**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO**

**PUC-SP**

**FACULDADE DE DIREITO**

**GIULIA MARTTA GUERRINI**

# OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NA TELEMEDICINA: A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA PROTEÇÃO DE DADOS SENSÍVEIS

SÃO PAULO

2025

GIULIA MARTTA GUERRINI

# OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NA TELEMEDICINA: A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA PROTEÇÃO DE DADOS SENSÍVEIS

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Pontifícia Universidade Católica de São Paulo para obtenção do título de bacharel em Direito.

Orientadora: Prof.ª Dra. Flávia de Campos Pinheiro

SÃO PAULO

2025

Aos meus pais, que sob o Sol, fizeram-me chegar até aqui, na sombra.

## AGRADECIMENTOS

À minha mãe, Vivian Izilda Martta Guerrini, que nunca duvidou da minha capacidade e sempre disse que eu iria conseguir — e eu consegui. Cada conquista minha carrega um reflexo da sua coragem, da sua persistência e da sua força.

Ao meu pai, Laercio Guerrini, que sempre encontrou as palavras certas nos momentos fáceis e, sobretudo, nos difíceis. O meu maior exemplo de sabedoria, integridade e serenidade.

À minha irmã, Larissa Guerrini e ao meu irmão, Leandro Guerrini, que sempre foram minha referência de apoio e permaneceram ao meu lado em cada etapa da minha vida.

Ao meu namorado, Gabriel Andres Silva Garcia Martinez, que esteve junto a mim muito antes desta jornada iniciar. Com quem eu dividi a minha juventude e escolhi para ser o único amor de todas as vidas que eu venha a ter, além desta.

Aos demais familiares, que através da força das nossas raízes, o afeto dos encontros e a confiança depositada em mim foram pilares fundamentais ao longo dessa caminhada.

Às minhas queridas amigas, Ana Clara Beraldo, Amanda Mainini, Gabriela Vianna, Maria Fernanda Melo e Valentina Sampaio que me acompanharam nesta jornada desde os primeiros dias de aula até a tão sonhada aprovação no Exame da Ordem. Em meio a tantas pessoas, nos reconhecemos e escolhemos permanecer juntas, criando um laço que resistiu ao tempo, às incertezas da vida e aos desafios da graduação. Vocês transformaram essa travessia em algo memorável, leve e genuinamente bonito. Existimos juntas e resistimos juntas. A amizade de vocês foi abrigo, respiro e alegria.

Obrigada a todos, em cada conquista minha, há um pedaço da força que recebi de vocês.

Esse diploma é, também, de vocês.

*“Ain't about how fast I get there,*

*Ain't about what's waiting on the other side,*

*It's the climb. ”*

*(The Climb - Miley Cyrus)*

## RESUMO

GUERRINI, Giulia Martta. **Os desafios da segurança da informação na telemedicina: A aplicação da Lei Geral de Proteção de Dados na proteção de dados sensíveis.**

O presente trabalho tem por objetivo investigar os desafios enfrentados na proteção dos dados sensíveis no contexto da telemedicina, à luz da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD). A pesquisa parte do reconhecimento de que a saúde digital tem se expandido significativamente, especialmente após a pandemia de COVID-19, impulsionando o uso de plataformas de teleatendimento médico e, por consequência, elevando a exposição de informações pessoais e sensíveis dos pacientes.

Nesse sentido, foram abordados os principais aspectos legais relacionados à proteção de dados sensíveis, como os fundamentos constitucionais da privacidade, os direitos dos titulares e as obrigações dos agentes de tratamento, analisando sua aplicação prática na telemedicina. Destacam-se, também, os riscos jurídicos, como vazamentos, acessos indevidos e uso não autorizado de informações, bem como a responsabilidade civil decorrente do descumprimento da LGPD.

Por fim, o estudo objeto deste trabalho destaca a relevância da adoção de estratégias eficazes de gestão de dados pessoais sensíveis e de conformidade digital como pilares essenciais de garantia de proteção de privacidade e da saúde dos indivíduos nas interações médicas virtuais.



**Palavras-chave:** telemedicina; dados sensíveis; privacidade; saúde digital; LGPD; direito à saúde.

## ABSTRACT

GUERRINI, Giulia Martta. **The challenges of information security in telemedicine: The application of the General Data Protection Law in the protection of sensitive data.**

This study aims to investigate the challenges faced in protecting sensitive data within the context of telemedicine, under the framework of the Brazilian General Data Protection Law (Law No. 13.709/2018 – LGPD). The research begins with the acknowledgment that digital health has significantly expanded, especially after the COVID-19 pandemic, boosting the widespread use of telemedicine platforms and, consequently, increasing the exposure of patients personal and sensitive information.

In this context, it was addressed key legal aspects related to the protection of sensitive data, such as the constitutional foundations of privacy, the rights of data subjects, and the duties of data controllers and processors, analyzing their practical application in telemedicine. It also highlights legal risks, including data breaches, unauthorized access, and improper use of information, as well as the civil liability resulting from non-compliance with the LGPD.

Finally, the study that is the subject of this work highlights the relevance of adopting sensitive personal data management and digital compliance strategies as essential pillars for guaranteeing the protection of privacy and the health of individuals in virtual medical interactions.



**Keywords:** telemedicine; sensitive data; privacy; digital health; LGPD; right to health.

## SUMÁRIO

## INTRODUÇÃO

O presente tema decorre do aumento da relevância da telemedicina como instrumento de alternativa ao acesso à saúde e, simultaneamente, da preocupação com a segurança das informações sensíveis dos pacientes no ambiente digital. Com a evolução da tecnologia e a consolidação de atendimentos médicos à distância, especialmente após a pandemia do Covid-19, fez-se presente a reflexão sobre os limites e as responsabilidades legais no tratamento de dados pessoais no setor da saúde.

A telemedicina, enquanto prática inovadora, representa não apenas uma mudança no paradigma na forma da prestação de serviços da saúde, mas um desafio ético e jurídico. Assim, intentou-se em demonstrar a dualidade desta nova prática, ao passo que expande o acesso ao atendimento médico, mas ao mesmo tempo incorre em riscos de exposição de dados sensíveis relacionados aos seus consumidores/usuários.

A partir dos dilemas acompanhados no contexto internacional, com a promulgação do Regulamento Geral de Proteção de Dados (GDPR) pela União Europeia, o Brasil alinha a sua legislação com as tendências internacionais, de forma que entrou em vigor a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Nesse sentido, a proteção de dados sensíveis em ambientes digitais ganhou destaque, de forma que o tratamento de informações pessoais, incluindo aquelas relativas à saúde, passou a ser disciplinado de forma ampla. Em sequência, o ordenamento jurídico constitucional elevou a proteção de dados ao patamar de direito fundamental com a promulgação da Emenda Constitucional nº 115/2022.

O imbróglio deste tema encontra-se na tensão entre o avanço tecnológico e a efetiva proteção dos direitos fundamentais. Assim, este trabalho busca contribuir para a análise crítica do arcabouço normativo brasileiro à luz da realidade prática da telemedicina, compreendendo até que ponto a Lei Geral de

Proteção de Dados tem sido suficiente para garantir a segurança da informação e a efetivação do direito à saúde em sua dimensão digital.

Para a construção deste trabalho foi utilizado o método de pesquisa bibliográfica, com base em artigos científicos, monografias, teses de mestrado e doutorado que tratam da proteção de dados sensíveis, segurança da informação, telemedicina e direito à saúde no contexto da legislação brasileira. Assim selecionadas e integralmente revisadas, permitindo a identificação de temas e contribuições relevantes inerentes ao tema.

Para tanto foram consultadas publicações disponíveis em bibliotecas digitais e repositórios acadêmicos, como SciELO, Repositório Institucional da PUC, Fiocruz e demais instituições acadêmicas, que possibilitaram uma análise crítica e atualizada da aplicação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) no âmbito da saúde digital.

Além disso, utilizou-se também de jurisprudências extraídas de tribunais e notícias que versam sobre proteção de dados, responsabilidade civil por vazamento de informações de saúde e conflitos entre inovação tecnológica e direitos fundamentais, demonstrando que a proteção jurídica, embora robusta em teoria, ainda enfrenta tensões em sua aplicação prática.

## 1. DIREITOS FUNDAMENTAIS E A PROTEÇÃO DE DADOS NA ERA DIGITAL

### 1.1. O conceito e a evolução dos direitos fundamentais

Os direitos fundamentais, em seu sentido contemporâneo, correspondem a um conjunto de garantias reconhecidas aos indivíduos diante do Estado, assegurando-lhes dignidade, liberdade e igualdade e entre outros. Norberto Bobbio define os direitos do homem como "*direitos históricos*", ou seja, construídos e reconhecidos em diferentes contextos sociais e políticos ao longo do tempo (BOBBIO, 1992).

Desta forma, o conceito de direitos fundamentais precede a atualidade, transitando desde a Antiguidade e a Idade Média até chegar ao que se entende

hoje por "*a era dos direitos*", na qual o indivíduo passa a ser titular de direitos oponíveis ao Estado (BOBBIO, 1992).

Anterior ao protagonismo do homem como centro de perspectiva do mundo, o Estado articulava-se como o poder centralizador e, então, o paradigma trouxe uma mudança a partir da compreensão de que a dignidade humana seria anterior à do próprio Estado. Esta ideia surge originariamente a partir do pensamento jusfundamentalista no século XVI, o qual os direitos fundamentais emergem com a chamada Escola Ibérica da Paz, um conjunto de teólogos e juristas ibéricos que, durante a colonização das Américas, desenvolveram uma crítica revolucionária às práticas colonizadoras de seu tempo.

