

A EMERGÊNCIA DA PROTEÇÃO DE DADOS SENSÍVEIS NO DIREITO À SAÚDE

THE EMERGENCE OF SENSITIVE DATA PROTECTION WITHIN THE RIGHT TO HEALTH

¹ Rosimerie Policiano
Mendes Constantino 

² Luiz Claudio
Gonçalves Junior 

RESUMO | O objetivo geral é analisar a importância da proteção dos dados pessoais sensíveis no contexto do direito fundamental à saúde. Como objetivos específicos, busca examinar a evolução histórica do direito à privacidade e da proteção de dados no Brasil, analisar os deveres impostos aos profissionais e instituições de saúde quanto ao tratamento dessas informações e investigar o entendimento jurisprudencial acerca da LGPD. O problema de pesquisa consiste em verificar em que medida a LGPD é capaz de assegurar a proteção dos dados sensíveis na área da saúde. A hipótese sustentada é a de que a efetiva observância dos princípios e regras previstos na LGPD fortalece a proteção do direito fundamental à saúde, reduz os riscos de discriminação, etc. A justificativa fundamenta-se na crescente utilização de tecnologias digitais, sistemas de telemedicina e dados na prestação de serviços de saúde. Adotou-se a revisão bibliográfica, legislação, doutrina especializada e jurisprudência pertinente.

Palavras-chave: Lei Geral de Proteção de Dados; direito à saúde; dados pessoais sensíveis; privacidade; proteção de dados.

Abstract | The general objective of this study is to analyze the importance of protecting sensitive personal data within the context of the fundamental right to health, in light of the General Personal Data Protection Law. Specific objectives include examining the historical evolution of the right to privacy and data protection in Brazil, understanding the legal framework applicable to sensitive health-related data, analyzing the obligations imposed on healthcare professionals and institutions regarding the processing of such information, and investigating judicial precedents concerning the application of the law in this sector. The research problem lies in determining the extent to which the law ensures the protection of sensitive data in healthcare, balancing the necessary sharing of medical information with the preservation of fundamental rights to privacy, personal intimacy, and human dignity. The hypothesis maintained is that effective adherence to the principles and rules set forth in the LGPD strengthens the protection of the fundamental right to health and reduces the risks of discrimination, data breaches, and the misuse of sensitive information, while also fostering greater legal certainty and trust in the relationship between patients and healthcare institutions. This rationale is grounded in the increasing use of digital technologies, electronic health records, telemedicine systems, and databases in healthcare delivery factors that heighten the risks associated with the improper handling of sensitive information and make the implementation of the protection mechanisms provided by law essential. The research employed a literature review method, analyzing legislation, specialized legal scholarship, and relevant case law, thereby highlighting the need to strengthen a data protection culture as an indispensable tool for realizing the fundamental right to health.

1 Aluna do Curso de Direito do Centro
Universitário de Volta Redonda - Uni-
FOA

2 Professor e pesquisador do Centro
Universitário de Volta Redonda - Uni-
FOA

INTRODUÇÃO

A tecnologia traz dinamismo e mudança aos dados pessoais por causa da criação e recriação de ferramentas utilizadas no mundo digital. Disso surge o problema do limite imposto à proteção de dados em relação ao meio técnico e como tais ferramentas são usadas para acessar essas informações específicas.

Com o desenvolvimento da tecnologia, que proporcionou uma nova forma de organizar, transmitir, coletar, armazenar e processar informações na Internet, a informação foi cada vez mais utilizada para desenvolver necessidades econômicas e segurança do usuário. No entanto, a posição do proprietário da informação e do consumidor de bens foi duramente criticada e tornou-se mais vulnerável, pois a informação passou a circular entre os participantes da atividade econômica e a intimidade e as opções foram ultrapassadas pelos interesses de grandes empresas em detrimento da vontade individual.

Além disso, o indivíduo passa por um processo de despersonalização ao perder o direito exclusivo à sua personalidade. Justamente nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) é criada para mobilizar a sociedade e o mercado quanto à importância dos dados pessoais para avaliar qual limite de exposição é aplicável e quando é permitido. A LGPD controla a regulamentação do relacionamento entre as partes envolvidas e, além da fiscalização do caso, esclarece a rotulagem positiva, as regras e as penalidades cabíveis caso o uso adequado e sigiloso dos dados coletados para fins financeiros não sejam seguidos.

No contexto da saúde, a proteção dos dados é especialmente crucial, uma vez que informações sensíveis e privadas dos pacientes são frequentemente coletadas, armazenadas e compartilhadas por profissionais de saúde, hospitais, clínicas e seguradoras. Com a implementação da LGPD, os profissionais de saúde e as instituições médicas devem adotar medidas adequadas para garantir a segurança e a privacidade dos dados dos pacientes. A aplicação adequada da LGPD nesse setor pode garantir que os pacientes tenham controle sobre suas informações pessoais e que esses dados sejam tratados com responsabilidade, evitando vazamentos, acesso não autorizado ou uso indevido.

O objetivo da lei é proteger os direitos básicos das pessoas físicas à liberdade, à privacidade, bem como, garantir que o processamento relacionado à coleta de dados pessoais seja realizado de forma responsável, de boa fé e de acordo com as melhores práticas previstas na legislação em vigor. Sendo assim, faz-se necessário uma análise atual da conjuntura da privacidade bem como da legislação para que se possa assumir uma perspectiva coesa e coerente com o novo paradigma da intimidade.

O presente estudo adota a revisão bibliográfica como método científico, procurando destacar a importância e a urgência de adequar as práticas de tratamento de dados sensíveis na área da saúde, explorando as possíveis consequências da aplicação inadequada da LGPD no direito à saúde, como o comprometimento da confiança entre pacientes e prestadores de serviços de saúde, a exposição de informações sensíveis que podem levar a discriminação ou constrangimento, bem como as sanções e penalidades previstas na lei para aqueles que não cumprem suas disposições.

1 SÍNTESE HISTÓRICA DO DIREITO DE PRIVACIDADE

O objetivo deste capítulo é fazer uma breve descrição a despeito do desenvolvimento da proteção de dados pessoais no Brasil, que possui como importante marco legal a Lei Geral de Proteção de Dados Pessoais (LGPD), conforme será demonstrado nas subseções a seguir.

1. 1 A evolução da internet: breves apontamentos

O século XX foi uma época de enorme desenvolvimento tecnológico, de circulação de informações, de aperfeiçoamento da comunicação, como o computador, que iniciou sua trajetória em 1943, e de criações como a Internet, que começou a ser criada em 1969. Após a popularidade da Internet, ela gradualmente se desenvolveu e se tornou indispensável na vida humana, como um computador. Quando o computador foi conectado à Internet, o desenvolvimento tecnológico atingiu uma velocidade sem precedentes e se espalhou pelo mundo (DONEDA, 2011).

