

TECNOLOGIA E SAÚDE: A PROTEÇÃO DE DADOS NO SISTEMA ÚNICO DE SAÚDE E A TELEMEDICINA

Technology and Health: Data Protection in the Unified Health System and Telemedicine

Izadora Rodrigues Normando Simões¹

SUMÁRIO

1. Introdução; 2. A LGPD e a Proteção dos Dados; 3. Dados de Saúde: Estrutura Legal; 3.1 Os dados na Constituição Federal de 1988; 3.2. Direito à saúde; 4. A LGPD: A Proteção de Dados de Saúde; 5. Dados Pessoais da Saúde: Dados Sensíveis; 6. Construção de Políticas Públicas – Controle e Avaliação; 6. 1. Tecnologia e Saúde: a Telemedicina e a Proteção de Dados; 7. Conclusão; Referências Bibliográficas.

RESUMO

O presente artigo discorre sobre a Lei Geral de Proteção de Dados (LGPD), instituída pela Lei Federal nº 13.709, de 14 de agosto de 2018, regulamentada no âmbito do Estado de São Paulo pelo Decreto nº 65.347, de 9 de dezembro de 2020, explorando a perspectiva dos dados pessoais relativos à saúde, os quais requerem melhor estudo, diante do ambiente desafiador proporcionado pelas novas tecnologias, o armazenamento em grande escala de bancos de dados e pela telemedicina. O propósito é despertar a atenção ao fato de que, sem a devida regulamentação e conformidade com a LGPD, dados sensíveis de saúde podem ser utilizados para diversos fins éticos duvidosos, por vezes de forma irregular ou ilícita. No intuito de melhor desenvolver o tema, após breve desenvolvimento sobre questões conceituais atinentes ao assunto em testilha, propõe-se uma análise legislativa, com pesquisa bibliográfica e leitura crítica de doutrinas, dissertações, artigos acadêmicos e científicos. Pretende-se concluir com a investigação dos principais desafios a serem trabalhados pelos operadores imersos no fluxo da telemedicina.

Palavras-chave: LGPD. Dados Sensíveis. SUS. Telemedicina.

ABSTRACT

This article examines the General Data Protection Law (LGPD), enacted by Federal Law No. 13,709 of August 14, 2018, and regulated within the State of São Paulo by Decree No. 65,347 of December 9, 2020. It explores the perspective of personal health data, which requires further study in light of the challenging environment created by new technologies, large-scale data storage, and telemedicine. The purpose is to draw attention to the fact that, without proper regulation and compliance with the LGPD, sensitive health data may be used for various ethically questionable purposes, sometimes in an irregular or unlawful manner. In order to further develop the topic, after a brief discussion of conceptual issues related to the subject at hand, a legislative analysis is proposed, based on bibliographic research and critical reading of legal doctrines, dissertations, and academic and scientific articles. The study aims to conclude by investigating the main challenges to be addressed by professionals operating within the telemedicine framework.

Keywords: General Data Protection Law (LGPD). Sensitive Data. Unified Health System (SUS). Telemedicine.

¹ Graduação em Direito pela Universidade Paulista. Pós-graduação em Direito Administrativo, Processo Civil e Direito Digital e Inovação pela Escola Superior da Procuradoria-Geral do Estado de São Paulo.

1. INTRODUÇÃO

A crise sanitária global causada pela emergência em saúde pública da covid-19² conduziu a um significativo avanço na transformação digital da área da saúde, havendo, em curto espaço de tempo, um uso exponencial de tecnologias digitais de informação e comunicação (TICs), entre elas a telemedicina e a telessaúde, na relação entre os profissionais de saúde e os pacientes, trazendo novos contornos para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção da saúde.

A tecnologia vem permitindo, ainda, entre outros pontos: o armazenamento em grande escala e o volume de dados estruturados e não estruturados, provenientes de várias fontes e bases de dados, cujo contexto ultrapassa o conceito de telemedicina; aplicativos que tratam em massa dados de saúde; prontuário eletrônico do paciente³, ou seja, há todo um cenário tecnológico hoje que envolve a área da saúde.

A Lei Federal nº 14.510⁴, de 27 de dezembro de 2022, consagrou a telessaúde no Brasil, alterando a Lei Orgânica da Saúde (Lei nº 8.080, de 19.09.90), que estrutura o Sistema Único de Saúde (SUS), para autorizar e disciplinar a prática em todo o território nacional. Sendo assim, reconhecida a modalidade de Teleatendimento dentro da cadeia de serviços do SUS.

A telessaúde é um conceito amplo, que envolve diferentes serviços remotos de assistência, diagnóstico, educação e pesquisa em saúde, além de ser um método

² A Emergência em Saúde Pública de Âmbito Nacional em decorrência da Infecção Humana pelo novo coronavírus (2019-nCoV), denominado oficialmente de vírus SARS-CoV-2, foi decretada pela Portaria GM-MS nº 188, de 3 de fevereiro de 2020, e encerrada pela Portaria GM/MS nº 913, de 22 de abril de 2022. Destacam-se algumas medidas no âmbito do Estado de São Paulo, após a imposição da quarentena no contexto da pandemia da COVID-19, pelo Decreto nº 64.881, de 22/03/2020, podem ser verificadas nas seguintes normas: Decreto nº 64.994, de 28/05/2020; Decreto nº 65.044, de 03/07/2020; Decreto nº 65.100, de 29/07/2020; Decreto nº 65.110, de 05/08/2020; Decreto nº 65.141 de 19/08/2020; Decreto nº 65.163, de 02/09/2020; Resolução SS-127, de 11/09/2020; Decreto nº 65.319, de 30/11/2020; Decreto nº 65.460, de 08/01/2021; Decreto nº 65.487 de 22/01/2021; Decreto nº 65.529 de 19/02/2021; Decreto nº 65.545 de 03/03/2021; Decreto nº 65.563 de 11/03/2021; Decreto nº 65.596 de 26/03/2021; Decreto nº 65.613 de 09/04/2021; Decreto nº 65.635 de 16/04/2021; Decreto nº 65.663 de 30/04/2021; Decreto nº 65.680 de 07/05/2021; Decreto nº 65.716 de 21/05/2021; Decreto nº 65.731 de 28/05/2021; Decreto 65.792, de 11/06/2021; Decreto nº 65.839, de 30/06/2021; Decreto nº 65.856, de 07/07/2021; Decreto nº 65.897, de 30/07/2021 e, por fim, o Decreto nº 67.529, de 03/03/2023, que retirou a obrigatoriedade do uso de máscara.

³ Para fins de exemplificação, sugere-se consulta ao: (I) Seade Coronavírus. Disponível em: https://coronavirus.seade.gov.br/?utm_source=portal&utm_medium=banner&utm_campaign=bo%20etim-completo.%20%C3%9Altimo%20acesso%20em%2010%2F06%2F2021. Acesso em 30 mar. 2026; (II) Painel de Monitoramento (Divisão de Dengue, Chikungunya e Zica). Disponível em <https://dengue.saude.sp.gov.br/dengue/>. Último acesso em: 25 maio 2024.

⁴ BRASIL. Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm. Acesso em: 30 mar. 2026.

que abrange outros profissionais da saúde. Enquanto a telemedicina, regulamentada pela Resolução do Conselho Federal de Medicina nº 2.314, de 20.04.22⁵, é um “braço” da telessaúde e se dedica ao suporte diagnóstico remoto, por meio de soluções como laudos médicos à distância e uma segunda opinião qualificada, por exemplo. Utilizada especificamente para serviços médicos, refere-se a atos e procedimentos realizados por ou sob responsabilidade de um médico; assim, a assistência (remota) à saúde se realiza pelas ações de diferentes profissionais. O médico não é o mais importante e nem o único agente no processo.

A tecnologia em saúde permite o tratamento massivo e síncrono de dados de saúde por diversos meios digitais, por vezes, sem interação com o paciente. Seu avanço permite o aumento do tráfego síncrono de dados pessoais sensíveis, como os de saúde, em diferentes meios digitais, integrados por meio de *Application Programming Interfaces* (APIs), tornando a saúde digital vulnerável a ataques cibernéticos e outros tipos de incidentes.

A tecnologia na área da saúde é uma importante aliada e um caminho sem volta, e vai impactar, cada vez mais rapidamente, as formas de pesquisar, prevenir, diagnosticar e tratar doenças⁶.

Ainda, o tratamento irregular, ilícito ou inseguro, sem a devida regulamentação e fiscalização, dos dados sensíveis corpóreos que trafegam hoje no complexo ecossistema da saúde digital pode resultar na utilização desses dados com objeto de análise e na aplicação de técnicas avançadas para criar classificações, perfilações e, inclusive, previsões e padrões comportamentais que permitem a oferta de serviços adicionais e de produtos a partir do tratamento secundário (e terciário) de dados pessoais sensíveis de saúde. Trata-se de atividade de “alto risco”, com potencial discriminatório e lesivo para o sujeito mais vulnerável, o paciente digital, resumido a informações contidas em vastos bancos de dados.

A legislação brasileira, ao contrário do Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, General Data Protection Regulation (GDPR)⁷, não definiu diretamente o conceito de “dados pessoais relativos à saúde”. Cabe ao intérprete buscar essa definição no quadro legislativo atual e acompanhar o desdobramento do tema por meio das orientações da Agência Nacional de Proteção De Dados (ANPD), pela própria compreensão do

⁵ CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.314/2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. **Diário oficial**, Brasília, 5 maio 2022, Seção I, p. 227.