Em contraposição ao ideal de guerra, a conversão forçada e a escravização de povos indígenas, estes autores propuseram uma visão radicalmente inovadora e humanista, afirmando existência de um "ser humano universal", dotado de razão e dignidade próprias, que independe de pertença religiosa ou cultural (FRANÇA, 2022). A concepção universalista dos ibéricos à aquela época conquistou uma concepção jurídica crítica que coloca os direitos fundamentais acima dos interesses individuais, consolidando mais tarde a base principiológica acerca da dignidade humana, liberdade, igualdade e outros.

Com o Iluminismo e as Revoluções Burguesas dos séculos XVII e XVIII, esse entendimento começou a se consolidar em documentos jurídicos e políticos. A Declaração de Direitos do Homem e do Cidadão de 1789, por exemplo, consagrou o direito à liberdade, à igualdade perante a lei e à propriedade. Nesse contexto, o Estado, assim como mencionado pelos ibéricos, passa a ser visto não mais como expressão da vontade divina, mas como uma construção racional, que só é legítima se respeitar certos limites, sendo estes os direitos fundamentais.

A partir dessa evolução, a doutrina passa a organizar os direitos fundamentais a partir de suas "*dimensões*" ou "*gerações*", correspondendo às camadas sucessivas de conquista de liberdades e garantias.

A primeira geração refere-se aos direitos civis e políticos, surgidos no liberalismo e das revoluções burguesas do final do século XVIII, tratando-se de

uma prestação negativa do Estado, onde este se abstém de exercer sua defesa e poder e, então, abre-se espaço para autonomia individual (ARAÚJO; NUNES JÚNIOR, 2021).

Já a segunda geração corresponde aos direitos econômicos, sociais e culturais, que ganharam força no século XX, demandando, neste plano, a prestação positiva do Estado para o exercício destes direitos (ARAÚJO; NUNES JÚNIOR, 2021).

Por fim, a terceira geração, delineada a partir da segunda metade do século XX, abrange os direitos difusos e coletivos, caracterizado por uma transindividualidade, ou seja, inerentes à coletividade e ao próprio indivíduo (ARAÚJO; NUNES JÚNIOR, 2021).

Nesse sentido, observou-se que desde o conceito e a caracterização dos direitos fundamentais, estes perpassam por um lento processo histórico, até a sua afirmação nos dias de hoje. As contribuições das vozes dissonantes da Escola Ibérica da Paz estruturam-se em documentos jurídicos de direitos que, posteriormente, foram definidos em camadas de dimensões para proteção de todas as esferas de direitos.

No entanto, como bem observa Norberto Bobbio, "*o problema fundamental em relação aos direitos do homem, hoje, não é tanto o de justificá-los, mas o de protegê-los*" (BOBBIO,1992), de modo que, ainda que haja o seu reconhecimento, o cerne da reflexão encontra-se em tornar efetivos e invioláveis os direitos fundamentais.

## 1.2. O direito fundamental à proteção de dados pessoais: a Emenda Constitucional nº 115/2022

O avanço digital reflete diretamente na urgência de uma articulação da proteção jurídica dos dados pessoais. Ocorre que a vastidão de conteúdos e informações que circulam online expõem, inevitavelmente, uma quantidade sem precedentes de dados. Diante desse cenário, observou-se que a tutela da privacidade tradicional, embora fundamental, era insuficiente diante do volume de dados pessoais circulando na rede.

Inicialmente, é preciso distinguir o direito à privacidade do direito à proteção de dados pessoais, que *à priori* apresentam-se como conceitos relacionados, porém são distintos na teoria jurídica contemporânea.

A privacidade remete ao resguardo da vida privada e à ausência de intromissões indevidas na esfera pessoal, classicamente definida como o "*direito de ser deixado só; estar a salvo de interferências alheias*" (BIONI, 2021).

Já a proteção de dados pessoais vai além do mero sigilo ou intimidade, diz respeito ao controle sobre as informações pessoais que identificam ou possibilitam identificar alguém, bem como às regras para seu tratamento adequado. Por exemplo, nome, localização, preferências de consumo e até mesmo números identificadores (como *Internet Protocol* ou Cadastro de Pessoa Física) são considerados dados pessoais, pois se referem a uma pessoa identificada ou identificável (PINHEIRO, 2020).

Nesse sentido, os dados supracitados podem não ser sigilosos por natureza. Contudo, a maneira como são coletados, armazenados e compartilhados, a depender, podem impactar diretamente direitos e liberdades individuais, daí surgindo a necessidade de proteção jurídica específica.

No ordenamento brasileiro, a privacidade e a intimidade são direitos fundamentais expressos na Constituição Federal de 1988 (art. 5º, X), que garante a inviolabilidade da vida privada, da intimidade, da honra e da imagem. Esses direitos tradicionais garantem ao indivíduo um espaço de refúgio contra divulgações não autorizadas de aspectos de sua vida pessoal.

No entanto, com o avanço tecnológico e a complexidade crescente das interações digitais, reconheceu-se que os dados pessoais mereciam proteção mais abrangente. Estes transcendem o conceito de intimidade *stricto sensu*, envolvendo informações que, conforme mencionado, ainda que não sigilosas, podem ser utilizadas de maneira a influenciar perfis, comportamentos e decisões sobre a pessoa.

É possível inferir a existência de um direito fundamental implícito à proteção de dados como corolário do princípio da dignidade da pessoa humana,

ligado especialmente ao livre desenvolvimento da personalidade do indivíduo (SARLET, 2020). Em 2020, esse entendimento ganhou força jurisprudencial: o Supremo Tribunal Federal, ao suspender os efeitos da Medida Provisória 954/2020 (que determinava o compartilhamento massivo de dados telefônicos ao IBGE), reconheceu expressamente o direito fundamental à autodeterminação informativa, isto é, o direito de cada pessoa controlar os próprios dados pessoais, como integrante dos direitos da personalidade e da privacidade (VALENTE, 2020).

Paralelamente, a legislação brasileira avançou para positivar a proteção de dados pessoais. A aprovação da Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em 2020, estabeleceu princípios, direitos dos titulares e obrigações para agentes de tratamento de dados, inspirada em legislações estrangeiras como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

Ainda assim, verificava-se que faltava consolidar o status constitucional dessa proteção. Por isso, tramitou no Congresso Nacional a Proposta de Emenda à Constituição nº 17/2019, de iniciativa do Senado Federal, visando incluir expressamente a proteção de dados pessoais entre os direitos fundamentais.

A proposta foi aprovada em ambas as Casas Legislativas sem grandes resistências, refletindo um consenso sobre a relevância do tema, e, resultando, na Emenda Constitucional nº 115, de 10 de fevereiro de 2022 (SENADO FEDERAL, 2022).

Assim, com a promulgação da EC 115/2022, o Brasil passou a reconhecer no texto magno o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais. A Emenda acrescentou o inciso LXXIX ao art. 5º da Constituição Federal:

> "*Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à*

> *liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
>
> *LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais*. (BRASIL, 2022)

Em síntese, pode-se afirmar que a Emenda Constitucional 115/2022 não só constitucionalizou a proteção de dados, mas também a elevou a um patamar autônomo e hierarquicamente superior no ordenamento jurídico, alinhando-a aos demais direitos e garantias fundamentais (ACIOLY *et al*., 2024).

Atualmente, em uma era dominada por *big data* e inteligência artificial, o controle sobre as informações pessoais se torna um pilar essencial não apenas para o pleno exercício do direito à proteção de dados, mas também para a garantia de princípios como a dignidade humana e a liberdade individual.

## 2. TELEMEDICINA E O TRATAMENTO DE DADOS NO DIREITO À SAÚDE

### 2.1. O conceito de telemedicina e seu avanço no acesso à saúde

A telemedicina é definida, segundo o Dicionário da Academia Brasileira de Letras, como a "*prática médica exercida à distância, por meio de chamadas de vídeo e/ou outras tecnologias da comunicação e da robótica*" (ABL, 2020). No entanto, tal definição já não acompanha a realidade, uma vez que os desenvolvimentos tecnológicos e sociais expandiram este conceito para além da prática estritamente médica.

Hoje a telemedicina engloba diversas áreas da saúde, como enfermagem, fisioterapia, nutrição, psicologia e outras que estão incorporando a tecnologia em suas atuações profissionais (KHOURI, 2003).

Apesar da prática da telemedicina ter surgido no Brasil por volta dos anos 1990, a sua efetivação é relativamente recente. Apenas em fevereiro de 2019 que o Conselho Federal de Medicina (CFM) autorizou a prática de telemedicina no país, através da Resolução nº 2.227/2018, incluindo modalidades como teleconsulta, telediagnóstico e telecirurgia.

Contudo, a normativa foi revogada ainda no mesmo mês, revelando resistência por parte dos profissionais médicos e a ausência de consenso quanto à sua aplicação (CFM, 2018).

Com a pandemia do Covid-19, lastreada em 2020, trouxe um cenário mundial de emergência sanitária, marcado pelo distanciamento social, fechamento de estabelecimentos e sobrecarga dos sistemas de saúde. Nesse contexto, a telemedicina volta a ser adotada, ressurgindo como alternativa para a manutenção do acesso e assistência à saúde, ganhando espaço para sua consolidação (CAETANO *et al*., 2020).

Assim, a telemedicina foi regulamentada em caráter emergencial através da Lei nº 13.989/2020, que autorizou seu uso em todas as esferas da saúde (pública, suplementar e privada) enquanto perdurasse a crise sanitária (BRASIL, 2020).