A chamada World Wide Web, chamada de Internet, foi desenvolvida durante a Guerra Fria com fins militares. O computador foi utilizado pelos militares dos Estados Unidos como meio alternativo de comunicação diante das forças inimigas. Foi assim que surgiu a “Advanced Research Projects Administration” (ARPANET) como a primeira rede nacional de computadores (1969). Foi incumbida de conectar computadores em laboratórios de pesquisa, universidades e, principalmente, em instituições militares. Em 1972, houve a possibilidade de compartilhamento de informações, pesquisas e estratégias militares. Em 1980, foi lançado o protocolo aberto TCP IP (Transmission Control Protocol), que permitia a conectividade de sistemas heterogêneos (CASTELLS, 2015).

A rede foi estendida para vários dispositivos como microcomputadores, estações de trabalho e mainframes, mas foi em 1983 que a definição da Internet foi separada da rede civil e ambiente militar. Em 1991, nasceu a rede mundial de computadores World Wide Web (WWW), que possibilitou a transmissão de vídeos, fotos e sons, com maior amplitude na web (ADRIEN, 2014).

A internet se difundiu e ganhou dimensões globais. No Brasil, passou a ser utilizada na década de 90, segundo o Sindicato Brasileiro dos Provedores de Serviços de Comunicação em 1996, com trezentos mil brasileiros online. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), em 2014, mais da metade dos domicílios brasileiros tinha acesso à Internet (cerca de 36,8 milhões de domicílios), decorrente do acesso à internet por celulares, tablets, televisões e outros aparelhos. Acrescente-se, ainda, a evolução dos smartphones (BOFF; FORTES, 2014).

De acordo com a empresa de rastreamento de tráfego de Internet StatCounter, em 2016, o acesso à internet via tablets e celulares foi pela primeira vez superior ao dos computadores tradicionais, embora o uso de computadores ainda seja significativo (CAVALCANTI; SANTOS, 2018).

Merece atenção o chamado ciberespaço, que segundo Lévy, é um novo meio de comunicação que surge da interligação global de computadores. Essa terminologia abrange não apenas a infraestrutura física das comunicações digitais, mas também o vasto oceano de informações contido nele, bem como as pessoas que exploram e contribuem para esse universo. Por outro lado, o termo “cibercultura” define as tecnologias (tanto materiais quanto intelectuais), práticas, atitudes, formas de pensamento e valores que se desenvolvem juntamente com o crescimento do ciberespaço (LÉVY, 2000).

A era cibernético-tecnológica influenciou o cotidiano das pessoas de diversas formas, pois com sua criação foi introduzido um ambiente virtual, que possibilita amizades virtuais, comunidades, tornando a navegação nesses ambientes uma prioridade na vida das pessoas, como meio de comunicação social. Dadas as muitas interações e compartilhamento de informações, é importante saber a diferença entre informações pessoais e categorias especiais de informações, conforme discutido no próximo tópico.

1. 2 Principais especificidades sobre dados pessoais e categoriais de informação

A importância da proteção legal dos dados pessoais reside no fato de que tanto esses como outros dados deles obtidos quase representam uma pessoa perante a sociedade, o que representa uma parte real de sua personalidade. Portanto, embora nem sempre de uso prático óbvio, uma explicação da diferença entre os conceitos de dados pessoais e informações pessoais pode ser útil para uma discussão aprofundada sobre o assunto (BOFF; FORTES, 2014).

Quando se utilizam os termos dados pessoais e informações pessoais, é inegável que os dois se sobrepõem em diferentes circunstâncias e representam certos aspectos do fato, da realidade. Em termos de detalhes, dados podem ser vistos como um termo primitivo e fragmentado, que pode ser entendido como informação em estado potencial, que se torna informação somente quando é transmitida, recebida e compreendida (CAVALCANTI; SANTOS, 2018).

Segundo Souza (2018) esse conhecimento é anterior ao processo interpretativo e criativo. Assim, aparece como uma conjuntura de eventos, ações humanas que tendem a mudar as pessoas, conteúdos, entre outras coisas, segundo a personalidade, afetividade.

Normalmente, os objetos devem ser identificadas ou pelo menos identificáveis, mas nem sempre é esse o caso, por exemplo, nos casos em que a informação se refere a pessoa de natureza não especificada. Em tais situações, segundo Souza:

As informações são mantidas anônimas e utilizadas para fins estatísticos e protegem as pessoas cujas informações foram previamente coletadas e armazenadas. Ressalta-se que, por serem esses dados anônimos e tratados de forma a impossibilitar a identificação, deixam de estar sujeitos à disciplina e proteção da proteção de dados pessoais, uma vez que não violam a natureza protetiva desse direito: a privacidade e personalidade humana (SOUZA, 2018, p.35).

Dados pessoais são algo que vão além do conteúdo e requerem um procedimento prévio para sua análise. Eles podem ser compartilhados de inúmeras formas, sejam fotos, vídeos, e diversas situações, inclusive coisas relacionadas a valores (CATALA, 2011).

Com base na Convenção de Strasbourg, uma boa forma de conceituar a terminologia seria a seguinte: “qualquer informação sobre uma pessoa natural identificada ou identificável” (SOUZA, 2018, p.41).

As informações pessoais, portanto, diferem das demais por um viés mais objetivo entre o indivíduo e as informações relevantes, independente das questões que lhes dizem respeito. Essa conexão subjetiva seria “além de outras categorias de informações que, embora possam ter alguma relação com a pessoa, não seriam exatamente informações pessoais” (DONEDA, 2011, p.78).

Diante disso, é muito importante esclarecer que o objetivo da proteção de dados ou informações pessoais é proteger a pessoa e sua personalidade, e não o dano em si (CAVALCANTI; SANTOS, 2018).

Com isso em mente, o tópico a seguir discute categorias de dados específicas que representam uma categoria de dados que representa uma ameaça maior à personalidade do indivíduo.

1.3 Categorias especiais de informação: eventuais riscos de discriminação

Essa análise desenvolve-se a partir do conhecimento de que determinados dados podem constituir uma ameaça mais grave, à personalidade e à liberdade da pessoa, podendo levar a ações discriminatórias, por exemplo (BOFF; FORTES, 2014).

É muito importante proteger todo tipo de informação, mesmo aquelas que não são consideradas tão importantes, pois mesmo que pareça algo insignificante, pode se tornar sensível ao longo do caminho (BOFF; FORTES, 2014).

Nesse sentido, Mendes acrescenta que: “É [...] com tratamento de dados sensíveis que é capaz de transformar dados inofensivos em dados potencialmente discriminatórios”. (MENDES, 2014, p.150).

Portanto, dados sensíveis podem se transformar em informações discriminatórias e gerar implicações éticas e legais significativas. A crescente utilização de tecnologias de Big Data e análise de dados exige uma reflexão cuidadosa sobre como equilibrar a privacidade dos indivíduos e os interesses das empresas e governos.

Segundo Martins: “informações insignificantes podem adquirir um novo valor. Dessa forma, deixarão de ser gerados dados irrelevantes no tratamento eletrônico de dados”. (MARTINS, 2014, p.02). Há casos em que a utilização é legal e necessária, por exemplo em atividades de investigação ou mesmo médicas, razão pela qual não cabe a recusa total no tratamento de dados pessoais (MARTINS, 2014).