⁶ Sugere-se consulta ao sítio eletrônico “#VacinaJá”, no qual é possível verificar as doses de vacinas aplicadas por município do estado de São Paulo, segundo diversos indicadores. Disponível em: <https://vacinaja.sp.gov.br/vacinometro/>. Acesso em: 30 maio 2024.

⁷ UNIÃO EUROPEIA. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR)**. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>. Acesso em: 30 mar. 2026.

problema pelos gestores do SUS e pelo aprimoramento dos instrumentos jurídicos, com foco na relação titular–controlador–operador–encarregado–agentes de tratamento, em especial, nos convênios e contratos de gestão de saúde e, eventualmente, em decisões judiciais.

A definição deve coincidir com o conceito amplo de saúde, adotado pelo artigo 3º da Lei Federal nº 8.080, de 19 de setembro de 1990⁸, com determinantes e condicionantes que contemplem, inclusive, o bem-estar físico, mental e social. Nesse sentido, perfazendo este “conceito ampliado de saúde”, conforme o § 1º do artigo 11 da LGPD: dados pessoais, em princípio “comuns”, como a geolocalização, a depender dos cruzamentos e inferências, podem revelar dados pessoais sensíveis de saúde, mitigando a tese da taxatividade estática do artigo 5º, II, da LGPD.

O tema ainda carece da devida regulamentação e há muito o que evoluir; como mencionado, dados sensíveis de saúde podem ser utilizados para diversos fins eticamente delicados e duvidosos, e com vantagem econômica, caso tratados de maneira irregular ou ilícita. A título de exemplo, podem: determinar quem vai ter um emprego ou não, com base nas condições de saúde; induzir demissões, com base em decisões automatizadas com o uso de algoritmos; definir qual o preço que uma pessoa pagará em seu plano de saúde; definir o valor do financiamento imobiliário, com base em potencial diagnóstico, como diabetes tipo II, conforme perfil de consumo na farmácia (ao informar o Cadastro de Pessoa Física - CPF); definir que tipo de condições de saúde serão admitidas nas políticas de imigração entre países; e induzir uma pessoa a determinados comportamentos, como os relacionados à vacinação.

Desse modo, o presente trabalho pretende apresentar essas questões e fazer uma breve análise da necessidade de aprimoramento de processos e protocolos para a proteção de dados pessoais relativos à área da saúde, em especial, na telemedicina.

2. A LGPD E A PROTEÇÃO DOS DADOS

Nas últimas décadas, vivemos um intenso processo de transformação digital, e a presença da tecnologia da informação se apresenta como mediadora nas mais diversas relações humanas com as máquinas, que estão cada vez mais autônomas. Em um mundo digital em constante evolução, a quantidade de informações e dados gerados na interação entre dispositivos tecnológicos e pessoas é incalculável.

Ainda que muitas vezes não se deem conta, as pessoas passaram a ser geradoras de dados. Isso ocorre porque, nas mais diversas relações – seja em compras em farmácias, em simples pesquisas em sites de busca de informações, na manutenção

⁸ BRASIL. Lei nº 8.080, de 15 de dezembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. **Diário Oficial**, Brasília, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 30 mar. 2026.

de perfil em redes sociais, na abertura de contas em banco, na utilização de ferramentas de vigilância, por meio de reconhecimento facial ou biométrico, em serviços de saúde etc. – dados pessoais são extraídos, transferidos e armazenados em inúmeros bancos de dados, nos quais nossa identidade é permanentemente analisada e utilizadas para os mais diferentes fins, tanto por instituições privadas quanto por instituições públicas.

No entender de Chiara Teffé⁹:

Os dados contam histórias sobre nós: indivíduos, grupos e sociedade. Quanto mais dados pessoais tratados e tecnologias sofisticadas empregadas, mais perfis serão criados e análises e previsões realizadas. A partir de informações pessoais, é possível conhecer hábitos, comportamentos, gostos preferências, descendências, estado de saúde e crenças de uma pessoa. Ao longo do tempo, a qualidade e a precisão das análises vêm sendo aperfeiçoadas, havendo inclusive a utilização de complexas estruturas de inteligência artificial nos processos, e seus resultados utilizados para os mais variados fins, por instituições públicas e privadas.

No que tange ao setor público, observa Lucas Borges¹⁰ que:

[...] entre outras inovações, o processo de digitalização permite que informações que, há algumas décadas, estavam registradas apenas de forma analógica, muitas vezes impressas em documentos arquivados em armários nas diversas repartições públicas, possam ser armazenadas em formato digital, em computadores com alta capacidade de processamento. Com isso, é possível não somente ampliar e acelerar a coleta de informações pessoais, como também inferir novas informações ou realizar o cruzamento entre as diversas bases de dados, destinando-as para múltiplas finalidades, em particular mediante o seu uso compartilhado com outros órgãos públicos e entidades privadas.

Nessa crescente transformação digital e produção de informações, os dados pessoais tornaram-se ativos valiosos para governos e empresas, sendo certo que a falta de proteção adequada desses dados pode levar a abusos, violações de privacidade, roubo de identidade e outros crimes cibernéticos.

Não há dúvidas de que a transformação digital vem resultando em inúmeros benefícios para a sociedade, e apresenta-se como um processo fundamental para ampliar a eficiência, não apenas no setor privado, mas também na atuação do Estado (como prestador de serviços, na sua função de formular políticas públicas e

⁹ TEFFÉ, Chiara Spadaccini de. **Problemas de direito civil**: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Janeiro: Forense, 2021, p. 97.

¹⁰ CARVALHO, Lucas Borges de. O Poder Público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 282, n. 2, p. 133-162, 2023, p. 16-17.

na garantia de direitos sociais, como os relacionados à educação, à saúde e ao trabalho). Entretanto, como mencionado, isso trouxe desafios importantes ao Direito, especialmente no que tange à proteção da privacidade dos indivíduos, uma vez que se ampliam os riscos de abusos e de violação aos direitos dos titulares, que podem ocorrer pelo mau uso de seus dados.

A Constituição Federal de 1988 estabelece em seu artigo 5º, inciso X, a garantia de proteção dos direitos fundamentais da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação, sendo este princípio constitucional a base para a proteção da privacidade no contexto digital.

Nessa perspectiva fática (constante evolução digital em que dados são gerados indiscriminadamente) e constitucional (proteção aos direitos fundamentais da privacidade, intimidade e liberdade), a LGPD¹¹ tem como disciplina o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião, à inviolabilidade da intimidade, da honra e da imagem, ao desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais (art. 2º, LGPD), nas mais diversas relações estabelecidas entre pessoas naturais e/ou pessoas jurídicas, e às tecnologias.

Aplicada tanto no setor público quanto no privado, assim como nos ambientes físico e virtual, estabelecendo regras para a coleta, armazenamento, tratamento e compartilhamento de dados, a LGPD impõe a completa releitura de todas as formas de tratamento de dados pessoais, nas mais diversas áreas. Nessa linha, defende Beatriz Freitas Santos que, ao estabelecer regras claras para a coleta, o armazenamento, o tratamento e o compartilhamento de dados, “a LGPD busca proteger os direitos fundamentais de liberdade e privacidade, promovendo também a segurança jurídica e o desenvolvimento econômico e tecnológico do Brasil”¹².

Pode-se dizer que a LGPD, ao proteger os dados pessoais, desempenha um papel crucial no cenário da transformação digital, pois fornece as bases para a confiança dos cidadãos e consumidores, sendo essencial para fortalecer a proteção efetiva dos direitos individuais, promovendo a confiança de investidores, empresas e cidadãos no ambiente digital.

¹¹ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 mar. 2026.

¹² SANTOS, Beatriz Freitas. Lei Geral de Proteção de Dados (LGPD) e a garantia de proteção dos direitos fundamentais de liberdade e de privacidade dos cidadãos à luz do Direito Constitucional. **Aporia Jurídica**, Ponta Grossa v. 1, n. 19, 2023.

Além disso, a LGPD contribui para melhorar a governança de dados e fomentar a justiça e a igualdade no acesso e na utilização de informações pessoais. A legislação também tem impacto na forma como as organizações gerenciam os dados, incentivando a adoção de práticas responsáveis e transparentes, evitando o mau uso das informações e promovendo a conscientização sobre a importância da proteção de dados. Em resumo, a LGPD é fundamental para garantir a segurança, a privacidade e a confiabilidade nos ambientes físico e digital, além de fortalecer a proteção dos direitos individuais e promover o desenvolvimento sustentável da inovação no Brasil.

Vale destacar que a LGPD contém expressa previsão de aplicação de suas normas às pessoas jurídicas de direito público (art. 1º):

[...] as quais devem observar princípios gerais como os da necessidade, finalidade e adequação (art. 6º), além de obrigações específicas de transparência (art. 23). Da mesma forma, aos usuários de serviços públicos foram assegurados importantes direitos, tais como os de acesso aos dados e correção de dados incompletos, inexatos ou desatualizados (art. 18, II e III), de oposição a tratamento efetuado sem consentimento (art. 18, § 2º) e de revisão de decisões automatizadas (art. 20). Por fim, em caso de irregularidades, a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar sanções administrativas a entidades e órgãos públicos (art. 52, § 3º)¹³.