A necessidade de urgência causada pela crise global fez com que a telemedicina ganhasse protagonismo, sendo reconhecida como estratégia para atendimento médico.

Entretanto, é possível encontrar obstáculos para a sua consolidação definitiva. Algumas delas são a resistência de alguns profissionais da saúde à adoção de tal prática, mas especialmente às questões estruturais brasileiras (LISBOA *et al*., 2023). A falta de acesso à internet, que atualmente, em tempos modernos, parece tão distante de alguns, é uma realidade para milhões de brasileiros que ainda lutam pelo acesso à internet diária (PWC, 2022).

Ainda assim, a implementação da telemedicina quando efetiva em sua integralidade, possibilita a realização de atendimentos, diagnósticos e monitoramentos à distância, evitando o deslocamento desnecessário, reduzindo a desigualdade regional e viabilizando o atendimento médico quando em localidades remotas ou que possuem escassez de profissionais (LISBOA *et. al*, 2023).

Além disso, permite que problemas de saúde tenham intervenções mais precoces e rápidas diante da agilidade de atendimento que evita longas horas

de espera ou filas que demoram meses para serem atualizadas (LISBOA *et. al*, 2023).

## 2.2. Proteção e sigilo de dados médicos

A informação médica, por sua própria natureza, está diretamente associada à esfera mais íntima do ser humano, devendo ser tratada com absoluto sigilo, respeitando-se a sua ligação ao elemento essencial da dignidade humana. Assim, o dado médico deve ser resguardado com o maior rigor, garantido o direito à privacidade e à intimidade dos titulares, bem como ao sigilo médico profissional.

A Lei nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), define três tipos de dados, sendo o mais relevante neste momento o dado pessoal sensível. Em seu artigo 5º, II, a lei conceitua dado pessoal sensível tudo aquilo inerente à uma pessoa natural que se refere a opinião política, convicção religiosa e/ou filosófica, informações médicas e biológicas e outros[1].

Dessa forma, conforme mencionado, o dado médico ao ser reconhecido como categoria de dado sensível merece proteção especial. Tal reconhecimento encontra relação plena com os direitos da personalidade, que conforme Maria Helena Diniz são definidos como[2]:

> "*O direito da personalidade é o direito da pessoa defender o que lhe é próprio, como a vida, a identidade, a liberdade, a imagem, a privacidade, a honra etc*."

Nesse sentido, o dado de saúde, ao ser relevado, exige compromisso ético e jurídico. Importante destacar que, ainda que compartilhados com

[1] É como estabelece o Art. 5º da Lei n. 13.709, de 14 de agosto de 2018 (LGPD): Para os fins desta Lei, considera-se: [...] II – dado pessoal sensível: 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 natural; (BRASIL, 2018).

[2] DINIZ, Maria Helena. Curso de Direito Civil Brasileiro, 2 - volume: Teoria Geral das Obrigações — 22. ed. rev. e atual de acordo com a Reforma do CPC — São Paulo: Saraiva, 2007, p. 119.

profissionais de saúde, as informações médicas permanecem sob a titularidade do paciente. Não há transferência de propriedade, o que ocorre, na verdade, é uma troca de confiança de informação entre médico-paciente. A proteção desses dados é imperativa e uma vez violada, pode gerar impactos às esferas morais do titular, causando danos reputacionais e até mesmo emocionais (ZAGANELLI, BINDA, 2023).

Não obstante a legislação federal, o direito à privacidade ao dado de saúde também é respaldado pelo Código de Ética Médica, o qual consagra o sigilo médico profissional como décimo primeiro princípio fundamental, reforçando o dever de sigilo como pilar da atuação da prática médica (CFM, 2019).

O artigo 73 do Código de Ética Médica, aprovado pela Resolução CFM nº 2.217/2018 afirma que é vedado ao médico:

> "*Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente*".

O dever de sigilo profissional entre os médicos é um compromisso ético, que atua muito além do que uma mera formalidade. A preservação da confiança depositada frente ao profissional da saúde é fundamental ao que se refere à dignidade da pessoa humana, afastando a exposição indesejada de informações sensíveis.

A esse respeito, a intervenção de saúde requer o conhecimento prévio de todo o histórico do paciente, que pode ser rastreado desde o nascimento (ROSA, 2018). Nesse sentido, menciona Sérgio Deodato no tocante à intervenção[3]:

> "*Um conhecimento do passado histórico de cada pessoa, que muitas vezes obriga a um conhecimento prévio familiar, naquilo a que se denomina pela história pessoal e familiar de*

[3] DEODATO, Sérgio. Proteção dos dados pessoais de Saúde – Universidade Católica Editora, 2017.

> *saúde. Ou seja, a intervenção de saúde necessita aprofundar significativamente o conhecimento sobre a pessoa e a sua família, para que possa diagnosticar e intervir de forma eficaz*".

Diante disso, percebe-se que o sigilo médico é um dos eixos centrais da proteção de dados em saúde. Este não se esgota com o cumprimento de requisitos técnicos ou legais, há o aprofundamento na dimensão ética do profissional atuante, inerente à atividade médica de reconhecer a condição da complexidade biopsicossocial do ser humano. Nesse contexto, o uso de tecnologias apenas reafirma este compromisso de preservação de confidencialidade.

## 3. APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA TELEMEDICINA

### 3.1. A edição da Lei Geral de Proteção de Dados (LGPD) e sua principiologia

Com o propósito de fortalecer a privacidade no ambiente digital, o Brasil promulgou a Lei Geral de Proteção de Dados (LGPD) em 2018 (Lei nº 13.709). A iniciativa brasileira alinhou-se a uma tendência internacional de regulamentação da privacidade, à medida que a proteção de dados se tornava um tema central na era digital, no qual foi um movimento espelhado, por exemplo, no Regulamento Geral de Proteção de Dados (GDPR), que entrou em vigor concomitantemente (FRANCO, 2022).

A LGPD preencheu uma lacuna então existente no ordenamento jurídico brasileiro, estabelecendo um marco legal unificado para o tratamento de dados pessoais.

A relevância desse direito foi reafirmada com a Emenda Constitucional nº 115/2022, que incluiu a proteção de dados pessoais no rol de direitos fundamentais da Constituição Federal (art. 5º, inciso LXXIX), atribuindo-lhe o status de "*cláusula pétrea*" (LOBATO,2024). Nesse sentido, esse status lhe confere permanência e inalterabilidade, consagrando a proteção de dados como um pilar essencial no cenário atual da sociedade.

Ao dispor em seu artigo 2º, a LGPD disciplina a proteção de dados pessoais com fundamentos de direitos humanos, como o livre desenvolvimento da personalidade, a dignidade da pessoa natural e o exercício da cidadania, entre outros[4].

Com isso, sua principiologia está conectada com valores constitucionais que ressoam sobretudo na dignidade da pessoa humana. Desde a Constituição de 1988, a dignidade humana figura como fundamento da República Federativa do Brasil, irradiando-se sobre os direitos, como o da privacidade.

A tutela dos dados pessoais insere-se exatamente nesse contexto: trata-se de uma garantia cuja efetivação se apoia no princípio da dignidade humana. É possível transportar esse entendimento através das palavras proferidas por Sarmento[5]:

> "*O reconhecimento da centralidade do princípio da dignidade da pessoa humana é recorrente na jurisprudência brasileira, tendo o STF armado que se trata do "verdadeiro valor-fonte" que conforma e inspira todo o ordenamento constitucional vigente em nosso país*".

Os princípios previstos nos incisos do artigo 6º da LGPD são a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

---

[4] É como estabelece o Art. 2º da Lei n. 13.709, de 14 de agosto de 2018 (LGPD): "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." (BRASIL, 2018).

[5] SARMENTO, Daniel. Dignidade da Pessoa Humana: conteúdo, trajetória e metodologia. 3ª edição, Belo Horizonte: Editora Fórum, [2021].

Os três primeiros referem-se a coleta e o uso proporcional dos dados, delimitando o tratamento com propósitos legítimos, informados e estritamente indispensáveis (NUNES, 2022).

Os três seguintes asseguram que o indivíduo possa consultar, compreender e confiar no modo como suas informações são utilizadas, ressaltando a transparência e a possibilidade de acesso a qualquer tempo (NUNES, 2022).

Por fim, os cinco últimos são direcionados àqueles que irão realizar o manuseio destes dados. Assim, estes últimos príncipios impõem aos agentes de tratamento o dever de proteger dados contra riscos, evitar danos, não utilizá-los de forma discriminatória e comprovar conformidade com a lei (NUNES, 2022).

Em síntese, estes princípios estabelecem parâmetros para o tratamento dos dados fornecidos de forma que os direitos fundamentais não sejam comprometidos. Ao exigir suas circunstâncias, é possível verificar a centralidade do indivíduo na troca de informações sensíveis, garantindo que o tratamento seja respeitado e preservado conforme a dignidade humana, assegurando a coexistência dos dados e do titular em harmonia em todos os contextos da sociedade.

### 3.2. A normatização da Lei Geral de Proteção de Dados (LGPD) na telemedicina

A telemedicina consolidou-se como um dos maiores avanços na área da saúde nos últimos anos, tendo seu triunfo a partir da pandemia de Covid-19. Nesse período, a necessidade de manter o atendimento médico ainda que com o distanciamento social, despertou a necessidade de criar uma base legal que garantisse tanto a continuidade do direito à saúde quanto a proteção da intimidade dos pacientes.