Por último, importa referir que o artigo 6.º do RGPD (Regulamento Geral de Proteção de Dados), que regula a matéria na União Europeia, não impede a plena utilização desta informação, apenas em alguns casos (BOFF; FORTES, 2014).

As principais preocupações de proteção de dados pessoais referentes à saúde dizem respeito a não discriminação e à manutenção das oportunidades sociais. Em atenção a esse imperativo, a LGPD confere grau de proteção especial, ao tratar as informações relativas à saúde como dados pessoais de natureza sensível, submetidos a regime limitado de tratamento, especialmente em relação ao consentimento ou não do titular dos dados. Ou seja, o regime adotado para a saúde pela LGPD depreende que os dados sejam utilizados para a sua finalidade, exigindo coerência entre a natureza do dado e o respectivo emprego, de forma que não sujeite o seu titular a práticas discriminatórias.

O direito fundamental de proteção à saúde e ao bem-estar dos cidadãos é um bem coletivo, com status normativo e fundamentação no ordenamento jurídico brasileiro. A Constituição Federal de 1988 contém diversas disposições relacionadas a esse direito, incluindo o objetivo fundamental da República de promover o bem-estar de todos, sem discriminação, e o direito social à saúde, além de outras garantias.

A LGPD estabelece penalidades administrativas que somente a ANPD (Autoridade Nacional de Proteção de Dados) pode aplicar em caso de violação do direito fundamental à saúde. A Lei confere ainda prioridade à ANPD na salvaguarda dos dados pessoais, sobrepondo-se a qualquer outra entidade ou órgão da administração pública. A importância dos direitos e liberdades fundamentais justifica um tratamento especial para os dados pessoais que são inerentemente sensíveis.

1.4 Evolução da proteção de dados no Brasil

A proteção à privacidade no Brasil aconteceu mediante a evolução da tecnologia, principalmente na questão da comunicação e informação. Por isso, a nossa legislação enfatizou o princípio da proteção, com

instrumentos normativos e controle da distribuição das informações pessoais, visando assegurar a privacidade e inviolabilidade dos dados. Essa preocupação veio tardiamente, em que pese a sua relevância jurídica e sociocultural (BOFF; FORTES, 2014, p.245).

Com o conceito de ciberespaço, também surgiu a criação dos primeiros softwares para navegação nas World Wide Web, por conta da Guerra Fria, onde não há um confronto direto, mas de guerra de informações, narrativas ideológicas. Com o tempo, finda a guerra fria, ocorreu uma democratização da informação, o acesso a população e processos de inclusão digital para a população (BOFF; FORTES, 2014).

A partir disso, surgem os problemas jurídicos decorrentes da popularização do uso das redes. Por isso, a necessidade de diretrizes e marcos regulatórios em escala global, com o objetivo de criar normas para o uso das redes, visando proteger a privacidade de dados (BOFF; FORTES, 2014).

O direito à privacidade abrange a preservação da intimidade, vida privada, inviolabilidade e assegura o direito a indenização pelo dano material ou moral, decorrente dessas violações. Havia uma lacuna na legislação e no sistema jurídico brasileiro em relação às violações de garantias e direitos fundamentais na rede, bem como à proteção de dados e à infraestrutura tecnológica para garantir o acesso à internet a toda a população, entendido como um direito essencial para o exercício da cidadania. Isso inclui o sigilo das comunicações, a não suspensão da conexão e a inviolabilidade. Essa falta foi suprida com a aprovação do Marco Civil da Internet (BRASIL, 2014).

Um dos exemplos do uso de forma subsidiária para a proteção de privacidade dos dados é o Código de Defesa do Consumidor, que dispõe sobre a possibilidade de acesso pelo consumidor a qualquer espécie de dados cadastrados no banco de dados da empresa. Também há a lei de habeas data que permite o conhecimento ou retificação de informações em bancos de dados de entidades governamentais ou de caráter público.

Contraditoriamente, foi aprovada a Lei do Cadastro Positivo (Lei nº 12.414/11), o qual permite a troca de dados entre instituições financeiras sobre informações de adimplemento ou não dos débitos, para então haver a formação criação de histórico de crédito, então por seguinte criar uma linha de crédito diferenciado, com juros diversos aos que estejam adimplentes em dia (bom pagador). Há a Lei de acesso à informação (Lei nº 12.527/11), respaldada no inc. XXXIII do Art. 5 da Constituição Federal. Vale mencionar a Lei Carolina Dieckmann (Lei nº 12.737/2012), que trouxe para o ordenamento jurídico brasileiro a criminalização da conduta de invasão de dispositivo informático, inserindo ao Código Penal brasileiro o artigo 154-A (BRASIL, 2012).

Outra lei importante foi o Marco Civil da internet (Lei nº 12.965/14), a qual regulamentou o uso da internet, sob o prisma de 3 princípios: Princípio da neutralidade da rede (trata-se da obrigação dos provedores de internet de tratar todos os dados que trafegam na rede de forma isonômica, sem distinção de conteúdo, origem, destino ou serviço); Privacidade (Esse princípio assegura a inviolabilidade e o sigilo da troca de informações entre os usuários e o da liberdade de expressão, prevendo a devida responsabilização e a quebra do sigilo de dados, sob intimação judicial, para os casos em que os dados coletados possam contribuir para descoberta de ilícitos) e princípio da colaboração (estabelece que a governança da internet deve ser feita de forma colaborativa, envolvendo diversos setores da sociedade, como governo, empresas, sociedade civil e academia).

Portanto, como se pode observar, conforme a evolução dos mecanismos tecnológicos, tem sido uma tendência a evolução das leis, de maneira a tutelar os bens jurídicos mais importantes no ordenamento jurídico brasileiro.

1. 5 Do direito à privacidade e a proteção de dados pessoais

No final do século XIX, aumentou o debate sobre o direito à privacidade. Os pioneiros na área criticaram a invasão de privacidade por jornais, fotografia e outras tecnologias emergentes, argumentando que as pessoas têm o direito de proteger sua privacidade e intimidade contra a invasão da imprensa sensacionalista e da exposição pública não autorizada de suas vidas privadas. Desde então, o direito à privacidade tornou-se um tema central no debate sobre as implicações das tecnologias de informação e comunicação (DONEDA, 2016).

A proteção dos dados pessoais extrapola seu escopo e pode ser compreendida como um fenômeno coletivo em razão dos danos causados pelo uso indevido dessas informações, os quais demandam uma proteção jurídica coletiva específica.

Não é fácil resolver todos os problemas decorrentes do processamento de dados pessoais em relação à privacidade. Isso ocorre porque o conceito não abrange os problemas individuais e coletivos decorrentes dos sistemas atuais de classificação e risco, como o uso de informações genéticas de pacientes de planos de saúde ou a discriminação em supermercados com base no CEP (DONEDA, 2016).

Com as novas tecnologias, o armazenamento e o processamento eficiente de dados pessoais possibilita a proteção da privacidade e a combinação dessas informações. A mudança não se restringe apenas ao conteúdo dos direitos da personalidade, mas também aos conceitos presentes em sua própria nomenclatura, tais como a confidencialidade da informação, a proteção de dados pessoais e o direito à autodeterminação da informação, entre outros. Atualmente, esses dados são considerados reflexos da própria personalidade do indivíduo. (MENDES, 2008).