Nas relações com as instituições públicas, deve-se considerar que o cidadão é o elo mais frágil e vulnerável, uma vez que suas informações pessoais são coletadas de forma compulsória e, se não adotadas as devidas salvaguardas, podem ser utilizadas para fins abusivos, associados às práticas de discriminação ou de vigilância.

A coleta de informações dos cidadãos pelo Estado está muito bem estabelecida e estruturada, envolvendo quantidades massivas de dados pessoais, muitas vezes, armazenadas em formato digital e tratadas de forma automatizada. Nesse sentido, os dados pessoais constituem um insumo relevante para ampliar a eficiência da ação estatal, por exemplo, por meio do compartilhamento de informações entre entidades e órgãos públicos ou, ainda, mediante a produção de evidências que embasam a formulação de políticas públicas.

Como ressalta Miriam Wimmer¹⁴:

A questão sobre o quanto bem o Estado deve conhecer seus cidadãos já foi enfrentada em variados contextos e em diferentes momentos históricos, tendo por pano de fundo o reconhecimento de que, ao mesmo tempo que o tratamento de dados pessoais pelo Estado é pré-requisito para o exercício

¹³ CARVALHO, *op. cit.*, p. 2.

¹⁴ WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: MENDES, Laura, *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 273.

da cidadania, a expansão da quantidade e da variedade de dados pessoais custodiados pelo Estado suscita riscos de violações de direitos. Dito de outro modo, a visibilidade do Estado sobre seus cidadãos permite ampliar a sua capacidade de intervenção, tenha ela por objetivo atingir finalidades sociais justas (e.g., viabilizar a distribuição de benefícios sociais) ou nefastas.

Quanto ao processo de coleta massiva de dados pessoais, alerta Lucas Borges¹⁵ que este gera um “excedente comportamental”, ou seja:

[...] uma espécie de sobrevalor, que transcende os propósitos originais da operação de coleta. Como consequência, mesmo após exauridos os seus objetivos iniciais, o uso de um conjunto de dados pessoais tende a permanecer atrativo e valioso para outras finalidades. Esse uso subsequente e contínuo dos dados pessoais permite gerar um valor adicional significativo – seja ele de ordem pública, política ou econômica – a um custo marginal reduzido, em particular diante da possibilidade de realização de novas inferências a partir de técnicas de análise de dados ou de simples agregação de novas informações, entre outras possibilidades, sempre visando ao controle, à previsão e ao direcionamento de comportamentos.

É importante salientar que, conforme a legislação, no setor público, o tratamento de dados pessoais para propósitos distintos daqueles que justificaram a coleta inicial deve, entre outras condições, sempre atender a uma finalidade pública. Conforme disposto de forma expressa no seu art. 26, a LGPD estabelece que “o uso compartilhado de dados pessoais pelo Poder Público deve atender à finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas”.

É fundamental que a LGPD e sua aplicação continuem a ser aprimoradas e aperfeiçoadas, a fim de se manterem atualizadas e relevantes em um ambiente digital em constante evolução. Investir em educação e conscientização sobre a importância da privacidade e da proteção de dados é uma ferramenta eficaz para promover uma cultura de respeito à privacidade e à segurança digital.

3. DADOS DE SAÚDE: ESTRUTURA LEGAL

3.1 Os dados na Constituição Federal de 1988

A Constituição Federal de 1988 originalmente previu a proteção do acesso a dados e informações pela criação de instrumento processual denominado *Habeas Datas* (art. 5º, inciso LXXII), nos seguintes termos:

¹⁵ CARVALHO, *op. cit.*, p. 10.

LXXII - conceder-se-á “*habeas-data*”:

a) para assegurar o **conhecimento de informações** relativas à pessoa do impetrante, constantes de registros ou **bancos de dados de entidades governamentais ou de caráter público**;

b) **para a retificação** de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; [...] ¹⁶

No ano de 2022, foi incluída, pela Emenda Constitucional nº 115/2022¹⁷, a proteção de dados pessoais entre os direitos e garantias fundamentais, inclusive digitais, dando competência privativa a União para legislar sobre a proteção e o tratamento de dados pessoais: “XXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Incluído pela Emenda Constitucional nº 115, de 2022)”.

Classificou-se a emenda constitucional como uma “medida meritória” que reforça a segurança jurídica e favorece os investimentos em tecnologia no Brasil, a qual complementa, lastreia e reforça dispositivos inseridos recentemente na legislação ordinária, como o Marco Civil da Internet, de 2014, e a Lei Geral de Proteção de Dados, de 2018¹⁸.

Assim, como dito, a emenda constitucional incorporou a proteção dos dados pessoais ao catálogo de direitos e garantias fundamentais, alcançando, a despeito das intersecções e articulações com outros direitos, esse direito à categoria de direito fundamental autônomo, com esfera de proteção própria, acabando por atribuir, de modo inquestionável, o pleno regime jurídico constitucional de direito fundamental, material e formal.

Conforme bem elucida Ingo Sarlet¹⁹:

- 1) como parte integrante da constituição formal, os direitos fundamentais possuem status normativo superior em relação a todo o restante do ordenamento jurídico;

¹⁶ BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial**, Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 abr. 2026. Grifo nosso.

¹⁷ BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 abr. 2026.

¹⁸ PROMULGADA emenda constitucional de proteção de dados. **Agência Senado**, 10 fev. 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados>. Acesso em: 8 abr. 2026.

¹⁹ SARLET, Ingo. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Consultor Jurídico**, 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/>. Acesso em: 30 mar. 2026.

- 2) na condição de direito fundamental, assume a condição de limite material à reforma constitucional, devendo, ademais disso, serem observados os assim chamados limites formais, circunstanciais e temporais, nos termos do artigo 60, parágrafos 1º a 4º, da CF;
- 3) também as normas relativas ao direito à proteção de dados são – nos termos do artigo 5. 1º, CF – dotadas de aplicabilidade imediata (direta) e vinculam diretamente todos os atores público, bem como – sopesadas as devidas ressalvas – os atores privados.
- 4) Mediante a redação dada pela EC 115/22, o direito fundamental à proteção de dados pessoais passa a estar submetido a uma expressa reserva legal simples, que empodera o legislador infraconstitucional para efeito de estabelecer intervenções restritivas no âmbito de proteção do direito, implicando, por outro lado, a observância das exigências da reserva de lei, pela de inconstitucionalidade da restrição.
- 5) O direito fundamental à proteção de dados assume particular relevância, pelo fato da existência de uma série de lacunas regulatórias, porto que a LGPD não contempla os setores da segurança nacional, segurança pública, investigação criminal, execução penal, apenas para citar os mais relevantes. Por tal razão, como o reconhecimento do referido direito fundamentas, para a inexistir uma “zona livre” de proteção dos dados pessoais na ordem jurídica brasileira.

Por fim, importa destacar que nos termos do artigo 5º, §§ 2º e 3º, da CF/88, o marco normativo que concretiza e formata o âmbito de proteção do direito fundamental à proteção de dados pessoais é, também, integrado pelos tratados internacionais de direitos humanos ratificados pelo Brasil, destacando-se a Convenção Americana de São José da Costa Rica e o Pacto Internacional de Direitos Civis e Políticos.

3.2. Direito à Saúde

A Constituição Federal de 1988 criou a Seguridade Social como um conjunto integrado de ações de iniciativa do poder público e da sociedade, destinada a assegurar os direitos relativos à saúde, à previdência e à assistência social, nos termos do artigo 194, *caput*, da Constituição Federal.

Inovou ao criar três estruturas distintas dentro da seguridade social: saúde, previdência e assistência social, financiadas por toda a sociedade, de forma direta e indireta, nos termos da lei, mediante recursos provenientes dos orçamentos da União, dos Estados, do Distrito Federal e dos Municípios, além da previsão de contribuições sociais.

Na nossa Carta Constitucional de 1988, a saúde passou a ser definida como um direito fundamental de todos (artigo 6º) e um dever a ser garantido pelo Estado, “garantido mediante políticas sociais e econômicas que visem à redução do risco de

doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação”²⁰, instituindo, assim, o princípio da universalidade no atendimento à saúde.

Contemplando este entendimento, o SUS é o conjunto de ações e serviços de saúde, prestados por órgãos e instituições públicas dos três âmbitos da federação, da administração direta e indireta e das fundações mantidas pelo poder público, com validade em todo o território nacional, regulamentados estruturalmente pela Lei nº 8.080, de 19 de dezembro de 1990, conhecida como a Lei Orgânica da Saúde (LOS), complementada pela Lei nº 8.142, de 28 de dezembro de 1990, matrizes do sistema no âmbito infraconstitucional.

Importante destacar, ainda, que, para cumprir esse princípio constitucional, foi facultado aos gestores do SUS complementar a oferta dos serviços de assistência à saúde em cooperação com entidades privadas de assistência à saúde (artigos 197 e 199, § 1º, da CF/88). Dito isto, participam do SUS não somente as entidades públicas, mas também a iniciativa privada²¹.

A concretização do direito à saúde pressupõe respeito aos princípios da igualdade, do acesso universal e da integralidade. A sua estrutura pressupõe a participação consciente da comunidade e o fortalecimento do sistema federativo, por ter sido desenhado com base em uma rede hierarquizada e regionalizada, com ênfase na atuação dos Municípios e nas medidas de prevenção.