A aprovação da Lei nº 14.510/2022, conhecida como Lei da Telessaúde, representou um marco regulatório ao disciplinar de forma definitiva a prática da telemedicina no Brasil, em conformidade com a Constituição Federal, a Lei do SUS (Lei nº 8.080/90) e a Lei Geral de Proteção de Dados Pessoais (SANTOS; THEBALDI, 2024).

Diante da normatização, houve a necessidade de relacionar-se a lei com os valores constitucionais, especialmente aos de direito fundamental à saúde, a privacidade e à proteção de dados pessoais. Conforme explicitado, os dados pessoais relacionados a saúde são de caráter sensível nos termos da LGPD, exigindo maior cautela e zelo no tocante ao seu tratamento.

Com isso, a telemedicina não pode ser compreendida apenas como ampliação do acesso à saúde, mas também como um espaço em que se deve observar, de forma rigorosa, os limites da individualidade informativa do paciente.

A Lei da Telessaúde, uma adição à Lei do SUS, incorporou no seu artigo 26-A, inciso VI, como princípio fundamental, além de outros, a confidencialidade dos dados médicos transmitidos em meio digital. [6]

Não obstante, também trouxe a observação dos preceitos previstos no Marco Civil da Internet e na própria LGPD, afirmando a natureza íntima da informação sensível como condição de validade para o funcionamento do sistema (SANTOS; THEBALDI, 2024).

Tal previsão concretiza a ideia de que a relação médico-paciente, tradicionalmente pautada pelo dever de sigilo, deve ser preservada mesmo quando feita através por tecnologias digitais, sob o risco de violar a confiança que sustenta a prática médica (SANT'ANNA, 2008).

Apesar do avanço disciplinado pela legislação, a doutrina aponta que ainda existem lacunas importantes. É possível extrair que a Lei da Telessaúde acaba por remeter excessivamente a outros diplomas normativos, sem detalhar de forma específica as obrigações aplicáveis ao tratamento de dados médicos, o que pode fragilizar a efetividade da proteção (SANTOS; THEBALDI, 2024).

Trazem também o desafio da desigualdade no acesso a tecnologias digitais no Brasil, no qual impõe limites à concretização da telemedicina como

[6] Confira na íntegra o artigo 26-A, inciso VI da Lei da Telessaúde de nº 14.510/2022: Art. 26-A. A telessaúde abrange a prestação remota de serviços relacionados a todas as profissões da área da saúde regulamentadas pelos órgãos competentes do Poder Executivo federal e obedecerá aos seguintes princípios: VI - confidencialidade dos dados (BRASIL, 2022);

instrumento democrático de saúde pública, demandando políticas públicas que complementem a prática para garantir tanto o acesso quanto a segurança no uso dessas ferramentas digitais (ALMEIDA *et. al.*, 2005).

Em síntese, a normatização da LGPD na telemedicina positiva e densifica a proteção do paciente em ambiente digital, reconhecendo a confidencialidade como princípio da prática e traduzindo a relação do médico-paciente pautada no dever do sigilo.

No mais, evidencia uma adaptação do direito às transformações tecnológicas, de forma que a legislação constitucional e infraconstitucional serve de amparo ao processo, trazendo os parâmetros para o tratamento dos dados nesse contexto.

### 3.3. O papel da Autoridade Nacional de Proteção de Dados (ANPD) na fiscalização da telemedicina

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) instituiu a criação da Autoridade Nacional de Proteção de Dados (ANPD) como órgão responsável por zelar pela aplicação da LGPD, expedir normas e fiscalizar sua observância.

Apesar de aplicável a todos que manuseiam dados, a autoridade possui tamanha relevância no setor da saúde, especialmente na telemedicina, pois o manuseio de informações sensíveis ocorre de forma intensa e mediada por tecnologias digitais (HAWRYLISZYN *et al.*,2021).

A autoridade surge para prestar ao papel como mecanismo de proteção coletiva, atuando tanto na prevenção quanto na repressão a violações, de modo a assegurar a autodeterminação informativa dos cidadãos. Esse aspecto é particularmente importante na telemedicina, já que o fluxo de informações médicas, como prontuários eletrônicos, laudos ou consultas online aumenta cada vez, podendo acarretar na exposição a riscos como vazamentos, usos indevidos ou acessos não autorizados (HAWRYLISZYN *et al.*,2021).

Os Capítulos VIII e IX da LGPD reforçam essa função ao estabelecerem as regras para sanções e a estrutura institucional da ANPD.

O Capítulo VIII (arts. 52 a 54-B) prevê sanções administrativas que vão desde advertências, multas, bloqueio até a eliminação de dados pessoais, instrumentos que se mostram especialmente rigorosos quando aplicados a informações de saúde, cujo mau uso pode comprometer direitos fundamentais.

Já o Capítulo IX (arts. 55-A a 55-L) cria a própria ANPD, definindo-a como o órgão responsável por "*zelar, implementar e fiscalizar o cumprimento*" da lei, com poderes para expedir regulamentos e guiar a atuação de controladores e operadores (art. 55-J). A implementação da competência da entidade reforça que para além do plano normativo, a fiscalização deve ser efetiva e contínua, condição essencial à confiança e o bom funcionamento do sistema de telessaúde.

Não obstante, a atuação da ANPD não deve ser compreendida apenas no viés punitivo. O seu poder sancionador cumpre também função preventiva, servindo para sinalizar a observância da lei e promover a conscientização institucional sobre os riscos jurídicos e éticos decorrentes do mau uso de dados de saúde (MINGHELLI *et al.*, 2024).

Ao lado desse caráter sancionatório, a ANPD desempenha igualmente uma função orientadora. Busca estimular os agentes de tratamento a criarem estruturas de conformidade a cultura de dados e nomearem encarregados capazes de dialogar com a autoridade e implementar medidas adequadas de segurança (MINGHELLI *et al.*, 2024).

Dessa forma, a ANPD cumpre um papel pedagógico, fornecendo parâmetros técnicos e orientações regulatórias que possibilitam aos serviços de saúde alinhar suas práticas tanto às exigências normativas quanto aos princípios da transparência e da dignidade da pessoa humana (MINGHELLI *et al.*, 2024). Nesse equilíbrio entre sanção e orientação, a autoridade reforça o tratamento correto de dados no setor de saúde e contribui para que o sistema de saúde digital seja exercido de maneira legítima.

## 4. OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NA PROTEÇÃO DE DADOS MÉDICOS

### 4.1. O consentimento do paciente e os limites da coleta de dados

Os avanços tecnológicos impulsionaram uma enorme circulação de dados de saúde, de forma que se exige o rigor na obtenção do consentimento do paciente e de estabelecer limites para a coleta de seus dados.

Para isso, o consentimento qualificado do paciente torna-se requisito essencial para qualquer tratamento de dados sensíveis, atuando em conjunto com práticas robustas de segurança da informação para salvaguardar os direitos fundamentais do indivíduo (LEME; BANK, 2020).

Desta forma, sem a autorização expressa, clara e consciente do titular, não se admite que seus dados médicos sejam coletados ou utilizados, exceto nas hipóteses legais previstas.

A Lei Geral de Proteção de Dados (LGPD) estabeleceu o consentimento do titular como a principal base legal para tratar dados pessoais, inclusive na área da saúde. Por definição legal, através do inciso XII do artigo 5º da referida lei, o consentimento consiste na "*manifestação livre, informada e inequívoca pela qual o paciente concorda com o tratamento de seus dados para uma finalidade determinada*". No caso de dados pessoais sensíveis, a lei exige um consentimento específico e em destaque, vinculado a finalidades explícitas (BOTELHO; CAMARGO, 2021).

Conforme mencionado anteriormente, é proibido que o consentimento seja genérico e sem finalidade específica. Assim, a exigência se dá em razão da precisão e do elevado grau de transparência ao titular, conferindo também segurança jurídica ao responsável pelo controle destes dados, sendo certo que este é que tem o ônus probatório de demonstrar que obteve o tal consentimento de forma legalmente regular (MALDONADO, 2019).

Em suma, o profissional de saúde ou a instituição que controla tais dados deve obter do paciente uma anuência explícita para cada propósito de tratamento de seus dados médicos, sob pena de a coleta e utilização dessas informações serem consideradas inválidas e ilegais.

A exigência de rigor na obtenção do consentimento do paciente está diretamente ligada à natureza sensível das informações médicas. Informações sobre o estado de saúde, histórico médico, genética ou vida sexual de um indivíduo são classificados como sensíveis justamente por terem o potencial de causar discriminação, estigmatização ou violar intimidade e dignidade do titular, caso utilizadas de forma inadequada (BOTELHO; CAMARGO, 2021).

Por esse motivo, a LGPD estabelece tratamento especial e mais protetivo a esses dados, havendo uma preocupação do legislador em evitar que tais informações sejam empregadas contra os titulares, restringindo seu acesso a bens ou serviços ou o exercício de direitos (BOTELHO; CAMARGO, 2021). O propósito central da lei é coibir o uso abusivo ou discriminatório dos dados pessoais, garantindo o processamento adequado (LEME; BANK, 2020).

Embora o consentimento do titular seja fundamental à proteção de dados, a LGPD reconhece que, em circunstâncias excepcionais, o tratamento de dados sensíveis pode ocorrer sem o consentimento do titular.