A doutrina brasileira faz uso de uma profusão de termos distintos para se referir à privacidade: vida privada, intimidade, segredo, sigilo, recato, reserva, entre outros. Isso ocorre porque, tanto o constituinte quanto o legislador ordinário, ao elaborarem a Constituição de 1988 e o Código Civil de 2002, escolheram não fazer menção expressa ao termo “privacidade”, mas das expressões “vida privada” e “intimidade”.

O direito à vida privada e à intimidade são considerados ramificações do direito à privacidade, portanto, a diferenciação entre vida privada e intimidade não possui muita utilidade, vez que são atributos da personalidade que podem assumir o mesmo significado ou alcance jurídico em razão da subjetividade que carregam. Em razão disso, a jurisprudência tem utilizado a expressão privacidade para se referir, sem distinção, à proteção da intimidade e da vida privada. (SCHREIBER, 2013).

A Constituição de 1988 não menciona explicitamente o termo “privacidade”, mas utiliza as expressões “vida privada” e “intimidade”. A falta de uma definição clara desses conceitos na legislação permitiu que a doutrina jurídica elaborasse diferentes interpretações e distinções entre eles. Assim, na doutrina brasileira, é comum encontrar uma variedade de termos e definições para se referir à privacidade. Cada termo pode ser usado em contextos específicos para abordar nuances e aspectos particulares relacionados à proteção da privacidade.

A privacidade é consagrada como um direito fundamental e faz parte do conjunto dos direitos de personalidade. A proteção à privacidade encontra-se tanto na legislação infraconstitucional, art. 21 do Código Civil, quanto na Constituição, no qual o constituinte alude expressamente à inviolabilidade da “intimidade” e da “vida privada”, assegurando no art. 5º, inciso X: “o direito a indenização pelo dano material ou moral decorrente de sua violação”. O Art. 5º, inciso XII e XI, faz menção ao termo “sigilo” ao garantir a inviolabilidade do sigilo das comunicações, das correspondências, das comunicações telegráficas, de dados e telefônicas e expande o âmbito da privacidade individual ao garantir a inviolabilidade da casa do indivíduo.

O legislador ordinário limitou-se a repetir o conteúdo do art. 5º, inciso X, da Constituição e, desta forma, falhou em desenvolver o comando constitucional para regular as hipóteses de violação à privacidade e oferecer mecanismos para prevenção e solução de conflitos.

No que tange aos remédios constitucionais, o habeas data (art. 5º, inciso LXXII) é considerado instrumento útil para coibir e corrigir violações à privacidade. O direito à privacidade, deve ser reconhecido em sentido genérico e amplo, “de modo a abarcar todas as manifestações da esfera íntima, privada e da personalidade, que o texto constitucional consagrou” (SILVA, 2013).

Ademais, a tutela da privacidade, em todas as suas perspectivas, deve garantir, antes de tudo, a liberdade da pessoa para a construção e desenvolvimento de sua identidade e esfera íntima. Nesse sentido, importante se faz abordar a Lei Geral de Proteção de Dados Pessoais (LGPD), que é um importante marco no ordenamento jurídico brasileiro para o tema em questão, conforme será demonstrado a seguir.

2 DIREITO FUNDAMENTAL À SAÚDE E A APLICABILIDADE DA LGPD

O presente capítulo tem por finalidade analisar os principais aspectos do Direito à Saúde sob o contexto da Lei Geral de Proteção de dados, em especial, no que diz respeito a proteção de dados sensíveis, os quais necessitam de consentimento especial para seu tratamento, conforme será abordado ao longo deste tópico.

2.1 Do direito à saúde na Constituição Federal de 1988.

Sabe-se que a promulgação da Constituição Federal de 1988 foi um grande marco, principalmente por consagrar diversos direitos aos cidadãos, como os direitos sociais, econômicos, políticos e culturais.

A nova ordem constitucional, fundamentada no Estado Democrático de Direito, consagrou uma série de princípios fundamentais, incluindo a soberania, a cidadania e a dignidade da pessoa humana. Dessa forma, se estabeleceu que “todo poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição” (FIGUEIREDO, 2017, p.150).

A Constituição Cidadã foi elaborada com a participação ativa da sociedade civil e por trazer importantes avanços na proteção dos direitos fundamentais e sociais. Um dos grandes avanços da Constituição de 1988 foi a consagração do direito à saúde como um direito social, garantindo a todos o acesso aos serviços públicos de saúde de forma gratuita e universal, sendo um dever do Estado.

Com o transcorrer dos anos, as alterações na definição do que seria saúde ajudaram ainda mais na efetivação deste direito. Essa evolução permitiu um entendimento mais abrangente do que realmente seria essa garantia hodierna. Constituindo-se com um direito humano e fundamental, o direito à saúde é fruto de uma longa e expressiva jornada na formulação não somente de um direito, porém também de uma ideia mais própria do que seria a saúde (FIGUEIREDO, 2017).

A garantia do direito à saúde pode ser interpretada de diversas maneiras, a depender da titularidade e da divisibilidade do bem tutelado. Embora haja um direito individual à saúde, enquanto um direito restrito à incolumidade ou segurança pessoal, a tendência contemporânea deve ser centrada na dimensão de proteção dos direitos metaindividuais da sociedade (SOBRINHO, 2016).

Tendo em vista a importância global deste direito, fora firmada pela Declaração Universal dos Direitos Humanos em 1948, a saúde como um direito humano fundamental, estabelecendo a obrigação dos

Estados de garantir um padrão de vida capaz de assegurar a saúde e o bem-estar. Por isso, consta no artigo 6º da Constituição Federal de 1988, a saúde como um direito social de todos, tendo o Estado a responsabilidade de garanti-los de maneira universal e igualitária.

A Carta da República de 1988 elevou o direito a saúde a um patamar irrevogável, agasalhando-o não apenas como um bem jurídico digno de tutela, mas com o status de direito fundamental, reconhecendo-lhe maior proteção jurídica (SARLET, 2012).

O direito fundamental à saúde é reconhecido como direito humano universal e previsto na Constituição Federal brasileira. A garantia deste direito implica na necessidade de proteção dos dados pessoais dos indivíduos, especialmente no contexto da saúde, fortalecido pela Lei Geral de Proteção de Dados (LGPD).

2. 2 Dados sensíveis e a LGPD

Os dados pessoais sensíveis são definidos como aqueles que estão diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo. Dessa forma, são considerados dados pessoais sensíveis informações que dizem respeito à origem racial ou étnica, crença religiosa, opinião política, filiação a sindicato ou a organizações religiosas, filosóficas ou políticas, dados relativos à saúde ou à vida sexual, dados genéticos ou biométricos quando vinculados a um indivíduo. O conceito de dados sensíveis é abordado no artigo 5º, II, da Lei Geral de Proteção de Dados, que inclui informações relacionadas à saúde. Esses dados são considerados extensões da personalidade do indivíduo e são relevantes para sua privacidade e identidade, merecendo uma proteção jurídica mais robusta.