Além dos princípios constitucionais aplicáveis aos direitos fundamentais e à seguridade social (art. 194, parágrafo único, CF), há os princípios específicos, previstos na Constituição Federal e no art. 7º da LOS, que deverão ser aplicados a todas as ações e serviços públicos que integram o SUS, incluindo a rede pública e os serviços privados contratados ou conveniados.

Entre eles, cabe destacar o princípio da informação, o qual compreende duas vertentes: i) aspecto individual, em que as pessoas assistidas têm o direito de saber os dados sobre sua saúde; ii) aspecto coletivo, que compreende o direito à divulgação de informações quanto ao potencial dos serviços de saúde e a sua utilização pelo usuário²². Dessa forma, é importante entender que o trâmite de dados na área da

²⁰ BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial**, Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 abr. 2026. Art. 6º.

²¹ No mesmo sentido, a Lei Federal nº 8.080/1990, prevê nos artigos 4º, § 2º, e 24, que “A iniciativa privada poderá participar do Sistema Único de Saúde (SUS), em caráter complementar. Art. 24: Quando as suas disponibilidades forem insuficientes para garantir a cobertura assistencial à população de uma determinada área, o Sistema Único de Saúde (SUS) poderá recorrer aos serviços ofertados pela iniciativa privada. BRASIL. **Lei nº 8.080, de 15 de dezembro de 1990**, *op. cit.*

²² WERNER, Patricia Ulson Pizarro. Direito à saúde. In: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (coord.). **Enciclopédia jurídica da PUC-SP**. 2. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/170/edicao-2/direito-a-saude>. Acesso em: 30 mar. 2026.

saúde deve respeitar harmoniosamente a proteção dos dados e o acesso, conforme a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI) (Lei Federal nº 12.527/11).

Nesse cenário, diante da quantidade de órgãos e entidades envolvidos, é possível visualizar a grande complexidade da questão do fluxo de dados em um sistema inserido em uma rede regionalizada e hierarquizada, que abrange: (i) os vários níveis da federação, com fluxo entre União, Estados e Municípios; e (ii) a relação entre as diversas categorias, como saúde pública propriamente dita, saúde complementar (§ 1º, art. 199, CF/88) e saúde suplementar.

A integração dos serviços de saúde no formato de rede no contexto federativo, incluindo, segundo Werner, Municípios, “Consórcios Municipais, Estados, Distrito Federal e União”²³, cada qual exercendo suas atribuições fixadas em lei, de modo articulado com a programação da rede regionalizada e hierarquizada²⁴, para que não haja sobreposição de serviços, mas, ao mesmo tempo, se garanta o amplo acesso a todos, é um desafio.

Na saúde, há uma série de sistemas informatizados por meio dos quais dados pessoais de saúde são inseridos e tratados, tais como: o Sistema Nacional de Informação em Saúde (DATASUS)²⁵, o Sistema de Informação sobre Mortalidade (SIM), o Sistema de Informações sobre Nascidos Vivos (SINASC), o Sistema de Informações de Internações Hospitalares (SIH), os prontuários eletrônicos, os aplicativos que tratam em massa de dados de saúde, entre outros. Dito isto, existe uma enorme quantidade de dados a serem controlados, sendo imperiosa a necessidade de se enfrentar a complexidade semântica para categorizá-los; afinal, o próprio conceito de saúde traz uma amplitude intrínseca que requer atenta análise.

O Brasil adere, em sua legislação, ao conceito fixado pela Organização Mundial da Saúde (OMS) como um “estado de completo bem-estar físico, mental e social e consiste somente na ausência de uma doença ou enfermidade”²⁶.

Na sequência, estabelecem-se os princípios que devem guiar a compreensão da saúde, que podem ser sintetizados nos seguintes pontos:

²³ WERNER, *op. cit.*, item 3.5.

²⁴ Rede hierarquizada compreende o desenho da complexidade dos fluxos e das conexões dos serviços e ações de saúde nos planos micro, meso e macroinstitucionais.

²⁵ Gerenciado pela União, pelo Departamento de Informática do SUS (DATASUS), que contém sistemas integrados de: (i) informatização de ambiente hospitalar; (ii) informações sobre orçamentos públicos em saúde, (iii) descentralização do Sistema de Informações Hospitalares do SUS (SIH/SUS); (iv) cadastro nacional de estabelecimentos do SUS; e) cadastro nacional e sistema de informações do programa nacional de imunizações Sistemas de Informação em Saúde – Ministério da Saúde.

²⁶ ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Constituição da Organização Mundial da Saúde**. Genebra: OMS, 1946.

Igualdade: é um direito fundamental garantido a todo ser humano, sem distinção de raça, religião, ideologia política e condição econômica social; (ii) Paz e segurança: a saúde de todos os povos é uma condição fundamental para atingir a paz e a segurança, por depender de uma ampla cooperação das pessoas e do Estado; (iii) Fomento e proteção evita o perigo comum: os resultados alcançados por cada Estado no fomento e desenvolvimento da proteção à saúde são valiosos para todos; principalmente, em relação às doenças transmissíveis que constituem um período comum; (iv) Desenvolvimento da criança: a criança tem uma importância fundamental, sendo indispensável o estímulo à capacidade de viver em harmonia com o mundo que muda constantemente; (v) Conhecimento: estender para todos os povos os benefícios dos conhecimentos médicos, psicológicos e afins são essenciais para alcançar o mais alto grau de saúde; (vi) Informação: a opinião pública bem informada e a cooperação ativa por parte do público são de importância capital para a melhoria da saúde de um povo; (vii) Responsabilidade do Estado: o governo tem responsabilidade pela saúde de seu povo, principalmente, deve adotar medidas sanitárias e sociais adequadas²⁷.

Destaca-se a realização da I Conferência Internacional sobre Cuidados Primários de Saúde em Alma-Ata, no Cazaquistão, quando se fixou a política de “Saúde para Todos no Ano 2000”, pacto assinado por 134 países, com grande influência nas diretrizes adotadas pelo Brasil, por ressaltar a importância dos cuidados primários de saúde²⁸.

A partir desse breve contexto, fica evidente a alta complexidade do tema que envolve dados de saúde e a sua proteção, uma vez que é inerente a dificuldade de se estabelecer o controle rigoroso de cada parte do processo de trâmite dos dados, sendo complexo controlar a aplicação das regras de resguardo, capacitar e conscientizar todos os atores e partes envolvidos.

4. A LGPD: A PROTEÇÃO DE DADOS DE SAÚDE

A LGPD prevê que a proteção dos dados deve ser guiada pelos princípios da boa-fé e do interesse público envolvido, fixando os seguintes preceitos hermenêuticos em seu artigo 6º²⁹:

I. **Finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

²⁷ *Ibid.*

²⁸ WERNER, *op. cit.*

²⁹ BRASIL. Lei nº 13.709, de 14 de agosto de 2018, *op. cit.*, art. 6º.

II. **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III. **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados

IV. **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V. **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI. **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII. **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII. **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX. **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X. **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

É uma Lei que traz uma série de instrumentos e garantias para aumentar o poder e o controle do titular sobre seus dados, priorizando a autodeterminação informativa, uma vez que, no entender de Chiara Teffé³⁰:

Vivemos em um ambiente marcado por elevada assimetria informacional: uma parte, geralmente grandes empresas e Estados, detém mais poder, recursos e melhores informações do que a outra, o cidadão comum, por vezes, consumidor nas relações desenvolvidas. [...] Tal assimetria informacional não se revela apenas no poder que os agentes dispõem sobre os dados pessoais de terceiros, mas, também nas novas modalidades de negócios, em que informações pessoais de seus usuários representam uma das bases centrais do sistema desenvolvido.

Dentro dessa dinâmica, a LGPD se apresenta com um caráter preventivo, com o objetivo de evitar danos e vazamento de dados. Essa lógica preventiva é muito

³⁰ TEFFÉ, Chiara Spadaccini de, *op. cit.*, p. 15.

clara quando pensamos no cuidado que a referida norma impõe no tratamento de dados e nos direitos dos titulares que ali são inseridos, bem como, pelo próprio relatório de impacto à proteção de dados que é mencionado no inciso XVII do artigo 5º.

Conforme bem elucida Chiara Teffé:

A norma traz a lógica de *privacy by design* (art. 46, § 6º, da LGPD)³¹, ao preconizar que a privacidade e a proteção de dados devem ser consideradas desde sua concepção e durante todo o ciclo de vida de projetos, sistemas, serviços, produtos e processos que envolvam o tratamento de dados, especialmente se eles foram sensíveis, devendo, por consequência, ser incluídas avaliações prévias de impacto, medidas técnicas e organizacionais adequadas e instrumentos de prestação de contas (*accountability*)³².

A área da saúde entra na LGPD em pesquisa e saúde pública (art. 13), bem como na qualificação da coleta e do tratamento de dados pessoais sensíveis (art. 11). Especialmente os §§ 3º e 4º do art. 11 abordam a questão da vedação do uso econômico dos dados pessoais sensíveis. O § 4º do art. 11 trouxe importante flexibilização do conceito de que todo compartilhamento de dados sobre paciente é permitido, desde que em benefício dos titulares. Isso ocorre porque, na medicina, os dados não são utilizados somente para tratar de um indivíduo, mas, também, para criar protocolos para o próximo paciente, sendo certo que sempre haverá o compartilhamento de dados na saúde, tendo em vista que todo protocolo médico foi criado com base em evidências, e estas nada mais são do que dados.