O artigo 11, inciso II, da lei elenca sete hipóteses específicas em que a coleta e o uso de dados pessoais sensíveis são permitidos independentemente da anuência do paciente. São elas, em síntese, quando feitas pela administração pública; para estudos realizados por órgãos de pesquisa, valendo-se da anonimização do dado sensível; para o exercício regular de direitos; para proteção da vida em situações de incolumidade física do titular ou de terceiro; para a tutela de saúde quando realizada por profissionais ou serviços desta área e, por fim, para prevenir fraude e garantir a segurança do titular quando em processos de identificação eletrônicos ou em sistemas digitais.[7]

[7] Assim estabelece o Art. 11, inciso II da Lei n. 13.709, de 14 de agosto de 2018 (LGPD): "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: 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

Importante destacar que mesmo nos casos autorizados acima, a lei impõe a condição da indispensabilidade. Ou seja, só é possível dispensar o consentimento se o uso dos dados for absolutamente necessário para atingir a finalidade legítima prevista em lei. Isso significa que, se houver uma alternativa menos invasiva à privacidade do paciente, que permita alcançar o mesmo objetivo, o tratamento sem consentimento não será permitido e será considerado ilegal.

Esta interpretação está alinhada aos princípios da máxima efetividade dos direitos fundamentais e da interpretação *pro homine*, que orientam a aplicação da norma sempre em favor da pessoa. Dessa forma, evita-se que exceções legais sejam distorcidas e utilizadas como justificativa para práticas arbitrárias ou para transformar exceções em regra (BOTELHO; CAMARGO, 2021).

Além disso, mesmo quando o consentimento não é exigido, permanecem em vigor outros deveres de proteção, como o direito de ser informado sobre o tratamento de seus dados pessoais nessas circunstâncias excepcionais, garantindo a anonimização sempre que possível, de modo a resguardar a privacidade do paciente (BOTELHO; CAMARGO, 2021).

No caso específico da hipótese de tutela da saúde (art. 11, II, alínea *f*), a LGPD foi clara ao estabelecer limites, de modo que a dispensa de consentimento se aplica apenas a procedimentos de proteção da saúde conduzidos exclusivamente por agentes qualificados (como profissionais e autoridades sanitárias).

Esta exceção tem como objetivo atender situações em que o uso dos dados, sem autorização prévia, seja realmente necessário para proteger a saúde do paciente ou da coletividade, evitando que essa exceção seja usada de forma indevida ou generalizada.

Diante do cenário legal, é fundamental que a prática profissional em saúde se ajuste aos ditames da LGPD, tanto por dever legal quanto ético profissionais da área e instituições de saúde precisam adotar as melhores práticas de

Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais." (BRASIL, 2018)

segurança da informação sob pena de incidência das sanções do art. 52 da lei (LEME; BANK, 2020).

No entanto, a conformidade com a LGPD vai além da mera prevenção de penalidades, pois representa uma extensão dos deveres de sigilo profissional e respeito à autonomia do paciente já consagrados na ética médica. Trata-se de um equilíbrio necessário entre o avanço tecnológico no campo médico e a preservação dos valores da intimidade, da autonomia e do respeito à pessoa humana.

### 4.2. Riscos de vazamentos e ataques cibernéticos

Como mostrado ao longo deste trabalho, a inserção da tecnologia na rotina do ser humano trouxe inúmeros benefícios, mas também expõe fragilidades latentes na proteção da circulação dos dados sensíveis. A elevada massa de fluxo e armazenamento de dados potencializam o risco de uso abusivo e de vazamentos, mesmo que tenham sido anonimizados (ARAGÃO; SCHIOCCHET, 2020).

Assim, apesar do elevado arcabouço normativo protetivo, admite-se a ocorrência de incidentes de segurança. Estudos demonstram que a difusão dos meios digitais na medicina expõe o paciente titular dos dados a vulnerabilidades, seja por negligência no tratamento das informações, seja pela comercialização indevida ou vazamento de dados pessoais de saúde (LEME; BANK, 2020).

Não obstante, dada a natureza destes dados, é muito comum a pretensão por cibercriminosos, pois através de estudos entendeu-se que dados médicos possuem um alto valor quando ingressados no mercado ilícito, superando até mesmo os dados de um cartão de crédito (HUMER; FINKLE, 2014), podendo chegar a alcançar centenas de dólares (CHERNYSHEV *et al.*, 2018).

No mais, atrela-se ao fato de registros médicos manterem informações permanentes, como nome, idade, contato, podendo ser um facilitador a crimes de fraude de identidade e outros delitos correlacionados (POOL *et al.*, 2018).

Veja, a International Business Machines Corporation (IBM), divulgou o Relatório *Cost of a Data Breach* que demonstrou que o valor médio de uma violação de dados em 2024 é o equivalente a US$ 4,44 milhões.

No setor da saúde, este valor chegou a US$ 10,93 milhões (ELGAN, 2024). Estes números explicam o porquê ataques cibernéticos ao setor saúde vêm crescendo com frequência. Os ataques cibernéticos ocorrem, muitas das vezes, através de *malwares* ou *ransomwares*, espécies estas de códigos de *softwares* escritos para a invasão de sistemas e computadores dirigidos a obter acesso não autorizado a dados confidenciais (IBM, 2024).

Em paralelo às ameaças externas (ataques de *hackers*), há também riscos internos, como acessos indevidos ou divulgações não autorizadas por funcionários, perda de dispositivos contendo dados ou descarte inadequado de informações sensíveis, todos fatores que podem culminar em vazamentos.

Com isso, depreende-se que os efeitos negativos de um vazamento de dados médicos são graves e multidimensionais. Como já mencionado, a exposição de informações de saúde pode acarretar danos morais e riscos concretos à segurança do titular dos dados, caso informações clínicas sensíveis sejam usadas para constrangê-lo ou discriminá-lo.

Alguns autores sustentam que o "*vazamento de dados pessoais de pacientes configura uma forma de "violência hospitalar*", pois viola a confiança depositada na relação terapêutica e pode sujeitar o paciente a humilhações e injustiças (SABROZA *et. al*., 2023).

No mais, diante destes cenários a preocupação com a privacidade após um vazamento influencia negativamente a confiança e a disposição dos indivíduos em fornecer dados nos sistemas de saúde, o que pode afetar os resultados assistenciais e a eficiência do sistema como um todo (MATA, 2022).

Em síntese, os vazamentos de dados médicos e os ataques cibernéticos contra sistemas de saúde configuram hoje um desafio, que precisa ser enfrentado em múltiplos planos (SOBROZA *et al*., 2023).

No plano jurídico-normativo, impõe-se o fortalecimento da cultura de proteção de dados nas entidades de saúde, cumprindo integralmente as exigências da LGPD e demais regulações (como normas de Conselho Federal de Medicina sobre prontuário eletrônico, sigilo profissional, etc.) (SOBROZA *et al*., 2023).

No plano técnico, é essencial investir em infraestruturas seguras que garantam a integridade e o *compliance* dos dados que estão em tramitação, demonstrando confiança e agilidade para rápida recuperação diante de falhas, evitando maiores transtornos e desestabilização destes sistemas utilizados pela maioria esmagadora da população (SOBROZA *et al.*, 2023).

No plano ético, deve-se lembrar que a proteção dos dados de saúde é, em última instância, a proteção da pessoa do paciente em sua esfera mais íntima, de forma que a violação do dever de custódia informacional é um abalo a relação terapêutica, seja com o profissional da saúde ou com a instituição física (SOBROZA *et al.*, 2023).

## 4.3. Estudos de caso: incidentes de segurança na digitalização da saúde e suas consequências jurídicas

### 4.3.1. Vazamento de dados de pacientes da COVID-19 no Ministério da Saúde (2020)

Um dos casos mais emblemáticos de falha de segurança em saúde digital ocorreu em 2020, quando informações pessoais e médicas de 16 milhões de pacientes com suspeita ou diagnóstico de COVID-19 foram expostas indevidamente em todo território nacional.

Esse vazamento ocorreu após *logins* e senhas de acesso a sistemas internos do Ministério da Saúde terem sido publicados por um funcionário do Hospital Albert Einsten em plataforma aberta, permanecendo disponíveis por quase um mês. Entre os dados sensíveis acessíveis estavam nomes e documentos de identificação (SOBROZA *et al.*, 2023).

Tal exposição violou gravemente a privacidade dos pacientes e os sujeitou a potenciais situações de discriminação e uso indevido de suas informações, considerando este episódio auxiliou na propagação de desinformação e alimentação a ataques contra pessoas idosas e de origem chinesa que foram afetadas pelo vírus (SOBROZA *et al.*, 2023), parcelas estas últimas da população que, pela difusão de informações em massa, sofreram ataques xenofóbicos e racistas.

Diante da evidente violação de sigilo, esse incidente passou a ser tratado como um exemplo marcante dos riscos da violência hospitalar digital, dado o potencial de causar danos emocionais e sociais às vítimas (SOBROZA *et al.*, 2023).

As consequências jurídicas foram imediatas. A Controladoria-Geral da União (CGU) instaurou processo de responsabilização, concluindo pela aplicação de sanção administrativa à instituição envolvida.

No relatório final, a CGU recomendou a aplicação ao Hospital Albert Einstein (entidade vinculada ao incidente) de multa de R$ 210.000,00 (duzentos e dez mil reais), com fundamento na Lei de Acesso à Informação, por ter permitido o vazamento desses dados sensíveis. Esta penalidade administrativa baseou-se na infração aos deveres de proteção de informações pessoais custodiadas por entes privados em nome do poder público. Além disso, no âmbito civil, discute-se, ainda, a reparação dos danos morais aos pacientes afetados (BRASIL, 2021).

Nessa toada, faz-se necessário expor que a jurisprudência brasileira já vem se articulando e consolidando o entendimento de que a simples ocorrência e constatada do vazamento de dados pessoais pode gerar dano moral presumido, dispensando a comprovação de prejuízo concreto.

