar o profissional nos processos ético-profissionais, argumentando sobre os limites da responsabilidade diante de sistemas complexos e da ausência de normativas claras.

6 CONCLUSÃO: POR UMA SAÚDE DIGITAL CENTRADA NA PESSOA HUMANA

A inteligência artificial não é uma miragem futurista; é uma realidade presente e disruptiva no setor de saúde, seus benefícios potenciais são imensos, mas os riscos que a acompanham são igualmente profundos e exigem uma resposta à altura do Direito.

A simples transposição de institutos jurídicos tradicionais para o ambiente algorítmico mostra-se insuficiente. É preciso construir novas categorias, reinterpretar antigos princípios e, sobretudo, estabelecer um marco regulatório que equilibre inovação com proteção dos direitos fundamentais. A Resolução CFM nº 2.454/2026, assim como o PL n° 2.338/2023, representa um passo importante nessa direção, mas seu sucesso dependerá de uma implementação que respeite as especificidades do setor de saúde e, principalmente, que assegure a participação de todos os atores envolvidos no debate.

O papel do advogado, nesse contexto, transcende a mera aplicação da lei, cabe a ele atuar como um verdadeiro arquiteto da governança digital, construindo pontes entre o Direito, a tecnologia e a ética. Seja na defesa do paciente hipervulnerável, na orientação preventiva ao profissional e às instituições, ou na assessoria aos desenvolvedores, o operador do Direito é peça-chave para garantir que a revolução tecnológica na saúde não se desvie de seu fim último: **a promoção da vida, da dignidade e do bem-estar da pessoa humana.**

O futuro da saúde será digital, mas a decisão sobre que tipo de saúde digital queremos, se uma a serviço do lucro e do controle, ou uma a serviço do cuidado e da equidade, ainda está em nossas mãos. Que o Direito, com suas ferramentas e princípios, possa iluminar esse caminho, assegurando que, no centro de qualquer sistema, por mais autônomo que seja, esteja sempre o ser humano.

REFERÊNCIAS

ABRAMED. Regulamentação da Inteligência Artificial no Brasil: desafios e perspectivas na saúde. 2025. Disponível em: https://abramed.org.br/5435/regulamentacao-da-inteligencia-artificial-no-brasil-desafios-e-perspectivas-na-saude/. Acesso em: 21 fev. 2026.

ASSOCIAÇÃO MÉDICA BRASILEIRA (AMB). Crescimento da telemedicina fez aumentar venda clandestina de dados de saúde, aponta levantamento. 2023. Disponível em: https://amb.org.br/crescimento-da-telemedicina-fez-aumentar-venda-clandestina-de-dados-de-saude-aponta-levantamento/. Acesso em: 21 fev. 2026.

B3. InovaHC e B3 anunciam parceria para interoperabilidade de dados no setor de saúde. 16 dez. 2025. Disponível em: https://www.b3.com.br/pt_br/noticias/inovahc-e-b3-anunciam-parceria-para-interoperabilidade-de-dados-no-setor-de-saude.htm. Acesso em: 21 fev. 2026.

BONNA, Alexandre Pereira; SÁ, Victória Vasconcelos. Responsabilidade civil do médico por erros ocasionados no uso da inteligência artificial. Revista Brasileira de Direito Civil em Perspectiva, Florianopolis, v. 7, n. 1, p. 45–66, 2021. DOI: 10.26668/IndexLawJournals/2526-0243/2021.v7i1.7754.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.gov.br/conselho-nacional-de-saude/pt-br/acesso-a-informacao/legislacao/outras-normativas/constituicaofederal.pdf. Acesso em: 21 fev. 2026.

BRASIL. Decreto nº 12.560, de 23 de julho de 2025. Dispõe sobre a Rede Nacional de Dados em Saúde – RNDS e sobre as Plataformas SUS Digital. Diário Oficial da União: seção 1, Brasília, DF, 24 jul. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12560.htm. Acesso em: 22 fev. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 21 fev. 2026.

BRASIL. Lei nº 9.656, de 3 de junho de 1998. Dispõe sobre os planos e seguros privados de assistência à saúde. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9656.htm. Acesso em: 21 fev. 2026.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 21 fev. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 fev. 2026.

BRASIL. Projeto de Lei n° 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 21 fev. 2026.

BRASIL. Projeto de Lei n° 2.338, de 2023. Apensados. Brasília, DF: Câmara dos Deputados, 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 21 fev. 2026.

BRASIL PARALELO. Controle de natalidade. 2026. Disponível em: https://www.brasilparalelo.com.br/artigos/controle-de-natalidade. Acesso em: 21 fev. 2026.

CLICK PETRÓLEO E GÁS. A China acaba de instalar 2.200 quiosques médicos com IA: entrega diagnóstico em 4 minutos, cita 95% de exatidão e compara sintomas com 300 milhões de casos. 2026. Disponível em: https://clickpetroleoegas.com.br/a-china-acaba-de-instalar-2-200-quiosques-medicos-com-ia-entrega-diagnostico-em-4-minutos-

cita-95-de-exatidao-e-compara-sintomas-com-300-milhoes-de-casos-nmb91/. Acesso em: 21 fev. 2026.

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.454, de 11 de fevereiro de 2026. Normatiza o uso da inteligência artificial na medicina. *Diário Oficial da União*: seção 1, Brasília, DF, 27 fev. 2026. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cfm-n-2.454-de-11-de-fevereiro-de-2026-689247948. Acesso em: 4 mar. 2026.