Levando em conta o artigo 35 do Regulamento Geral de Proteção de Dados (RGPD), informações pertinentes à saúde incluem aquelas que dizem respeito ao estado de saúde do titular de dados e que revelem informações sobre sua saúde física ou mental no passado, presente ou futuro (DALLARI; MONACO, 2021).

Assuntos relacionados à saúde são de grande relevância, uma vez que afetam diretamente a privacidade e a intimidade do indivíduo, tornando-se, assim, dados sensíveis, os quais necessitam de maior proteção.

Os dados médicos e genéticos são considerados excepcionalmente sensíveis pelas leis de proteção de dados e possuem status especial que requer medidas adicionais de proteção, segurança e confidencialidade (TINTO, 2018).

A divulgação destes dados poderia vir a causar uma possível discriminação a um indivíduo, justificando assim a relevância de sua maior proteção, visto que detém um grande potencial de atingir os direitos humanos. O seu compartilhamento não autorizado pode causar discriminação e estigmatização social (VIEIRA; COSTA, 2021).

O setor médico, coleta e processa grandes quantidades de dados pessoais com base nos serviços prestados aos pacientes e tem grande responsabilidade pela proteção desses dados.

A violação de dados sensíveis em hospitais é agravada quando são considerados “devassáveis”. Diante disso, as organizações de saúde precisam proteger melhor a confidencialidade dos dados do paciente por meio de fortes políticas de privacidade que possam garantir transparência, simplicidade e acessibilidade do paciente. Os pacientes são, portanto, muito importantes porque são proprietários dos dados e devem ser informados sobre como eles são usados (TINTO, 2018).

A LGPD define em seu artigo 5º, inciso V, o titular como a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Os direitos do titular dos dados, sensíveis ou não, estão previstos no artigo 18 da LGPD. Além do direito de propriedade, são concedidos direitos de: confirmação da existência do tratamento; acesso aos dados; informações sobre o compartilhamento; correção de dados; eliminação de dados; portabilidade de dados; possibilidade de não consentimento; e retirada do consentimento (BRASIL, 2018).

As disposições normativas tratam especialmente de garantir seus direitos, visto que são os verdadeiros detentores dos dados. A LGPD conferiu aos seus detentores um conjunto de direitos que devem ser respeitados durante o processo de tratamento de dados, como o direito de solicitar a anonimização e a exclusão de dados desnecessários ou tratados com base no consentimento (DALLARI; MONACO, 2021).

A LGPD tem como princípio fundamental que as pessoas tenham conhecimento e controle sobre a coleta e o processamento de suas informações pessoais, especialmente aquelas que as identificam, permitindo que possam limitar esse processo, exigindo uma finalidade determinada, com medidas adequadas para prevenir danos e proteger as informações, mantendo-as apenas quando necessário e com o consentimento do titular durante todo o processo. O titular pode acessar e excluir seus dados (GREGORI, 2020).

O consentimento está previsto no artigo 7º, I, da LGPD, que afirma que o tratamento de dados pessoais apenas pode ocorrer com o consentimento de seu titular. Desse modo, o ordenamento normativo dá maior privilégio a participação ativa de seu titular, mediante a prioridade de seu consentimento (BRASIL, 2018).

O termo “livre” refere-se à ação do proprietário sem qualquer tipo de coação física, moral, mental ou artificial. Para obter informações, o titular deve ser informado de maneira clara e compreensível sobre o uso e o compartilhamento de suas informações. A finalidade específica requer a indicação clara e precisa dos objetivos do processamento de dados, proibindo licenças e usos que se afastem do contexto final (GREGORI, 2020).

O consentimento informado é uma escolha voluntária e informada que visa promover a autonomia, a autodeterminação, a integridade física do paciente. Entende-se que os pacientes têm direito a: participar nas decisões sobre os seus cuidados de saúde; de participar ativamente no aconselhamento sobre seus cuidados; de retirar o consentimento sem retaliação e ao consentimento informado sem coerção ou influência indevida. A partir disso, o autor obtém o direito de respeitar sua vida privada:

Tem uma ampla gama de aplicações no atendimento ao paciente, incluindo o direito de recusar qualquer tipo de tratamento, o direito de fazer escolhas quanto a visitas e exames físicos por profissionais médicos e o direito à confidencialidade das informações de saúde que eles respeitam. Direito de consentir em qualquer tipo de procedimento (ALBUQUERQUE, 2016).

Portanto, no âmbito da LGPD, os titulares devem ser notificados sobre o uso e a divulgação de seus dados de forma clara e compreensível. A finalidade declarada para o uso e processamento da informação deve ser clara e específica, sendo proibida a permissão geral e o uso fora do contexto.

2.3 Tratamento dos dados de saúde

No tocante à guarda dos prontuários, os profissionais ou a instituição que assistem o paciente são responsáveis por armazená-los de modo seguro (Art. 87 §2º, da Resolução CFM 2.227/2018), seja em meio físico ou digital, de modo a preservar-lhes o conteúdo e, conseqüentemente, o segredo e a não violação à esfera de privacidade e intimidade do assistido. Na área da saúde, portanto, a noção de que

os dados de saúde são espécies de dados sensíveis encontra respaldo na regulamentação ética e administrativa. O profissional da saúde deve saber que o histórico médico de um paciente contém informações sensíveis cujo vazamento acidental ou voluntário pode ser catastrófico para a vida dele e de seus familiares (LUCIANO; BRAGANÇA; TESTA, 2011).

Dados os riscos envolvidos no tratamento de dados de saúde, tem se formado uma legislação setorial robusta para impor obrigações e padrões mínimos de segurança no dever de guarda e manuseio dos registros dos pacientes, como as denominadas “e-Saúde”, que englobam serviços de teleconsultorias, teliagnóstico, telecirurgia, telemonitoramento, teleducação e prontuário eletrônico (KAMEDA; PAZELLO, 2015).

Também existem normas específicas que regulamentam o uso dessas tecnologias, tais como a Resolução nº 1.821/2007 do Conselho Federal de Medicina, que trata da telemedicina, e a Resolução nº 2.232/2019, que dispõe sobre o uso de sistemas eletrônicos para a guarda e manuseio de prontuários médicos.

Dessa forma, é fundamental que os profissionais de saúde e as instituições de saúde sejam diligentes na adoção de medidas de segurança e privacidade de dados, a fim de proteger a saúde e a privacidade dos pacientes, além de estarem em conformidade com as normas e leis em vigor.

O prontuário médico é um documento que reúne todos os dados da assistência prestada ao paciente. A Resolução CFM nº 1.638/2002, além de trazer o conceito de prontuário médico, traz informações sobre seu conteúdo essencial e as atribuições de responsabilidade sobre preenchimento, guarda e manuseio, bem como torna obrigatória a criação de Comissão de Revisão de Prontuários, a quem compete observar a qualidade dos dados inseridos no prontuário e verificar a presença dos requisitos mínimos para sua efetivação. Esses requisitos incluem a identificação completa do paciente, registro da anamnese, exame físico, exames complementares solicitados e seus resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento realizado, evolução diária do paciente, descrição de todos os procedimentos realizados e identificação dos profissionais responsáveis, com assinatura eletrônica quando armazenado em meio eletrônico, e, nos casos de prontuários em papel, a legibilidade da letra do profissional, identificação clara dos profissionais envolvidos (MALDONADO, 2015).