Verifica-se em precedente do Superior Tribunal de Justiça, REsp n. 2.121.904/SP, de relatoria da Ministra Nancy Andrighi, que o vazamento de dados pessoais sensíveis, no caso concreto, em contrato de seguro de vida, gera responsabilização objetiva da seguradora e caracteriza dano moral presumido, pois os dados vazados, protegidos tanto pelo Código de Defesa do Consumidor quanto pela LGPD, expõem o consumidor a riscos relevantes em sua honra, intimidade, patrimônio e segurança, sendo reconhecida a falha na prestação de serviços[8].

[8] Confira-se o precedente do Superior Tribunal de Justiça na íntegra: CIVIL. RECURSO ESPECIAL. CONTRATO DE SEGURO DE VIDA. RELAÇÃO DE CONSUMO. CÓDIGO DE DEFESA DO CONSUMIDOR. LEI GERAL DE PROTEÇÃO DE DADOS. VAZAMENTO DE DADOS SENSÍVEIS. RESPONSABILIDADE OBJETIVA. DANO MORAL PRESUMIDO. RECURSO CONHECIDO EM PARTE. DESPROVIMENTO. 1. Ação de obrigação de fazer c/c indenização por danos morais e materiais, da qual foi extraído o presente recurso especial, interposto em 28/6/2023 e concluso ao gabinete em 22/2/2024. 2. O propósito recursal é definir se, em contrato de seguro de vida, o vazamento de dados sensíveis do segurado gera: (a) dano moral presumido

Assim, o precedente supracolacionado, além de muitos outros, *mutatis mutandis*, serve de argumento suficiente para embasar juridicamente os pedidos que tem por razões as mazelas dos episódios em que vazamento de dados ocorrem.

Extrai-se, portanto, que independentemente de prova de dano material, a exposição indevida de dados de saúde, *per si*, fere direitos da personalidade privacidade e dignidade, ensejando o dever de indenizar.

Este caso evidenciou, portanto, tanto a responsabilização administrativa da pessoa jurídica (multada nos termos da legislação vigente) quanto a possibilidade de responsabilidade civil objetiva perante os titulares dos dados, em conformidade com a LGPD e a proteção constitucional da privacidade.

---

e (b) responsabilização objetiva da empresa seguradora.3. Inexistência de negativa de prestação jurisdicional. Acórdão do Tribunal de origem devidamente fundamentado para solucionar integralmente a controvérsia submetida à sua apreciação. 4. Não há cerceamento de defesa nas hipóteses em que o julgador resolve a questão controvertida, de forma fundamentada, sem a produção da prova requerida pela parte, em virtude de considerar suficientes os elementos que integram os autos.5. A matéria que não foi objeto de debate no acórdão recorrido, mesmo após a interposição de embargos declaratórios, não pode ser conhecida por meio de recurso especial. Súmula nº 211/STJ. 6. Cabe ao fornecedor o ônus de comprovar que cumpriu com seu dever de proteger dados pessoais do consumidor, sobretudo quando se tratam de dados sensíveis, nos termos do CDC (arts. 6º, VIII e 14, caput e §3º) e da LGPD (arts. 6º, X, 8º, §2º, 42, §2º e 48, §3º). 7. Há especial proteção legal aos chamados dados pessoais sensíveis: aqueles que, quando revelados, podem gerar algum tipo de discriminação, sobretudo os que incidem 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" (art. 5º, II, da LGPD).8. O tratamento de dados pessoais sensíveis observa requisitos significativamente mais rigorosos, sobretudo com a exigência, em regra, do consentimento específico e destacado do titular (art. 11 da LGPD). 9. Em contrato de seguro de vida, deve-se empreender um rigoroso esforço para a proteção dos dados pessoais, já que, para sua celebração, a seguradora, para a avaliação dos riscos, recebe dados sensíveis sobre aspectos pessoais, familiares, financeiros e de saúde do segurado. 10. O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, por si só, submete o consumidor a riscos em diversos aspectos de sua vida, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal. 11. Por isso, em seguro de vida, na hipótese de vazamento de dados sensíveis do segurado, verifica-se a responsabilização objetiva da seguradora e a caracterização de dano moral presumido. 12. Conforme entendimento desta Corte, a revisão da compensação por danos morais só é viável em recurso especial quando o valor fixado for exorbitante ou ínfimo, o que não se constata no recurso sob julgamento. 13. Hipótese em que o acórdão recorrido, ao manter a responsabilização da seguradora, reconheceu que: i) houve vazamento de dados pessoais do consumidor; ii) tais dados são classificados como sensíveis, de modo a abranger informações fiscais, bancárias e sobre a saúde do consumidor; iii) há nexo de causalidade entre o vazamento de dados sensíveis do consumidor e falhas na prestação do serviço pela recorrente, que não atendeu a seu dever de garantir a proteção dos dados sensíveis do consumidor. 14. Recurso especial parcialmente conhecido e, nessa extensão, desprovido. ” (REsp n. 2.121.904/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 11/2/2025, DJEN de 17/2/2025.)

### 4.3.2. Ataque hacker ao Conecte SUS e apagão de sistemas de saúde (2021)

No final de 2021, a infraestrutura digital do Ministério da Saúde sofreu um ataque cibernético de grandes proporções, revelando fragilidades na digitalização da saúde pública. *Hackers* invadiram os servidores ministeriais, incluindo a plataforma Conecte SUS, responsável pelos certificados nacionais de vacinação do COVID-19, fazendo com que usuários que tentavam acessar seus dados de vacinação deparavam-se com uma mensagem de autoria dos invasores, em vez das informações esperadas (SPDM, 2022).

Posteriormente, o grupo criminoso *LAPSUS$* assumiu a autoria do ataque, confirmando tratar-se de um sequestro de dados por *ransomware*. Como resultado, bancos de dados essenciais foram criptografados ou mesmo apagados, comprometendo a disponibilidade das informações (SPDM, 2022).

Embora o governo federal brasileiro tenha tranquilizado a população anunciando a existência de *backups*, a recuperação mostrou-se complexa, pois para o reestabelecimento pleno dos sistemas foram necessários mais de 40 (quarenta) dias, que ainda assim retornaram operando com falhas e instabilidades (OLIVEIRA, 2022).

Durante o período supracitado, serviços como a emissão de comprovantes de vacinação ficaram suspensos, prejudicando cidadãos e expondo a dependência crítica de sistemas digitais seguros na saúde (SPDM, 2022).

Do mesmo modo ao que foi apresentado no caso anterior, as implicações jurídicas desse incidente foram também significativas. Inicialmente, o caso foi investigado pela Polícia Federal, com o apoio do Gabinete de Segurança Institucional, dada a possibilidade de crime cibernético contra a Administração Pública (SPDM, 2022).

Paralelamente, o Ministério Público Federal (MPF) em Brasília manifestou preocupação com os dados sensíveis dos usuários potencialmente comprometidos, destacando o risco de lesão à privacidade coletiva (SILVA *et al.*, 2023). Apesar da gravidade, não se divulgou até o momento aplicação de sanções financeiras pela Autoridade Nacional de Proteção de Dados (ANPD) ao

Ministério. Contudo, o incidente serviu de catalisador para reforçar políticas de segurança da informação e acelerar investimentos em infraestrutura mais segura.

### 4.3.3. Violação de sigilo profissional no caso Klara Castanho (2022)

Nem todos os incidentes de segurança decorrem de ataques externos ou falhas humanas, quebras de confidencialidade dentro de instituições de saúde também podem ter repercussão tão graves quanto. Um caso de grande repercussão nacional foi o da atriz Klara Castanho, em 2022, que expôs os riscos da divulgação indevida de dados clínicos por parte de profissionais de saúde.

A artista, então com 21 anos, foi vítima de estupro que resultou em gravidez e, amparada pela lei, optou por entregar anonimamente o recém-nascido à adoção, resguardando sua intimidade durante todo o processo hospitalar (BARRETO; SANTOS, 2023).

Contudo, essas informações extremamente sensíveis, relativas à violência sexual sofrida e à entrega legal da criança, foram ilegalmente acessadas e vendidas por uma enfermeira do hospital onde ocorreu o parto, sem qualquer consentimento da paciente. Pouco depois, detalhes do caso vieram a público por meio das redes sociais e da imprensa, rompendo o sigilo médico-hospitalar a que a atriz tinha direito (BARRETO; SANTOS, 2023).

A divulgação não autorizada desses dados pessoais expôs a atriz a uma série de comentários e julgamentos na internet, causando-lhe grave impacto negativo em sua vida pessoal e profissional. Klara Castanho viu-se compelida a se pronunciar publicamente para se defender, revelando uma intimidade que em nenhum momento tinha o interesse de expor, o que ilustra o efeito irreversível de um vazamento dessa natureza (BARRETO; SANTOS, 2023).

No âmbito jurídico, o caso gerou indignação e mobilização. A conduta da funcionária configura evidente infração ética e disciplinar, violando o dever profissional de sigilo previsto em normativas médicas e pode caracterizar ilícitos civis e penais. Trata-se de um dado pessoal ultra-sensível, referente à saúde e à vida privada da paciente, cuja divulgação sem autorização infringe frontalmente a LGPD (arts. 11 e 13 da Lei 13.709/18) e os direitos fundamentais à privacidade e à dignidade humana.

O caso ilustra uma hipótese de responsabilidade civil objetiva especial, decorrente da violação do dever legal de segurança previsto na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). A conduta da enfermeira que acessou, divulgou e vendeu as informações sigilosas sem consentimento representa não apenas infração ética, passível de sanção pelo respectivo conselho profissional, como também ofensa direta à tutela jurídica dos dados pessoais sensíveis (VALDEMIRO, 2023).