Para o tratamento de dados pessoais se estabelece, como regra geral, o consentimento pelo titular do dado, abrindo espaço para o tratamento dos dados nas hipóteses do artigo 7º da LGPD. Assim, cabe destacar no âmbito da saúde, os seguintes pontos: fornecimento de consentimento pelo titular; cumprimento de obrigação legal ou regulatória pelo controlador; ou pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais e, conforme acréscimo realizado em 2019, tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária³³.

³¹ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit.*

³² TEFFÉ, Chiara Spadaccini de, *op. cit.*, p. 209-210.

³³ Redação dada pela Lei nº 13.853, de 2019. BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial**, Brasília, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 8 abr. 2026.

O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, referindo-se às finalidades determinadas, sendo certo que as autorizações genéricas para o tratamento de dados pessoais serão nulas, cabendo ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na Lei, sendo vedado o tratamento de dados pessoais mediante vício de consentimento (art. 8º, LGPD).

Ademais, é necessário criar a possibilidade de o sistema permitir a revogação, a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificando-se os tratamentos realizados sob amparo do consentimento anteriormente manifestado, enquanto não houver requerimento de eliminação, nos termos do art. 8º, § 5º, c/c o inciso VI do caput do art. 18 da LGPD.

Hoje, cada unidade da rede do SUS possui um sistema próprio de controle, o que é ampliado pelos serviços contratados via saúde complementar, razão, pela qual, estabelecer regras de unificação e controle trariam segurança e maior eficiência no SUS.

5. DADOS PESSOAIS DA SAÚDE: DADOS SENSÍVEIS

Os dados pessoais de saúde são uma categoria especial de informações que requerem proteção adicional, devido à sua natureza íntima e pessoal, sendo considerados sensíveis por expressa disposição legal (art. 5º, II, LGPD).

A lei define o que é dado pessoal e o que é dado pessoal sensível. Dado pessoal é a informação relacionada à pessoa natural identificada ou identificável (art. 5º, I, LGPD), enquanto os dados pessoais sensíveis (art. 5º, II, LGPD) são definidos como aqueles que compreendem:

[...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural³⁴.

É de extrema relevância a classificação trazida pela lei, conceituando dados pessoais e dados sensíveis, uma vez que os dados sensíveis apresentam um maior risco quando do seu mau uso, podendo ensejar discriminações ilícitas ou abusivas ao seu titular, devendo, portanto, ser protegidos de forma ampliada.

Assim, entende-se que, ao categorizar os dados pessoais sensíveis, a LGPD visa tutelar de forma ampliada as informações que comumente são utilizadas em processos discriminatórios ilícitos ou abusivos.

Esse é um tema de extrema importância, pois, atualmente, percebe-se, também, a possibilidade de inferências sensíveis a partir do tratamento de dados que

³⁴ BRASIL. Lei nº 13.709, de 14 de agosto de 2018, *op. cit.*

não são, na origem, sensíveis. Por exemplo: com a geolocalização de uma pessoa, pode-se chegar a dados relativos à saúde, a questões políticas e a questões religiosas; dados financeiros de uma pessoa, em determinados casos, direcionam a informações de saúde, tais como, despesas e reembolso médico. Nesse sentido, é importante a atenção para as possibilidades de inferência sensíveis com o cruzamento de dados, a atuação de inteligência artificial e o *Big Data*, que atuam diretamente nessas relações. Como se denota, atualmente, vive-se em um cenário em que é relativamente simples inferir ou mesmo extrair dados sensíveis nas mais diversas relações.

Proteger dados sensíveis é essencial para evitar cenários discriminatórios, de preconceito, ilícitos, abusivos e estigmatizantes. Proteger dados sensíveis, também, é fundamental para que se garanta a liberdade das pessoas naturais e para facilitar o acesso a bens e serviços. É nesse cenário que a aplicação da LGPD se mostra importante, especialmente no cuidado relativo aos dados pessoais sensíveis e o próprio direito antidiscriminação.

A regra é que o dado pessoal de saúde é sensível e seu tratamento deve ocorrer: (i) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; (ii) sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 11, LGPD).

A lei prevê hipóteses de exceção, as quais devem ser interpretadas de maneira restritiva, das quais se destacam: quando houver o consentimento para finalidades específicas; quando não houver o fornecimento de consentimento do titular, poderá haver exceção por força do cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, LGPD).

A Administração poderá tratar dados compartilhados necessários à execução de políticas públicas previstas em leis ou regulamentos e autorizar a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.

Outra possibilidade ocorre no caso de proteção da vida ou da incolumidade física do titular ou de terceiro e na tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária³⁵.

Atenção especial deve ser concedida aos dados pessoais de saúde de pacientes, pois é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º do art. 11 da LGPD, incluídos os serviços auxiliares de diagnóstico e terapia, em benefício dos interesses dos titulares de dados (art. 11, § 4º, LGPD), e para permitir: i) a portabilidade de dados quando solicitada pelo titular; ou ii) as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde.

Da mesma forma, é importante destacar que, até no âmbito da saúde suplementar, é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (art. 11, § 5º, LGPD).

O Poder Público deve dar especial atenção à área de Ciência, Tecnologia e Informação (CT&I), na qual o controle dos dados dos pacientes deve ser muito rigoroso, inclusive no controle da denominada pseudonimização, ou seja, o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador, em ambiente controlado e seguro (art. 13, § 4º, LGPD).

Destacam-se os critérios a serem utilizados nos estudos em saúde pública:

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

³⁵ Redação dada pela Lei nº 13.853, de 2019. BRASIL. Lei nº 13.853, de 8 de julho de 2019, *op. cit.*

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências³⁶.

Na área da saúde, sabemos que são possíveis as mais diversas discriminações, por esse motivo é necessário um cuidado adicional com os titulares de dados. Acrescente-se que, especialmente na área da saúde, é possível considerar como titular de dados, não só a criança, o adolescente e o adulto, mas até mesmo o nascituro, que já tem dados de saúde sendo tratados em exames pré-natais, exames laboratoriais de gravidez, entre outros.

Destaca-se que o nascituro nem tem personalidade jurídica, conforme o art. 2º do Código Civil, mas já tem informações sobre ele sendo tratadas.

Há aplicativos de controle da gestação, assim, essa preocupação com os dados de saúde é algo que preocupa desde o momento da concepção até o final da vida.

Nesse contexto, os dados falam sobre o nosso passado, presente e futuro. Dados pessoais falam sobre a nossa ascendência, nossa descendência, a nossa propensão a doenças e a nossa resposta a medicamentos; assim, é importante o estabelecimento de *compliance* voltado para a área específica da saúde, com normas e boas práticas direcionadas a esse setor.

No rol de dados sensíveis, temos várias categorias: questões raciais, questões étnicas, questões biométricas, questões genéticas e religiosas. São temas extremamente relevantes que exigem, por si só, um cuidado apurado, especialmente na área da saúde. O consentimento, sendo livre e informado, é de extrema relevância, bem como a existência de normas técnicas e jurídicas voltadas à proteção desses direitos.

Hoje, há uma preocupação com o tratamento de dados que não envolva um dado sensível, mas que tenham um viés discriminatório. É importante compreender com cuidado a dinamicidade das categorias e os diversos processos discriminatórios existentes em nossa sociedade.

Nesse sentido, o enunciado 690 da IX Jornada do Conselho da Justiça Federal (CJF) (que teve uma comissão específica para o Direito Digital) dispõe que: “A proteção ampliada conferida a LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no § 1º do art. 11 da LGPD”³⁷.

Houve, nesse enunciado, uma atenção às inferências sensíveis e aos tratamentos que revelam informações sensíveis. É necessário, então, que prestemos atenção tanto à proteção ampliada, que sempre deve ser conferida, mas, também às

³⁶ BRASIL. Lei nº 13.709, de 14 de agosto de 2018, *op. cit.*

³⁷ CONSELHO DA JUSTIÇA FEDERAL (CJF). IX Jornada Direito Civil: comemoração dos 20 anos da Lei nº 10.406/2022 e da instituição da Jornada de Direito Civil: enunciados aprovados. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022, p. 49.

possibilidades de inferências sensíveis e à obtenção de resultados sensíveis a partir de tratamento de dados. Isso é fundamental para o cenário democrático no Brasil e com os próprios direitos fundamentais.

Nesse aspecto, é importante tratar com muito cuidado a gestão de riscos nos processos que envolvem dados sensíveis, bem como assegurar que haja uma aplicação concreta do *data protection by design and default*, observando-se com muito cuidado as bases legais do art. 11 da LGPD. Assim, se houver uma relação que revele dados sensíveis, isso, desde já, atrai um rol de dados mais restrito. Da mesma forma, é importante a elaboração de relatório de impacto à proteção de dados pessoais, quando houver um tratamento de dado sensível, especialmente de alto risco. O risco é um elemento que atrai, como regra, o relatório de impacto, e geralmente ao tratar dado sensível, haverá um elemento de risco, no mínimo, em âmbito médio. O relatório de risco se mostra como uma boa prática e extremamente importante para a proteção de dados.

O fluxo de dados que merece atenção, especialmente na área da saúde, é o fluxo de dados sensíveis que envolve hipervulneráveis: crianças, adolescentes, idosos, pessoas com deficiência ou pessoas que tenham uma vulnerabilidade agravada por condições particulares. Neste íterim, deve-se manter o olhar atento ao fluxo de dados e aos sujeitos, quando pensarmos na gestão de risco e no desenvolvimento de boas práticas.