A Resolução CFM nº 1.821/2007, que revogou a Resolução CFM nº 1.639/2002, trouxe respaldo legal ao uso cada vez mais frequente de sistemas informatizados de guarda e manuseio dos prontuários, o chamado prontuário eletrônico do paciente (PEP) ou ainda prontuário médico eletrônico (PME). A legislação veio a tornar possível a eliminação total de prontuários em suporte de papel, desde que garantidos padrões mínimos de segurança aos sistemas informatizados aptos a garantir a preservação integral dos dados, o que compreende o uso de certificação digital e método de indexação que permita criar arquivo organizado, possibilitando a pesquisa de maneira simples e eficiente (KAMEDA; PAZELLO, 2015).

O Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS) firmaram um convênio de cooperação técnica científica para a elaboração de requisitos e avaliação da conformidade de sistemas de informação, mediante a edição contínua de manuais de certificação e expedição de selos de qualidade. O SBISCFM mantém em seu site cartilhas explicativas sobre a utilização de PEPs, bem como lista atualizada dos sistemas ativos certificados e auditados pelo convênio, com informações detalhas sobre o grau de segurança e as funcionalidades de cada sistema, o que denota a preocupação do setor em garantir o tráfego seguro de informações sensíveis de pacientes (LUCIANO; BRAGANÇA; TESTA, 2011).

Pesquisas indicam que a migração para prontuários eletrônicos ainda enfrenta uma série de desafios, como a falta de interoperabilidade entre os PME e outros sistemas de informação, não apenas entre diferentes sistemas, mas até dentro de um mesmo hospital ou clínica; o alto custo de sua implementação e de sua manutenção; e o impacto negativo real e/ou observado no fluxo de trabalho (SERPA NETO, 2017).

Em relação ao tratamento de dados e requisitos de segurança para equipamentos médicos, a Agência Nacional de Vigilância Sanitária (ANVISA) editou medidas regulatórias exigindo certificação compulsória de equipamentos que visam garantir a presença de mecanismos de segurança da informação, tendo em vista a importância dos dados sensíveis que trafegam em softwares médicos, bem como a interoperabilidade entre sistemas (RDC nº 40/2015).

No tocante à proteção dos dados produzidos em atividades de telessaúde no SUS, compete à Coordenação Nacional de Telessaúde Brasil Redes garantir a interoperabilidade e segurança das informações:

Art. 7º Compete à Coordenação Nacional do Telessaúde Brasil Redes: [...] V definir os padrões tecnológicos de interoperabilidade, conteúdo e segurança que permitirão a troca de informações entre os sistemas que viabilizam a operação do Telessaúde Brasil Redes e os diferentes sistemas de informação do SUS, incluídos o Cartão Nacional de Saúde e o Sistema de Cadastro Nacional de Estabelecimentos de Saúde (SCNES); VI definir o conjunto de dados que fará parte do Registro Eletrônico de Saúde (RES) a partir das Teleconsultorias realizadas, visando à implementação de um registro nacional e longitudinal, conforme Portaria nº 2.073/GM MS, 2073/GM/MS de 31 de agosto de 2011; e (Retificado no DOU nº 209 de 31.10.2011, Seção 1, página 74)(BRASIL, 2011, p.48).

Para além das inovações na comunicação entre profissionais da saúde, as tecnologias da informação e comunicação trouxeram possibilidades inovadoras para uso da telemedicina diretamente na relação profissional e paciente, tais como a teletriagem médica, a teleconsulta, telediagnóstico, telecirurgia, teleconferência de ato cirúrgico. A atividade, que está em pleno desenvolvimento na prática, chegou a ser regulamentada pelo CFM na Resolução CFM nº 2.227, no dia 13 de dezembro 2018, cujo objetivo era permitir e regulamentar a prática da modalidade no país, entretanto, devido a um elevado número de críticas e propostas de alteração por diversas entidades médicas, além do impacto social envolvido na medida, o órgão voltou atrás e revogou seu próprio ato, a fim de amadurecer a discussão e chegar a um novo texto.

3 REFLEXÕES JURISPRUDENCIAIS SOBRE A LGPD NA SAÚDE

Ao examinar a interpretação jurídica de diversos tribunais, que vão do Supremo Tribunal Federal aos Tribunais Estaduais, fica evidente que há um consenso de que o direito à saúde não é apenas um Direito Fundamental que atende a todos os indivíduos, mas também é um derivado constitucional que não pode ser separado do direito à vida.

3.1 Jurisprudências relacionadas à saúde

Em recente decisão recursal, o desembargador Nelson Schaefer Martins, do TJ-SC, enfatizou que é direito de todo cidadão receber assistência médica adequada, cabendo ao governo fornecê-la. De acordo com a Lex Fundamental, o tratamento de saúde deve incluir o fornecimento de medicamentos sem nenhum custo. Isso é essencial para garantir que aqueles que não podem pagar também possam manter uma boa saúde. Entre várias decisões judiciais que cercam o tema, uma delas foi proferida pelo Ministro Celso de Mello em um caso envolvendo um paciente soropositivo que fazia uso de medicamentos do Sistema Único de Saúde. O ministro reconheceu que esse direito carrega uma obrigação constitucional, que não pode ser dissociada do direito do indivíduo à vida.

A Suprema Corte possui inúmeros julgados sobre o assunto, em um destes, o Ministro Celso de Mello, julgando um caso de um paciente com HIV, dependente de medicamentos do Sistema Único de Saúde, garantiu que tal direito representa ônus constitucional, indissociável do direito à vida.

Ao julgar a ação cautelar 2.836, o ministro Ayres Britto, do Supremo Tribunal Federal, afirmou que “a saúde é qualificada constitucionalmente como um direito fundamental de dupla dimensão (direito social e individual indisponível)”. Em sua decisão sobre um Recurso Extraordinário, o Ministro Lewandowski afirmou que, quando confrontado entre proteger o direito à vida e à saúde ou priorizar um interesse financeiro secundário do Estado, o julgador deve fazer apenas uma escolha possível e ético-jurídica: aquela que favorece o respeito absoluto à vida e à saúde humana. Além disso, a ministra Carmen Lúcia considerou a distribuição de fraldas descartáveis a uma criança doente, um real fim terapêutico, não se configurando mera comodidade, afirmando ainda:

O direito à saúde de crianças e adolescentes detêm absoluta prioridade com respaldo nos artigos. 196 e 198 da CRFB/88 e no artigo 11, § 2º do ECA que atribui ao Poder Público o dever de fornecer gratuitamente àqueles que necessitem os medicamentos, próteses e outros recursos relativos a tratamento, habilitação ou reabilitação. (BRASIL, 2013).

Ante ao exposto, fica claro que é obrigação do Poder Público cumprir e avocar o direito que positivou, independentemente da forma utilizada para que tal direito seja concretizado, pois, de acordo com o artigo 23, inciso II, da Constituição Federal, cuidar da saúde é competência de todos os entes federados.