Em razão do desequilíbrio técnico e informacional entre paciente e instituição de saúde, os agentes hospitalares têm o dever reforçado de proteção das informações obtidas em contextos de vulnerabilidade, sendo inadmissível a divulgação indevida.

Assim, a responsabilização se consolida tanto no plano individual (profissional) quanto institucional (hospital), nos termos do artigo 42, § 1º, inciso I da LGPD[9] e do art. 932, inciso III do Código Civil[10], que impõe responsabilidade solidária ao empregador pelos atos de seus prepostos no exercício da função (VALDEMIRO, 2023).

No mais, à luz dos princípios do Direito e da Bioética, o episódio Klara Castanho evidencia como a quebra de confidencialidade no ambiente hospitalar equivale a uma forma de violência, lesando a integridade psíquica da paciente e abalando a confiança na relação médico-paciente.

Assim, o caso em tela serve como alerta contundente de que a digitalização da saúde apesar de inovadora, exige não só medidas técnicas de segurança, mas também o fortalecimento da ética profissional e da cultura de proteção de dados, sob pena de graves consequências jurídicas e sociais (SOBROZA *et al.*, 2023).

---

[9] Na inteligência do artigo 42, § 1º, inciso I da Lei Geral de Proteção de Dados: Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei.

[10] Não obstante, a inteligência do artigo 932, inciso III do Código Civil: Art. 932. São também responsáveis pela reparação civil: III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele.

## CONSIDERAÇÕES FINAIS

Conforme exposto, o avanço tecnológico e a crescente digitalização da saúde, especialmente impulsionada pela pandemia de COVID-19, fez com que a telemedicina consolidasse como prática indispensável ao cenário contemporâneo. No entanto, essa inovação exige mais do que infraestrutura tecnológica e, sim, demanda um compromisso ético, jurídico e institucional com a proteção dos dados sensíveis dos pacientes.

A análise da Lei Geral de Proteção de Dados Pessoais (LGPD), em conjunto com a Emenda Constitucional nº 115/2022 e demais normativas setoriais regulatórias, revelou que o ordenamento jurídico brasileiro possui um arcabouço robusto para a tutela da privacidade e da autodeterminação informativa. Contudo, os estudos de caso demonstraram que a efetividade dessas normas ainda enfrenta desafios práticos, como falhas humanas e ataques cibernéticos.

Os casos expostos, como o vazamento de dados da Covid-19, o ataque hacker ao Conecte SUS e a violação de sigilo no caso Klara Castanho, demonstram que vazamentos, acessos indevidos e compartilhamentos não autorizados revela a urgência de políticas de segurança da informação sólidas, baseadas em princípios de transparência, responsabilidade e prevenção. Não obstante, geram consequências sociais, jurídicas e emocionais ás vítimas graves.

Ademais, os desdobramentos jurídicos decorrentes do descumprimento da LGPD, como a responsabilização civil e administrativa e, dependendo, penais, demonstram a necessidade de adequação técnica e normativa por parte das instituições de saúde.

Assim, a atuação da Autoridade Nacional de Proteção de Dados (ANPD) e a responsabilização jurídica por incidentes de segurança são passos importantes, mas não suficientes.

Há necessidade de fomentar uma cultura institucional de proteção de dados, que envolva a implementação de programas e treinamentos para a capacitação contínua dos profissionais da saúde, atrelado também a investimentos em segurança da informação com estruturas sólidas de

armazenamento através de softwares com ferramentas de proteção avançadas e, não menos importante, o fortalecimento da ética profissional àqueles que atuam diretamente com o manuseio e a coleta destes dados.

Não obstante, os episódios demonstrados nos presentes estudos de casos deste trabalho, expostos os vazamentos e os riscos que estão atrelados, apenas reafirmam a necessidade desta articulação integrada e eficaz.

O caso da atriz Klara Castanho, ocorrido em 2022, revela, um dos, senão o maior, exemplos mais escrachados quanto a esta desconexão entre a norma e realidade. Não suficiente a violação da sua intimidade, na sua forma mais dilacerante, após sofrer violência sexual, teve, para além, este fato exposto publicamente.

O episódio evidencia de forma dolorosa que o dano causado por uma falha na proteção de dados sensíveis e na quebra da confidencialidade, no âmbito da relação do paciente para com o profissional e a instituição a que este representa, vai muito além de questões administrativas ou técnicas, podendo desencadear humilhações públicas, abalo psicológico e sofrimento à vítima que não há reparação suficiente para amenizar o que foi sofrido.

Por fim, este trabalho reafirma que a proteção dos dados médicos não é apenas uma exigência legal, mas uma extensão do direito constitucional do respeito à dignidade humana, orientada através da proteção da intimidade e da saúde dos indivíduos.

A compreensão pelos profissionais de saúde e suas instituições de que os dados dos pacientes não são apenas registros, mas são fragmentos de histórias pessoais que, conforme o caso da Klara, carregam dores pessoais, de vulnerabilidade e de medo.

Assim, a confiança depositada pelo paciente no ambiente digital deve ser preservada com o mesmo rigor ético e técnico que se espera no atendimento presencial. Assim, a consolidação da telemedicina como prática legítima e eficaz depende do aperfeiçoamento intersecional entre inovação tecnológica e salvaguarda dos direitos fundamentais, especialmente o direito à privacidade.

## REFERÊNCIAS BIBLIOGRÁFICAS

**ACIOLY, Luis Henrique de Menezes; SILVA, Matheus Fernandes da; MONTEIRO NETO, João Araújo.** A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e o enforcement da proteção de dados pessoais no Brasil. Revista de Investigações Constitucionais, [S. l.], v. 11, n. 3, p. e275, 2024. DOI: 10.5380/rinc.v11i3.92117. Disponível em: https://revistas.ufpr.br/rinc/article/view/92117. Acesso em: 11 maio. 2025.

**ALMEIDA, Lilia Bilati de; PAULA, Luiza Gonçalves de; CARELLI, Flavio Campos; OSÓRIO, Tito Lívio Gomes; GENESTRA, Marcelo.** O retrato da exclusão digital na sociedade brasileira. Journal of information systems and technology management, v. 2, n. 1, p. 55-67, 2005. Doi: https://doi.org/10.1590/s1807-17752005000100005. Acesso em: 16 de agosto de 2025.

**ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa.** Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. Reciis: Revista Eletrônica de Comunicação, Informação e Inovação em Saúde, Rio de Janeiro, v. 14, n. 3, p. 692-708,jul./set.2020. Disponível em: https://docs.bvsalud.org/biblioref/2020/10/1121860/2012-8932-1-pb.pdf. Acesso em: 04 de setembro de 2025.

**ARAÚJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano.** Curso de Direito Constitucional. 3. ed. São Paulo: Manole, 2021. Acesso em: 21 de junho de 2025.

**BARRETO, Iris Vitória Soares; SANTOS, Thayna Beatriz Oliveira dos.** Proteção à dignidade sexual e à aplicação do direito penal em casos que envolvam celebridades: o impacto da exposição midiática sofrido por Klara Castanho. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/34308. Acesso em: 07 de setembro de 2025.

**BIONI, Bruno Ricardo.** Proteção de Dados Pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. Acesso em: 21 de junho de 2025.

**BOBBIO, Norberto.** A Era dos Direitos. Tradução de Carlos N. Coutinho. Rio de Janeiro: Campus, 1992. Acesso em: 21 de junho de 2025.

**BOTELHO, Marcos César; CAMARGO, Elimei Paleari do Amaral.** A aplicação da Lei Geral de Proteção de Dados na saúde. Revista de Direito Sanitário, São Paulo, Brasil, v. 21, p. e0021, 2021. DOI: 10.11606/issn.2316-9044.rdisan.2021.168023. Disponível em: https://www.revistas.usp.br/rdisan/article/view/168023. Acesso em: 11 maio. 2025.

**BRASIL.** Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 maio 2025.

**BRASIL. Controladoria-Geral da União.** Relatório final do Processo Administrativo de Responsabilização nº 00190.103948/2021-69. Sociedade Beneficente Israelita Brasileira – Hospital Albert Einstein. Brasília, DF, 24 ago. 2021. Disponível em: https://sei.cgu.gov.br/conferir. Acesso em: 6 set. 2025.

**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 da União: seção 1, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 11 maio 2025.

**BRASIL.** Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível

em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 maio 2025.

**BRASIL. Superior Tribunal de Justiça.** Civil. Recurso especial. Contrato de seguro de vida. Relação de consumo. Código de Defesa do Consumidor. Lei Geral de Proteção de Dados. Vazamento de dados sensíveis. Responsabilidade objetiva. Dano moral presumido. Recurso conhecido em parte. Desprovimento. REsp n. 2.121.904/SP, Rel. Min. Nancy Andrighi, Terceira Turma, julgado em 11 fev. 2025, Diário da Justiça Eletrônico, 17 fev. 2025. Acesso em: 07 de setembro de 2025.

**CAETANO, Rosângela; SILVA, Angélica Baptista; GUEDES, Ana Cristina Carneiro Menezes; PAIVA, Carla Cardi Nepomuceno de; RIBEIRO, Gizele da Rocha; SANTOS, Daniela Lacerda; SILVA, Rondineli Mendes da.** Desafios e oportunidades para telessaúde em tempos da pandemia pela COVID-19: uma reflexão sobre os espaços e iniciativas no contexto brasileiro. Cadernos de Saúde Pública, Rio de Janeiro, v. 36, n. 5, e00088920, 2020. DOI: 10.1590/0102-311X00088920. Acesso em: 11 maio 2025.