CONSELHO FEDERAL DE MEDICINA (CFM). Código de Ética Médica: Resolução CFM nº 2.217/2018. Brasília: CFM, 2019. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acesso em: 21 fev. 2026.

CONSELHO FEDERAL DE MEDICINA (CFM). CFM prepara resolução para regulamentar aplicação de IA na medicina. Disponível em: https://portal.cfm.org.br/noticias/cfm-prepara-resolucao-para-regulamentar-aplicacao-de-ia-na-medicina. Acesso em: 21 fev. 2026.

ESTADÃO. Corredores de rua viram ciborgues ao espalhar eletrônicos pelo corpo; veja como. 2026. Disponível em: https://www.estadao.com.br/link/gadgets/corredores-de-rua-viram-ciborgues-ao-espalhar-eletronicos-pelo-corpo-veja-como-nprei/. Acesso em: 21 fev. 2026.

FACCHINI NETO, Eugênio; BARBOSA, Rodrigo Mambrini Sandoval. Viés da automação e responsabilidade civil médica por erro de diagnóstico realizado com auxílio da inteligência artificial. Civilistica.com, a. 12, n. 3, 2023.

G1. Operação da PF mira venda ilegal de dados de pacientes do SUS. 4 fev. 2026. Disponível em: https://g1.globo.com/google/amp/sp/sao-

paulo/noticia/2026/02/04/operacao-da-pf-mira-venda-ilegal-de-dados-de-pacientes-do-sus.ghtml. Acesso em: 21 fev. 2026.

GOV.BR. Rede Nacional de Dados em Saúde (RNDS). Ministério da Saúde, [2025]. Disponível em: https://www.gov.br/saude/pt-br/composicao/seidigi/rnds. Acesso em: 21 fev. 2026.

IBM. O que é tokenização? IBM Think, 2025. Disponível em: https://www.ibm.com/br-pt/think/topics/tokenization. Acesso em: 21 fev. 2026.

KFOURI NETO, Miguel; NAGAROLLI, Rafaella. Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia: uma abordagem de direito comparado (Estados Unidos, União Europeia e Brasil). In: ROSENVALD, Nelson; MENEZES, Joyceane Bezerra de; DADALTO, Luciana (Coords.). Responsabilidade civil e medicina. 3. ed. Indaiatuba/SP: Foco, 2025.

LEGALE EDUCACIONAL. Inteligência Artificial no Direito da Saúde: Desafios e Soluções Jurídicas. 2025. Disponível em: https://legale.com.br/blog/inteligencia-artificial-no-direito-da-saude-desafios-e-solucoes-juridicas/. Acesso em: 21 fev. 2026.

MARINANGELO, Rafael. Inteligência artificial e erro de diagnóstico. Civilistica.com, Rio de Janeiro, a. 14, n. 3, 2025. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/1155. Acesso em: 21 fev. 2026.

MEDICINASA. Crescimento da telemedicina fez aumentar venda clandestina de dados de saúde. 2023. Disponível em: https://medicinasa.com.br/venda-dados-saude/. Acesso em: 21 fev. 2026.

MEDICINASA. Tokenização na saúde: o que é e como funciona? 2024. Disponível em: https://medicinasa.com.br/tokenizacao-saude/. Acesso em: 21 fev. 2026.

MIGALHAS. CDC não é aplicável a atendimento custeado pelo SUS em hospitais privados conveniados, decide STJ. 6 ago. 2020. Disponível em: https://www.migalhas.com.br/amp/depeso/321163/uso-equivocado-do-codigo-de-defesa-do-consumidor-as-relacoes-entre-medico-e-paciente. Acesso em: 21 fev. 2026.

NAGAROLI, Rafaella. Responsabilidade civil médica e inteligência artificial: culpa médica e deveres de conduta no século XXI. São Paulo: Thomson Reuters Brasil, 2023.

SANTAELLA, Lucia. A inteligência artificial é inteligente? São Paulo: Almedina, 2023.

TIMES BRASIL. Nvidia e Eli Lilly investirão US$ 1 bi ao longo de cinco anos em laboratório conjunto de IA. 2025. Disponível em: https://timesbrasil.com.br/empresas-e-negocios/nvidia-e-eli-lilly-investirao-us-1-bi-ao-longo-de-cinco-anos-em-laboratorio-conjunto-de-ia/. Acesso em: 21 fev. 2026.

UOL. Australian Open: pulseiras, cuecas inteligentes. 31 jan. 2026. Disponível em: https://www.uol.com.br/esporte/ultimas-noticias/2026/01/31/australian-open-pulseiras-cuecas-inteligentes.htm. Acesso em: 21 fev. 2026.

USCOCOVICH, Carolina Martins; SANTOS, Romualdo Baptista dos. A perda de uma chance no direito médico e a jurisprudência do Superior Tribunal de Justiça. Civilistica.com, a. 12, n. 3, 2023.

UTAH. News Release: Utah and Doctronic Announce Groundbreaking Partnership for AI Prescription Medication Renewals. Utah Governor's Office of Economic Opportunity,

6 jan. 2026. Disponível em: https://commerce.utah.gov/2026/01/06/news-release-utah-and-doctronic-announce-groundbreaking-partnership-for-ai-prescription-medication-renewals/. Acesso em: 21 fev. 2026.

[^1]: O presente artigo é um exercício acadêmico que busca replicar o estilo de redação técnico, crítico e fundamentado característico da obra de Gabriela Alves Guimarães, respeitando as normas ABNT e a integridade das fontes consultadas. A autoria imputada é meramente ilustrativa e com finalidade estilística.