Conforme Schwartz, embora o direito à saúde dependa dos recursos materiais necessários para sua realização, é responsabilidade do Poder Público atuar na área da saúde e nenhum dos entes federativos que compõem a República Brasileira pode se eximir dessa obrigação. Além disso, os tribunais têm seguido essa mesma compreensão (SCHWARTZ, 2016).

A responsabilidade pelo fornecimento de atendimento médico é solidária entre a União, os Estados e os Municípios e, em caso de decisão sobre como dividir essa responsabilidade, cabe exclusivamente aos entes federativos fazê-lo em um momento adequado. Nenhum indivíduo pode ter seu direito constitucional à saúde limitado por ação da Administração Pública. Portanto, resguardar o direito a saúde é o mínimo que o Poder Público deve fazer ao cidadão, aja vista, que este é próprio do ser humano, sendo intrínseco ao mínimo existencial e se o Governo não garante de maneira administrativa, cabe ao judiciário o fazer, por meio da tutela jurisdicional.

A partir disso, uma das formas de proteger tal direito seria por meio da proteção de dados referentes a saúde, que ganhou especial contorno após a promulgação da LGPD, visto que além de exporem o paciente, muitas vezes, sem consentimento, tratam-se de dados sensíveis, os quais necessitam de consentimento especial para seu tratamento, conforme será abordado no tópico que segue.

3.2 Jurisprudências relacionadas à LGPD

A Lei Geral de Proteção de Dados entrou em vigor no Brasil em setembro de 2020, e desde então, já existem algumas decisões judiciais importantes relacionadas a ela como por exemplo na Liminar para exclusão de dados, onde, em decisão de novembro de 2020, o Tribunal de Justiça do Distrito Federal e dos Territórios concedeu uma liminar determinando a exclusão de dados pessoais de uma pessoa de uma plataforma de vendas online. A pessoa alegou que seus dados foram coletados sem seu consentimento e que a empresa não adotou medidas adequadas para proteger seus dados pessoais.

Na sua decisão, o desembargador Cesar Laboissiere Loyola afirmou que a atividade realizada pela ré configura o tratamento de dados pessoais, o que a torna sujeita à regulamentação pela norma legal

mencionada. Embora a norma permita o tratamento de dados para atender aos interesses legítimos do controlador ou de terceiros, ela também enfatiza a importância da proteção dos direitos e liberdades fundamentais do titular dos dados. Nesse sentido, mesmo que as informações em questão sejam normalmente fornecidas pelos indivíduos em suas relações comerciais e empresariais, como afirmado pelo juiz que proferiu a decisão inicial, a lei exige uma autorização específica para o compartilhamento desses dados.

Conforme alegado pelo Ministério Público, a prática em questão viola a Lei Geral de Proteção de Dados (LGPD), a qual atribui a responsabilidade pelo fluxo de dados pessoais na internet apenas ao proprietário dessas informações. Ademais, a conduta da empresa Serasa poderia infringir o direito à privacidade, à intimidade e à imagem dos indivíduos afetados, contrariando não apenas a LGPD, mas também disposições previstas na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor e no Marco Civil da Internet, de acordo com o MPDFT.

Recentemente, o juiz Douglas de Melo Martins, da Vara de Interesses Difusos e Coletivos do TJ-MA, decidiu condenar o Facebook ao pagamento de indenizações por danos morais a cada usuário que foi diretamente afetado pelo vazamento de dados pessoais ocorrido em 2021. Essa decisão foi tomada no Maranhão, e no Brasil, um total de 8.064 milhões de pessoas tiveram suas informações sensíveis expostas pela empresa.

“Instituto brasileiro de estudo e defesa das relações de consumo - ibedec - facebook serviços online do brasil ltda. –vazamento de dados – falha de segurança – falha na prestação de serviços, com fulcro na lei geral de proteção de dados – responsabilidade de reparar - dano moral in reipsa - dano moral coletivo” (Brasil, 2023).

O Ministério Público Estadual se pronunciou em relação a uma ação judicial e afirmou que os fatos apresentados na ação abalaram a relação jurídica, causando repugnância e desconfiança dos usuários do Facebook. Esses fatos envolvem a obtenção de dados pessoais dos usuários sem a observância da legislação brasileira, o que viola o princípio da boa-fé objetiva. O vazamento de dados pessoais é uma violação grave da privacidade dos usuários, e é cada vez mais comum em plataformas digitais como o Facebook. Nesse caso, a decisão do Tribunal de Justiça do Maranhão de condenar a empresa ao pagamento de indenização por danos morais aos usuários afetados é uma medida importante para garantir a proteção dos direitos dessas pessoas.

A Lei Geral de Proteção de Dados é um marco importante para a proteção dos direitos e liberdades fundamentais dos titulares de dados pessoais no Brasil. Como mencionado anteriormente, já houve algumas decisões judiciais importantes relacionadas a ela, e é fundamental que as empresas estejam em conformidade com a lei para evitar violações e possíveis sanções. As empresas precisam compreender a importância da proteção dos dados pessoais de seus usuários e implementar medidas adequadas para garantir a segurança dessas informações, como a adoção de políticas de privacidade claras e transparentes, a utilização de tecnologias de segurança eficazes e a realização de treinamentos e conscientização de seus funcionários.

Portanto, é importante que os usuários estejam cientes de seus direitos e saibam como exercê-los em caso de violação de seus dados pessoais, buscando reparação pelos danos sofridos. Enfim, a proteção dos dados pessoais é um tema cada vez mais relevante e deve ser tratado com seriedade pelas empresas e pelos usuários. A LGPD veio para fortalecer a privacidade e a segurança dos dados pessoais no Brasil, sendo fundamental que empresas e sociedade estejam conscientes de suas responsabilidades.

CONCLUSÃO

A proteção dos dados pessoais sensíveis constitui um dos maiores desafios impostos pela sociedade da informação, especialmente no âmbito da saúde, em que a utilização de tecnologias digitais, prontuários eletrônicos, plataformas de telemedicina e sistemas integrados de compartilhamento de informações exige um equilíbrio permanente entre a efetividade do direito fundamental à saúde e a preservação da privacidade dos indivíduos. Ao longo deste estudo, verificou-se que o avanço tecnológico, embora tenha proporcionado maior eficiência na prestação dos serviços de saúde, também ampliou significativamente os riscos relacionados ao tratamento inadequado de informações sensíveis, tornando indispensável a existência de um regime jurídico capaz de assegurar sua adequada proteção.

A análise histórica demonstrou que o direito à privacidade evoluiu em razão das constantes transformações tecnológicas, culminando na consolidação da proteção de dados pessoais como direito fundamental. Nesse cenário, a Lei Geral de Proteção de Dados Pessoais representa importante marco normativo ao estabelecer princípios, direitos e deveres voltados ao tratamento responsável das informações pessoais, conferindo especial tutela aos dados relativos à saúde em razão de seu elevado potencial discriminatório e de sua estreita relação com a dignidade da pessoa humana.