**CONSELHO FEDERAL DE MEDICINA (Brasil).** Código de Ética Médica: Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019. Brasília: CFM, 2019. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acesso em: 19 maio 2025.

**DEODATO, Sérgio.** Proteção dos dados pessoais de Saúde – Universidade Católica Editora, 2017. Acesso em: 19 maio 2025.

**DINIZ, Maria Helena.** Curso de Direito Civil Brasileiro, 2 - volume: Teoria Geral das Obrigações — 22. ed. rev. e atual de acordo com a Reforma do CPC — São Paulo: Saraiva, 2007. Acesso em: 18 maio 2025.

**ELGAN, Mike.** *Cost of a data breach: the healthcare industry*. IBM Think, 06 ago. 2024. Disponível em: https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry. Acesso em: 6 set. 2025.

**FRANÇA, Nathalia Penha Cardoso.** A escola ibérica da paz: as vozes contra a colonização das américas e o verdadeiro nascimento do direito internacional humanista. In: WAGNER MENEZES (org.). Tribunais internacionais e decolonização. 1 ed. São Paulo: ABDI Editora, 2022, v. 1, p. 66-79. Acesso em: 21 de junho de 2025.

**FRANCO, Walter de Oliveira.** A proteção de dados pessoais no Brasil: aspectos e reflexos da Emenda Constitucional 115/2022 no ordenamento jurídico brasileiro. 2022. Artigo científico (Bacharelado em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília (UniCEUB), Brasília, 2022. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/16205/1/21652791.pdf. Acesso em: 11 maio 2025.

**HAWRYLISZYN, Larissa Oliveira; COELHO, Natalia Gavioli Souza Campos; BARJA, Paulo Roxo.** Lei geral de proteção de dados pessoais (LGPD): O desafio de sua implantação para saúde. Revista Univap, v. 27, n. 55, 2021. Acesso em: 16 de agosto de 2025.

**KHOURI, Sumaia Georges El.** Telemedicina: análise da sua evolução no Brasil. 2003. 247 f. Dissertação (Mestrado em Ciências na Área de Fisiopatologia Experimental) – Faculdade de Medicina, Universidade de São Paulo. São Paulo, 2003. Acesso em 11 maio 2025.

**IBM Brasil**. O que é malware? *IBM Think*, [s.l.], s.d. Disponível em: https://www.ibm.com/br-pt/think/topics/malware. Acesso em: 6 set. 2025.

**LEME, Renata Salgado; BLANK, Marcelo.** Lei Geral de Proteção de Dados e segurança da informação na área da saúde. Cadernos Ibero-Americanos de Direito Sanitário, [S. l.], v. 9, n. 3, p. 210–224, 2020. DOI: 10.17566/ciads.v9i3.690. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690. Acesso em: 11 maio 2025.

**LIMA, Manuela Ithamar.** Do direito à proteção de dados em matéria de saúde na sociedade de informação. Arquivo Jurídico, Teresina, v. 4, n. 1, jan./jul. 2017.

Disponível em: https://revistas.ufpi.br/index.php/raj/article/download/7416/4303. Acesso em: 11 maio 2025.

**LISBOA, Kálita Oliveira; HAJJAR, Ana Clara; SARMENTO, Isabela Perin; SARMENTO, Rebecca Perin; GONÇALVES, Sérgio Henrique Resende.** A história da telemedicina no Brasil: desafios e vantagens. Saúde e Sociedade, São Paulo, v. 32, n. 1, e210170pt, 2023. DOI: 10.1590/S0104-12902022210170pt. Disponível em: https://www.scielo.br/j/sausoc/a/htDNpswTKXwVr667LV9V5cP/. Acesso em: 11 maio 2025.

**LOBATO, Janaina Muniz.** O princípio da dignidade da pessoa humana e o direito fundamental à proteção de dados pessoais no Brasil. Revista FT, v. 29, n. 140, nov. 2024. Disponível em: https://revistaft.com.br/o-principio-da-dignidade-da-pessoa-humana-e-o-direito-fundamental-a-protecao-de-dados-pessoais-no-brasil/. Acesso em: 11 maio 2025.

**MATA, Camila Rosa da Mata.** Desafios à proteção de dados pessoais no setor da saúde: enfrentando o risco de vazamentos. Revista CEJ, 5 dez. 2022. Acesso em: 06 de setembro de 2025.

**MINGHELLI, Marcelo; GARCIA, Bárbara Balbis; VALE, Mariene Alves do; SANTOS, Patrícia Siqueira.** Lei Geral de Proteção de Dados e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais. Em Questão, Porto Alegre, v. 30, 2024. Acesso em: 16 de agosto de 2025.

**NUNES, Marcelo Chuere; BEZERRA, Vandré Cabral; COHN, Amélia.** A lei federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – e o direito à saúde como bem público: interpretação para a proteção dos dados pessoais como direito humano fundamental. Unisanta Law and Social Science, [S. l.], v. 11, n. 2, 2024. Disponível em: https://ojs.unisanta.br/LSS/article/view/884. Acesso em: 11 maio 2025.

**OLIVEIRA**, **Ingrid.** Relatório da Saúde descarta apagão de dados após ataque cibernético. CNN Brasil, 12 jan. 2022. Disponível em:

https://www.cnnbrasil.com.br/saude/relatorio-da-saude-descarta-apagao-de-dados-apos-ataque-cibernetico/. Acesso em: 16 nov. 2025

**PWC – PricewaterhouseCoopers Brasil.** O abismo digital no Brasil. São Paulo, 2022. Acesso em: 11 maio 2025.

**RODRIGUES DOS SANTOS, Gabriela; DOTTO THEBALDI, Marina.** A proteção de dados na telemedicina na perspectiva do acesso ao direito à saúde. Revista de Direitos Humanos e Desenvolvimento Social, [S. l.], v. 5, 2024. DOI: 10.24220/2675-9160v5a2024e13765. Disponível em: https://seer.sis.puc-campinas.edu.br/direitoshumanos/article/view/13765. Acesso em: 11 maio. 2025.

**ROSA, Diogo Miguel Alcaçarenho.** Proteção de dados pessoais em saúde e hospitais E.P.E.: responsabilidade civil do responsável pelo tratamento. 2018. Dissertação (Mestrado Profissionalizante em Ciências Jurídico-Empresariais) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2018. Disponível em: https://repositorio.ulisboa.pt/bitstream/10451/37436/1/ulfd136577_tese.pdf. Acesso em: 11 maio 2025.

**SANT'ANNA, Ricardo Tofani.** Do direito à confidencialidade no atendimento por telemedicina e a efetividade da tutela jurídica. 2008. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/4075. Acesso em: 11 maio 2025.

**SARLET, Ingo Wolfgang.** Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. Direitos Fundamentais & Justiça, [S.l.], a. 14, n. 42, p. 179-218, 2020. Acesso em: 21 de junho de 2025.

**SARMENTO, Daniel.** Dignidade da pessoa humana: conteúdo, trajetória e metodologia. 3ª edição. Belo Horizonte: Editora Fórum, [2021]. Acesso em: 16 de agosto de 2025.

**SCHEUERMANN, Gabriela Felden.** Dados pessoais como um direito fundamental autônomo a partir da Emenda Constitucional nº 115/2022. Revista da Defensoria Pública do Estado do Rio Grande do Sul, Porto Alegre, v. 2, n. 33, p. 253–274, 2023. Disponível em: https://revista.defensoria.rs.def.br/defensoria/article/view/600. Acesso em: 11 maio. 2025.

**SILVA, Janielson dos Santos; OLIVEIRA, Rayssa Francyelle de.** Análise das falhas no armazenamento de dados do aplicativo Conecte SUS sob a ótica midiática: desafios da segurança da informação na saúde pública, 2023. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas) - Fatec Dom Paulo Evaristo Arns, São Paulo, 2023. Acesso em 06 set. 2025.

**SOUZA, Nicolle Bêtta de; ACHA, Fernanda Rosa.** A proteção de dados como direito fundamental: uma análise a partir da Emenda Constitucional 115/2022. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 8, n. 9, p. 666–684, 2022. DOI: 10.51891/rease.v8i9.6822. Disponível em: https://periodicorease.pro.br/rease/article/view/6822. Acesso em: 11 maio. 2025.

**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. DOI: 10.5281/zenodo.8335572. Disponível em: https://periodico.agej.com.br/index.php/revistamagis/article/view/44. Acesso em: 6 set. 2025.

**SPDM – Associação Paulista para o Desenvolvimento da Medicina.** *Ciberataques na área de saúde.* São Paulo: SPDM. Disponível em: https://spdm.org.br/wp-content/uploads/2022/06/2a-Ed.-CIBERATAQUES-NA-AREA-DE-SAUDE_Rev.pdf. Acesso em 06 set. 2025.

**VALDEMIRO, Vitória da Cruz.** O caso Klara Castanho: a responsabilidade civil do profissional no que concerne ao prontuário médico à luz da LGPD. 2023.

Monografia (Bacharelado em Direito) – Universidade Federal de Ouro Preto, Ouro Preto, 2023. Acesso em: 6 set. 2025.

**ZAGANELLI, Margareth Vetis; BINDA FILHO, Douglas Luis.** O sigilo médico e os dados sensíveis na telemedicina à luz da Lei Geral de Proteção de Dados. RECIIS, [S. l.], v. 17, n. 3, 2023. DOI: 10.29397/reciis.v17i3.3689. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/3689. Acesso em: 11 maio. 2025.