Cabe destacar que a Autoridade Nacional de Proteção de Dados (ANPD) não fixou orientações específicas para os dados sensíveis de saúde, mas disciplinou parâmetros para o Tratamento de Dados Pessoais pelo Poder Público (Versão 2.0, jun./23), com foco no critério da avaliação da compatibilidade entre a finalidade original e o uso secundário de determinado caso, por exemplo, quando se utiliza um dado de saúde para monitorar uma política pública de vacinação ou para o compartilhamento de dados de pesquisa. Assim, conclui-se que há conformidade com o princípio da finalidade, desde que se garanta a pseudonimização ou a anonimização dos dados, nos termos do art. 13 e do Capítulo IV da LGPD³⁸.

Destacou-se também a hipótese, muito comum na área da saúde, da ocorrência de um novo compartilhamento ou transferência posterior dos dados, entre o receptor dos dados no âmbito do próprio setor público ou para entes do setor privado. A orientação fixada é no sentido de que, “entre outras possibilidades, o instrumento que rege o uso compartilhado dos dados pode vedar a realização de novo compartilhamento ou, ainda, autorizá-lo sob determinadas condições, observadas as normas

³⁸ AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo. Tratamento de Dados Pessoais pelo Poder Público**. Versão 2.0, jun. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 mar. 2026.

aplicáveis”³⁹, como exemplo citou o caso de dados pessoais disponibilizados para a realização de estudos em saúde pública, no qual se deve aplicar o critério estabelecido no artigo 13, § 2.º, da LGPD, que impõe ao órgão de pesquisa a responsabilidade pela segurança da informação e expressamente não permite, “em circunstância alguma, a transferência dos dados a terceiro”.

Na mesma seara da pesquisa na área da saúde, a ANPD reforçou a ideia da proteção jurídica especial dos dados sensíveis de saúde ao mencionar “a vedação de serem revelados dados pessoais sensíveis por ocasião da divulgação de resultados de estudos em saúde pública (art. 13, § 1º, LGPD)”⁴⁰, e fixou a orientação de que, nos casos de estudos em saúde pública, deve-se adotar medidas adicionais de prevenção e segurança para o tratamento de dados sensíveis, tais como o seu armazenamento em ambiente controlado e seguro, bem como, sempre que possível, a sua anonimização ou pseudonimização⁴¹.

O Ministério da Saúde publicou a Portaria GM/MS nº 3.232, de 1º de março de 2024, que instituiu o Programa SUS Digital, que, entre outros pontos, versou sobre os objetivos gerais e específicos, a abrangência, as diretrizes, a operacionalização, a coordenação e a governança, bem como as competências de cada esfera de governo do programa. Nesse contexto, o artigo 4º, II, da Portaria estabeleceu o conceito de “dado pessoal sensível de saúde” como sendo “dado relativo à saúde de um titular de dados ou à atenção à saúde a ele prestada que revele informações sobre sua saúde física ou mental no presente, passado ou futuro”.

Segundo Analluza Bolivas Dallari⁴²,

[...] a definição de “dado pessoal sensível de saúde” é um importante passo para ampliar a proteção de direitos fundamentais do titular-paciente, uma vez que “a Lei 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) não conceitua dados pessoais sensíveis (artigo 5º, II da LGPD)”. O conceito traçado pela Portaria GM/MS 3.232/2024 “condiz com a perspectiva ampliada de saúde, segundo o artigo 3º da Lei 8.080 de 19 de setembro de 1990, que versa sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes (Lei Orgânica da Saúde), estando alinhado, ainda, com o considerando 35 do Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016”.

³⁹ *Ibid.*, p. 34.

⁴⁰ *Ibid.*, p. 38.

⁴¹ *Ibid.*, p. 40-41.

⁴² DALLARI, Analluza Bolivar. SUS Digital e o conceito de dado pessoal sensível de saúde. **JOTA**, 26 mar. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/sus-digital-e-o-conceito-de-dado-pessoal-sensivel-de-saude-26032024>. Acesso em: 30 mar. 2026.

O conceito de “dado pessoal sensível de saúde”, adotado pelo Ministério da Saúde, dialoga com o § 1º, do artigo 11, da LGPD, uma vez que este atrai para as hipóteses do artigo 11 da LGPD o tratamento de dados pessoais, cuja finalidade revele, a depender das técnicas aplicadas de tratamento e de inferências cada vez mais sofisticadas, dados pessoais sensíveis e que, assim, possam causar dano ao titular.

Enfim, observa-se que a adoção do conceito de “dado pessoal sensível de saúde”, na Portaria do Ministério da Saúde, que alcança passado, presente e futuro, marca um avanço importante na proteção de direitos fundamentais de liberdade, de privacidade e do livre desenvolvimento da personalidade da pessoa natural titular de dados, no contexto da transformação digital da saúde.

6. CONSTRUÇÃO DE POLÍTICAS PÚBLICAS – CONTROLE E AVALIAÇÃO

A avaliação das políticas públicas foi um tema introduzido recentemente na Constituição Federal, pela Emenda Constitucional nº 109/2021, nos seguintes termos:

Art 37 - § 16. Os órgãos e entidades da administração pública, individual ou conjuntamente, devem realizar avaliação das políticas públicas, inclusive com divulgação do objeto a ser avaliado e dos resultados alcançados, na forma da lei.

Dessa forma, resta evidente que há necessidade de se criar uma política pública específica para a concretização da preservação dos dados de saúde na categoria de “dados sensíveis”, em especial para preservar os usuários do SUS, incluindo as ações no campo da saúde complementar. Como controladores, cabem aos gestores do SUS adotar as medidas harmônicas válidas para todos os níveis federais, com o fim de garantir a devida proteção em face de terceiros, e o acesso seguro ao titular do dado.

6.1. Tecnologia e Saúde: a Telemedicina e a Proteção de Dados

As experiências efetivas de telemedicina e telessaúde no Brasil tiveram início na década de 1990. Essas iniciativas aconteceram tanto na área pública quanto na área privada, além do âmbito de algumas universidades⁴³. Com a pandemia da covid-19, ocorreu uma grande oportunidade para a o crescimento da utilização da telemedicina, pois ela (a pandemia) forçou o isolamento social e, portanto, a necessidade, tanto do trabalho remoto como também do acesso de forma remota a uma série de serviços, incluindo a saúde.

⁴³ KHOURI, Sumaia Georges El. **Telemedicina**: análise da sua evolução no Brasil. 2003. Dissertação (Mestrado em Ciências) – Universidade de São Paulo, São Paulo, 2003. Disponível em: <https://teses.usp.br/teses/disponiveis/5/5160/tde-24102007-143128/publico/sumaiagekhour.pdf>. Acesso em: 30 mar. 2026.

A telemedicina é regulamentada pela Resolução CFM nº 2.314, de 20 de abril de 2022, considerando que cabe ao CFM disciplinar o exercício profissional médico e zelar pela boa prática médica no país, a qual segue como parâmetro a Declaração da World Medical Association (WMA) sobre os princípios éticos da telemedicina⁴⁴.

O artigo 1º da referida Resolução define a Telemedicina como o “exercício da medicina mediado por Tecnologias Digitais, de Informação e de Comunicação (TDICs), para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção de saúde”⁴⁵, sendo permitida, conforme o seu artigo 2º, em tempo real *on-line* (síncrona) ou *off-line* (assíncrona), dentro do território nacional.

Pode ser exercida nas seguintes modalidades de teleatendimentos médicos: i) Teleconsulta; ii) Teleinterconsulta; iii) Telediagnóstico; iv) Telecirurgia; v) Telemonitoramento ou televigilância; vi) Teletriagem; vii) Teleconsultoria (art. 5º).

Importante destacar que, conforme estabelece o parágrafo único do artigo 15 da citada Resolução, em todo atendimento por telemedicina deve ser assegurado o consentimento explícito, no qual o paciente ou seu representante legal deve estar consciente de que as suas informações pessoais podem ser compartilhadas e sobre o seu direito de negar permissão para isso, salvo em situação de emergência médica.

Deve ser assegurado que as pessoas jurídicas que prestarem serviços de telemedicina, plataformas de comunicação e arquivamento de dados, deverão ter sede estabelecida em território brasileiro e estar inscritas no Conselho Regional de Medicina do Estado, onde estão sediadas, com a respectiva responsabilidade técnica de médico, regularmente inscrito no mesmo Conselho (artigo 17). No caso de o prestador ser pessoa física, deverá ser médico devidamente inscrito no Conselho Regional de Medicina de sua jurisdição e informar a entidade a sua opção de uso de telemedicina.

Nesse contexto, é necessário zelar pelo respeito ao Código de Ética Médica, considerando o grande fluxo de dados e informações que se estabelece entre médicos e entre médicos e pacientes.

O CFM fixa diretrizes a serem seguidas, partindo do pressuposto de que a consulta médica presencial é o padrão a ser seguido. A relação cada vez mais tecnológica entre médicos e pacientes, deve visar ao benefício e aos melhores resultados ao paciente. Assim, o médico deve avaliar se a telemedicina é o método mais adequado às necessidades do paciente, naquela situação determinada.