Também se constatou que a proteção dos dados de saúde não se limita ao cumprimento formal das exigências legais, mas exige a implementação de práticas efetivas de governança, segurança da informação, transparência e responsabilização por parte dos profissionais e das instituições de saúde. A observância dos princípios da finalidade, necessidade, adequação, segurança, prevenção e responsabilização fortalece a confiança entre pacientes e prestadores de serviços, reduz a ocorrência de vazamentos, acessos indevidos e tratamentos incompatíveis com as finalidades originalmente autorizadas, além de contribuir para a efetivação dos direitos fundamentais à intimidade, à privacidade e à autodeterminação informativa.

Sob o aspecto jurisprudencial, verificou-se que o Poder Judiciário brasileiro vem consolidando o entendimento de que tanto o direito à saúde quanto a proteção de dados pessoais possuem natureza fundamental, exigindo interpretação harmônica entre esses direitos. As decisões analisadas evidenciam que a responsabilização pelo tratamento inadequado de dados pessoais constitui importante instrumento de fortalecimento da LGPD, reafirmando a necessidade de observância rigorosa dos deveres legais por parte dos controladores e operadores de dados, especialmente quando se trata de informações médicas.

Dessa forma, os objetivos propostos foram alcançados ao demonstrar a relevância da proteção dos dados pessoais sensíveis no contexto do direito à saúde, analisando sua evolução normativa, os mecanismos instituídos pela LGPD e sua aplicação prática na proteção das informações dos pacientes. O problema de pesquisa também foi respondido, uma vez que se concluiu que a LGPD oferece instrumentos jurídicos adequados para conciliar o tratamento necessário dos dados de saúde com a proteção da privacidade, desde que suas disposições sejam efetivamente implementadas pelas instituições e acompanhadas por mecanismos de fiscalização e conscientização. Confirma-se, igualmente, a hipótese inicialmente formulada, pois a efetiva aplicação da Lei Geral de Proteção de Dados fortalece a tutela do direito fundamental à saúde, reduz riscos de discriminação, promove maior segurança jurídica e contribui para a construção de um ambiente digital pautado pela ética, pela transparência e pelo respeito aos direitos fundamentais dos titulares de dados. Assim, conclui-se que a proteção dos dados sensíveis na área da saúde não representa apenas uma exigência legal, mas um verdadeiro pressuposto para a garantia da dignidade da pessoa humana e para a consolidação de um sistema de saúde compatível com os valores constitucionais do Estado Democrático de Direito.

REFERÊNCIAS

ADRIEN, JAMMET. **The Evolution of EU Law on the Protection of Personal**. Issue, 2014

ALBUQUERQUE, Aline. **Direitos humanos dos pacientes**. Curitiba: Juruá, 2016.

BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental**: perspectivas de construção de um marco regulatório para o Brasil. Sequência (Florianópolis) [online]. 2014, n.68.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: <https://www2.senado.leg.br>. Acesso em: 10/03/2023.

_____. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br> Acesso em: 10/03/2023.

_____. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br> Acesso em: 10/03/2023.

_____. **Lei n. 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br> Acesso em: 10/03/2023.

_____. **Lei n. 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <http://www.planalto.gov.br> Acesso em: 10/03/2023.

CASTELLS, Manoel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2015.

CATALA, J. **Dados pessoais**: do conceito à proteção. Revista de Direito, Estado e Telecomunicações, 2011.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. A lei geral de proteção de dados do Brasil na era da big data. In: **Tecnologia Jurídica & Direito Digital – II**. Congresso Internacional de Direito, Governo e Tecnologia, 2, 2018, Belo Horizonte. Anais [...]. Belo Horizonte: Fórum, 2018, v.1, p. 351-366.

DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos e coordenação. **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011.

FIGUEIREDO, Luis. **Curso de direito constitucional**. São Paulo: Saraiva, 2017.

GREGORI, Maria Stella. **Os impactos da lei geral de proteção de dados pessoais na saúde suplementar**. Revista de Direito do Consumidor. v. 127, p. 171– 196, jan./fev. 2020.

KAMEDA, S. I.; PAZELLO, E. T. **Dados em Saúde e Regulação**: a Proteção de Dados Pessoais como Paradigma na Era da e-Saúde. Revista de Direito Sanitário, São Paulo, v. 16, n. 1, 2015.

LÉVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999.

LUCIANO, Eliane Maria Monteiro de Castro; BRAGANÇA, Maria de Lourdes; TESTA, Maria Lucia. **Privacidade e sigilo médico**: reflexões para a enfermagem. Revista da Escola de Enfermagem da USP, São Paulo, v. 45, n. 6, p. 1516-1521, dez. 2011. Disponível em: <https://doi.org/10.1590/S0080-62342011000600029>. Acesso em: 28/03/2023.

MALDONADO, Vinícius Navarro. **A importância do prontuário médico na prática médica.** Revista Médica de Minas Gerais, Belo Horizonte, v. 25, n. 1, p. 97-102, 2015.

MARTINS, Guilherme Magalhães. O direito ao esquecimento na Internet. In: **Direito Privado e Internet.** Coord: Guilherme Magalhães Martins. São Paulo: Editora Atlas, 2014.

MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) -Universidade de Brasília, Brasília, 2008. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 28/03/2023.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais.** Porto Alegre: Livraria do Advogado, 2012.

SCHREIBER, Anderson. **Direitos da personalidade.** São Paulo: Atlas, 2013.

SCHWARCZ, Lilia Moritz. **Brasil: Uma Biografia.** São Paulo: Companhia das Letras. 2016.

SERPA NETO. **Prontuários Médicos eletrônicos:** análise secundária para melhorar o atendimento ao paciente. TIC Saúde. Pesquisa Sobre o Uso de Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde brasileiros. Núcleo de Informação e Comunicação do Ponto BR; 2017.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** São Paulo: Ed. Malheiros, 2013.

SOBRINHO, Pilau. **A saúde como direito fundamental e o papel do Estado na sua garantia.** Revista Direitos Fundamentais & Democracia, v. 19, n. 1, 2016.

SOUZA, Rafael Santos de. Anonimização de dados pessoais: conflitos e desafios à proteção de dados pessoais. In: SOUZA, Guilherme Wunsch; CORREIA, Marcelo Roque Martins (Orgs.). **Proteção de dados pessoais:** doutrina e casos (pp. 31-48). Salvador: JusPodivm, 2018.

TINTO, Ana Rita Ramos Y Rio. **Proteção de dados de saúde Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Proteção de Dados da União Europeia.** 2018. Dissertação (Mestrado). Escola Nacional de Saúde Pública. Universidade Nova de Lisboa, Lisboa, 2018.

VIEIRA, Fabio Alonso; COSTA, Carolina Barbosa Cunha. **Data Privacy and Protection Relating to Healthcare in Europe, the United States and Brazil.** Latin Lawyer. August 2021. Disponível em: <https://latinlawyer.com/guide/the-guide-corporate-compliance/secondedition/article/24-data-privacy-and-protection-relating-healthcare-in-europe-the-united-statesand-brazil>. Acesso em: 10/03/2023