Os dados e imagens dos pacientes constantes nos registros do prontuário devem ser preservados nos termos da lei e das orientações do CFM, pertinentes à guarda, ao manuseio, à integridade, à veracidade, à confidencialidade, à privacidade, à irrefutabilidade e à garantia do sigilo profissional das informações, por meio do

⁴⁴ WORLD MEDICAL ASSOCIATION (WMA). **Declaración de la AMM sobre la ética de la telemedicina**. 2018. Disponível em: <https://www.wma.net/es/polices-post/declaracion-de-la-amm-sobre-la-etica-de-la-telemedicina/>. Acesso em: 30 mar. 2026.

⁴⁵ CFM. **Resolução CFM nº 2.314/2022**, *op. cit.*, art. 1º.

prontuário médico físico ou no uso de sistemas informacionais, em Sistema de Registro Eletrônico de Saúde (SRES) do paciente, atendendo aos padrões de representação, terminologia e interoperabilidade.

Cabe destacar o art. 3º § 2º da Resolução CFM nº 2.314:

Art. 3. § 2º O SRES utilizado deve possibilitar a captura, o armazenamento, a apresentação, a transmissão e a impressão da informação digital e identificada em saúde e atender integralmente aos requisitos do Nível de Garantia de Segurança 2 (NGS2), no padrão da infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito⁴⁶.

Os dados relacionados ao atendimento realizado via telemedicina, como os de anamnese e dados propedêuticos, resultados de exames complementares e a conduta médica adotada, devem ser preservados, conforme a legislação vigente, sob guarda do médico responsável pelo atendimento em consultório próprio ou do diretor/responsável técnico, no caso de interveniência de empresa e/ou instituição (art. 3º, § 3º, Resolução CFM nº 2.314).

É importante destacar, na área da saúde complementar, que, em caso de contratação de serviços terceirizados de arquivamento, a responsabilidade pela guarda de dados de pacientes e do atendimento deve ser contratualmente compartilhada entre o médico e a contratada, de modo que o SRES deve propiciar interoperabilidade/intercambialidade, com utilização de protocolos flexíveis, pelos quais dois ou mais sistemas possam se comunicar de forma eficaz e com garantia de confidencialidade, privacidade e integridade dos dados (art. 3º, §§ 4º e 5º, Resolução CFM nº 2.314).

Importante ressaltar que, a telemedicina não se resume ao atendimento paciente-médico por meio de uma ferramenta tecnológica. Ela envolve vários instrumentos: o estabelecimento de saúde, uma plataforma de emissão de documentos médicos eletrônicos, a farmácia etc., ou seja, os instrumentos que envolvem a telemedicina são interconectados com diversos operadores de dados da saúde e outros que não são da área da saúde, que não têm licença sanitária, como as plataformas de emissão de documentos médicos eletrônicos.

Ademais, a videoconferência é apenas uma pequena parcela da telemedicina, como explica o Professor Chao Lung Wen ⁴⁷:

A telemedicina, mais do que um recurso tecnológico para proporcionar atividades a distância, a telemedicina adquire efetividade quando ela está associada a um plano estratégico de saúde e vinculado a um processo de logística de distribuição de serviços de saúde.

⁴⁶ *Ibid.*, art. 3º, § 2º.

⁴⁷ WEN, Chao Lung. Telemedicina e a telessaúde: uma abordagem sob a visão de estratégia de saúde apoiada por tecnologia. **Chao Lung Wen**, 30 jan. 2002. Disponível em: <https://chaowen.med.br/artigos/telemedicina-e-a-telessaude-uma-abordagem-sob-a-visao-de-estrategia-de-saude-apoiada-por-tecnologia/>. Acesso em: 30 mar. 2026.

Melhor dizendo, a telemedicina não é uma ferramenta, mas um método que vai desde o paciente adentrar a plataforma, ter sua identidade verificada, ocorrer a elegibilidade do serviço, até a adequação da tecnologia, ou seja, a verificação de se o paciente está em condições de conectividade, a realização da consulta, a emissão de documentos e a obtenção do consentimento informado.

A telemedicina é um método de se praticar a medicina, sem grandes diferenças no raciocínio clínico médico ou nas condutas adotadas, estando o paciente a distância ou presencial. No entanto, o intuito principal é a transparência das informações, o paciente precisa saber quais são as limitações do método, e o termo de consentimento ajudará a cientificá-lo.

Hoje a telemedicina não é limitada por questões tecnológicas. No entanto, o que há são barreiras de processo, ou seja, de como você implementa um processo de atendimento que seja seguro, que garanta a privacidade dos dados e que garanta a boa prática da medicina.

Nesse aspecto, é importante tratar com muito cuidado a gestão de riscos nos processos que envolvem dados sensíveis, bem como assegurar que haja uma aplicação concreta do *data protection by design and default*, observando-se com muito cuidado as bases legais do art. 11 da LGPD. Havendo uma relação que revele dados sensíveis, isso, desde já, atrai um rol de dados mais restrito. Nesta esteira, faz-se muito importante a elaboração de relatório de impacto à proteção de dados pessoais, quando houver um tratamento de dado sensível, especialmente de alto risco.

7. CONCLUSÃO

A proteção de dados pessoais sensíveis de saúde ganha relevância e novos desafios de forma diretamente proporcional ao desenvolvimento de novas tecnologias e inovações na área da saúde. Se, por um lado, a evolução da medicina proporciona a produção de ferramentas que garantem melhor qualidade e mais precisão na prevenção e no tratamento de doenças, bem como, o aprimoramento da modelagem das políticas públicas, com a otimização da coleta de dados mais precisos e da identificação das necessidades de cada região de saúde, por outro, há patente risco na manipulação e no aumento do tráfego de dados, considerando que os dados pessoais dos pacientes tornam-se ativos valiosos para os governos e empresas, sujeitos a abusos, violações de privacidade, roubo de identidade e outros tantos crimes cibernéticos.

O desafio é compor, de forma harmônica e segura, várias realidades interligadas, as quais devem evoluir de forma conjunta na proteção dos dados, em suas várias dimensões: inovação em saúde, proteção dos direitos fundamentais do indivíduo e transparência.

A questão perpassa pelos desafios impostos pela enorme rede hierarquizada e regionalizada que delineiam o projeto constitucional do SUS, um dos maiores do mundo, o que demonstra a necessidade de se harmonizar o tema em todos os níveis

da federação, por meio de políticas públicas específicas, visando à devida regulamentação e à oferta da infraestrutura necessária para lidar com os dados gerados, bem como educar os usuários do SUS, médicos e todos que compõem a área de saúde e burocrática a adotarem boas práticas, controlarem e avaliarem as políticas públicas com a eficiência e rapidez que a área da evolução tecnológica requer.

A definição de “dados pessoais sensíveis de saúde” deve coincidir com a extensa concepção da própria noção de saúde, a qual considera como determinantes e condicionantes que contemplem, inclusive, o bem-estar físico, mental e social, segundo o artigo 3º da LOS. Pois bem, perfazendo este “conceito ampliado de saúde” conforme o § 1º do artigo 11 da LGPD, dados pessoais em princípio “comuns”, como a geolocalização, a depender dos cruzamentos e inferências, podem revelar dados pessoais sensíveis de saúde, mitigando a tese da taxatividade estática do artigo 5º, II, da LGPD.

A tele saúde é uma realidade prevista na Lei Federal n.º 14.510/2022 que alterou a LOS, sendo reconhecida a modalidade de teleatendimento dentro da cadeia de serviços do SUS. Toda a construção de sua implementação pressupõe respeito aos termos da LGPD, considerando que a proteção dos dados pessoais vai fornecer as bases para a confiança dos cidadãos nas instituições públicas e privadas no ambiente digital, sendo essencial para fortalecer a proteção efetiva dos direitos fundamentais individuais.

A legislação brasileira, ao contrário do Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, GDPR⁴⁸, não definiu diretamente o conceito de “dados pessoais relativos à saúde”. Cabe ao intérprete buscar essa definição no quadro legislativo atual e acompanhar o desdobramento do tema por meio das orientações da ANPD, pela própria compreensão do problema pelos gestores do SUS e pelo aprimoramento dos instrumentos jurídicos, com foco na relação titular–controlador–operador–encarregado–agentes de tratamento, em especial, nos convênios e contratos de gestão de saúde e, eventualmente, em decisões judiciais.

Faz-se, então, necessário construir, a partir da ideia de dados pessoais sensíveis, balizas para garantir o trâmite dos dados na área da saúde, incluindo a criação de mecanismos claros e a compreensão de como será realizado o tratamento dos dados, com o fim de garantir os princípios gerais de proteção e os direitos do titular, como o direito de acesso, bloqueio, eliminação e transferência.

A ANPD não fixou orientação específica para os dados sensíveis de saúde, mas disciplinou parâmetros para o “Tratamento de Dados Pessoais pelo Poder Público” (Versão 2.0, jun./23), com foco no critério da avaliação da compatibilidade entre a finalidade original e o uso secundário de determinado caso, com foco nos dados na área das pesquisas em saúde, como o compartilhamento, a transferência, a anonimização ou a pseudonimização dos dados.

⁴⁸ UNIÃO EUROPEIA. **Regulation (EU) 2016/679...** (GDPR). *op. cit.*

O Ministério da Saúde traçou paradigmas na Portaria GM/MS nº 3.232/2024, em consenso com a perspectiva ampliada de saúde, segundo o artigo 3º da LOS e com o Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, no sentido de que dado pessoal sensível de saúde é aquele “dado relativo à saúde de um titular de dados ou à atenção à saúde a ele prestada que revele informações sobre sua saúde física ou mental no presente, passado ou futuro” (artigo 4º, inciso II).

O conceito de “dado pessoal sensível de saúde” vem sendo construído no âmbito nacional, com a importante introdução da dimensão de tempo e espaço – no passado, presente e futuro –, representando um avanço importante na proteção de direitos fundamentais de liberdade, de privacidade e do livre desenvolvimento da personalidade da pessoa natural titular de dados, no contexto da transformação digital da saúde.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo. Tratamento de Dados Pessoais pelo Poder Público**. Versão 2.0, jun. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 mar. 2026.

AMARAL, Igor Silva, *et al.* Segurança cibernética para dispositivos móveis. **Revista Multidisciplinar do Nordeste Mineiro**, Teófilo Otoni, v. 1, n. 1, 2024. Disponível em: <https://pdfs.semanticscholar.org/a614/b93eed8282012a0c503d1c771a123b5c99d8.pdf>. Acesso em: 30 mar. 2026.

ARAUJO, Alex Rodrigues. **Métodos e técnicas de segurança para dispositivos IOT: uma revisão sistemática da literatura**. 2023. Monografia (Superior em Telemática) – Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campina Grande, 2023, Disponível em: <https://repositorio.ifpb.edu.br/bitstream/177683/3547/1/Araujo%2C%20Alex%20Rodrigues%20-%20TCC.pdf>. Acesso em: 30 mar. 2026.

BAHIA, Claudio José Amaral, *et al.* Direito à proteção de dados: trajetória e delineações do reconhecimento como um direito fundamental autônomo no Brasil. **Revista da Faculdade de Direito da UERJ**, Rio de Janeiro, n. 43, 2024. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rfduerj/article/view/67486?utm_source=chatgpt.com. Acesso em: 30 mar. 2026.

BARBOSA, Wuerles Bessa, *et al.* Impacto da telemedicina na prestação de cuidados de saúde em áreas rurais e remotas. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 8, p. 191-201, 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/10855?utm_source=chatgpt.com. Acesso em: 30 mar. 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial**, Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 abr. 2026.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 abr. 2026.

BRASIL. Lei nº 8.080, de 15 de dezembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. **Diário Oficial**, Brasília, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 30 mar. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 mar. 2026.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial**, Brasília, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 8 abr. 2026.

BRASIL. Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da tele saúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14510.htm. Acesso em: 30 mar. 2026.

BRASIL. **Guia de boas práticas para implementação na Administração Pública Federal**. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 30 mar. 2026.

CARVALHO, Lucas Borges de. O Poder Público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 282, n. 2, p. 133-162, 2023.

CONFEDERAÇÃO NACIONAL DE SAÚDE. **Código de boas Práticas: Proteção de dados para Prestadores Privados de Serviços em Saúde**. Brasília: CNSaúde, 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 mar. 2026.

CONSELHO DA JUSTIÇA FEDERAL (CJF). **IX Jornada Direito Civil**: comemoração dos 20 anos da Lei nº 10.406/2002 e da instituição da Jornada de Direito Civil: enunciados aprovados. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022.

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.314/2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. **Diário oficial**, Brasília, 5 maio 2022, Seção I, p. 227.

COSTA, Gustavo Amancio da; LIMA, Miqueias Sales de. **Exploração de vulnerabilidades em sistemas operacionais Linux**. 2023. Monografia (Bacharel em Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”, Americana, 2023. Disponível em: <https://ric.cps.sp.gov.br/handle/123456789/15462>. Acesso em: 30 mar. 2026.

COSTA JUNIOR, Jose Cassio. **Os desafios da Lei Geral de Proteção de Dados para pequenas empresas**: um estudo de caso em uma distribuidora em Natal/RN. 2023. Monografia (Bacharel em Administração) – Universidade Federal do Rio Grande do Norte, Natal, 2023. Disponível em: <https://repositorio.ufrn.br/server/api/core/bitstreams/da63035a-ad57-4151-810e-57614745c088/content>. Acesso em: 30 mar. 2026.

DALLARI, Analluza Bolivar. SUS Digital e o conceito de dado pessoal sensível de saúde. **JOTA**, 26 mar. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/sus-digital-e-o-conceito-de-dado-pessoal-sensivel-de-saude-26032024>. Acesso em: 30 mar. 2026.

GRANEMANN, Gabriel Maddalozzo. **Fatores que influenciam a intenção de uso da telemedicina no Brasil pelos pacientes**: um estudo exploratório via modelagem estrutural. 2021. Monografia (Bacharel em Engenharia de Produção) – Universidade de Brasília, Brasília, 2021. Disponível em: https://bdm.unb.br/bitstream/10483/34143/1/2021_GabrielMaddalozzoGranemann_tcc.pdf. Acesso em: 30 mar. 2026.

KHOURI, Sumaia Georges El. **Telemedicina**: análise da sua evolução no Brasil. 2003. Dissertação (Mestrado em Ciências) – Universidade de São Paulo, São Paulo, 2003. Disponível em: <https://teses.usp.br/teses/disponiveis/5/5160/tde-24102007-143128/publico/sumaiaagekhouri.pdf>. Acesso em: 30 mar. 2026.

NIUKA, Josias Kuingua Bernardo. **A Proteção de Dados Pessoais de Saúde à luz do RGPD**. 2023. Dissertação (Mestrado) – Universidade de Coimbra, Faculdade de Direito, Coimbra, 2023. Disponível em: https://estudogeral.uc.pt/retrieve/265833/Dissertac%CC%A7a%CC%83o%20juri%CC%81dico-forense%20Mestrado_Josias%20Niuka_12jun23.pdf. Acesso em: 30 mar. 2026.

OLIVEIRA, Larissa de Jesus; NOVAIS, Thyara Gonçalves. Lei geral de proteção de dados pessoais: responsabilidade civil no vazamento de informações. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 5, p. 1614-1631, 2024. Disponível em: <https://periodicorease.pro.br/rease/article/view/13668>. Acesso em: 30 mar. 2026.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Constituição da Organização Mundial da Saúde**. Genebra: OMS, 1946.

PROMULGADA emenda constitucional de proteção de dados. **Agência Senado**, 10 fev. 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados>. Acesso em: 8 abr. 2026.

SANTOS, Beatriz Freitas. Lei Geral de Proteção de Dados (LGPD) e a garantia de proteção dos direitos fundamentais de liberdade e de privacidade dos cidadãos a luz do Direito Constitucional. **Aporia Jurídica**, Ponta Grossa v. 1, n. 19, 2023.

SARLET, Ingo. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Consultor Jurídico**, 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/>. Acesso em: 30 mar. 2026.

SILVA, Angélica Baptista. **Telessaúde no Brasil: conceitos e aplicações**. Rio de Janeiro: Editora DOC, 2014.

SILVA, Kaian Notier Gomes da; OLIVEIRA, Rômulo de Moraes. Conflito entre o princípio da publicidade tratado na lei 6.015/73 e os dados sensíveis tratados pela Lei Geral de Proteção de Dados-LGPD nas serventias extrajudiciais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 5, p. 2091-2107, 2024. Disponível em: <https://periodicorease.pro.br/rease/article/view/13986>. Acesso em: 30 mar. 2026.

SOBROZA, Bianca Amaral; ARRUDA, Juliana Gonçalves de; MARINI, Bruno. Vazamento de dados pessoais sensíveis de pacientes atendidos por instituições de saúde como forma de violência hospitalar: uma análise global sob o viés da bioética e do biodireito. **Revista de Direito Magis**, Betim, v. 2, n. 1, 2023. Disponível em: <https://periodico.agej.com.br/index.php/revistamagis/article/view/44>. Acesso em: 30 mar. 2026.

SOUZA, Julio César de. **Um estudo de caso sobre medidas de segurança para preservar a confidencialidade e integridade das informações**. 2024. Monografia (Bacharel em Engenharia da Computação) – Universidade Federal de Mato Grosso, Várzea Grande, 2024. https://bdm.ufmt.br/bitstream/1/3954/1/TCC_2024_Julio%20C%C3%A9sar%20de%20Souza.pdf. Acesso em: 30 mar. 2026.

TEFFÉ, Chiara Spadaccini de. **Problemas de direito civil: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos**. Rio de Janeiro: Forense, 2021.

UNIÃO EUROPEIA. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR)**. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>. Acesso em: 30 mar. 2026

WEN, Chao Lung. Telemedicina e a telessaúde: uma abordagem sob a visão de estratégia de saúde apoiada por tecnologia. **Chao Lung Wen**, 30 jan. 2002. Disponível em: <https://chaowen.med.br/artigos/telemedicina-e-a-telessaude-uma-abordagem-sob-a-visao-de-estrategia-de-saude-apoiada-por-tecnologia/>. Acesso em: 30 mar. 2026.

WERNER, Patricia Ulson Pizarro. Direito à saúde. In: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (coord.). **Enciclopédia jurídica da PUC-SP**. 2. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/170/edicao-2/direito-a-saude>. Acesso em: 30 mar. 2026.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: MENDES, Laura, *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

WORLD MEDICAL ASSOCIATION (WMA). **Declaración de la AMM sobre la ética de la telemedicina**. 2018. Disponível em: <https://www.wma.net/es/policies-post/declaracion-de-la-amm-sobre-la-etica-de-la-telemedicina/>. Acesso em: 30 mar. 2026.

Submetido em: 02/12/2024

Aprovado em: 16/09/2025

