UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO

DIEGO MAIKON PALHETA DE SOUSA

ANÁLISE DA PROTEÇÃO DE DADOS SENSÍVEIS SOB A ÓTICA DA LGPD: ESTUDO DE CASOS DE VAZAMENTO DE DADOS NO SISTEMA ÚNICO DE SAÚDE (SUS)

BELÉM
2025

ANÁLISE DA PROTEÇÃO DE DADOS SENSÍVEIS SOB A ÓTICA DA LGPD: ESTUDO DE CASOS DE VAZAMENTO DE DADOS NO SISTEMA ÚNICO DE SAÚDE (SUS)

Trabalho de Conclusão de Curso apresentado a Faculdade de Direito, do Instituto de Ciências Jurídicas do Campus Universitário de Belém, da Universidade Federal do Pará como requisito parcial para obtenção do título de bacharel em Direito.

Orientador: Prof. Dr. Fabrício Vasconcelos de Oliveira.

BELÉM

2025

DIEGO MAIKON PALHETA DE SOUSA

ANÁLISE DA PROTEÇÃO DE DADOS SENSÍVEIS SOB A ÓTICA DA LGPD: ESTUDO DE CASOS DE VAZAMENTO DE DADOS NO SISTEMA ÚNICO DE SAÚDE (SUS)

Trabalho de Conclusão de Curso – TCC apresentado a UNIVERSIDADE FEDERAL DO PARÁ como requisito parcial para obtenção do título de bacharel em direito.

Aprovado em: __/__/____.

BANCA EXAMINADORA

_____

Fabrício Vasconcelos de Oliveira (orientador)

_____

Integrante da Banca II

_____

Integrante da Banca III

BELÉM

2025

Dedico este trabalho a todos meus familiares e amigos que me apoiaram em toda a minha vida acadêmica.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus pelo dom da vida e em mais esta batalha conquistada, pois chegar a este momento exigiu muito sacrifício e dedicação.

Agradeço e sempre serei grato ao apoio e dedicação dos meus pais, irmãos e demais familiares pelo suporte, sem o qual seria impossível atingir esta meta. Além deles, gostaria de homenagear minha avó Alenilda Felipe de Sousa pela lição de vida e fé inabalável em Deus e em minha pessoa.

Agradeço aos meus colegas de sala, os quais uniram forças quando foi preciso para exigirmos um ensino condizente com a importância desta instituição. Ademais, não poderia esquecer da Áurea Helena, Carlos Eduardo, Erik Rafael, João Louzada, Ana Carolina e José Aleff, membros da turma 40/2019 que apesar das divergências, sempre foi um grupo animado, onde surgiram boas amizades.

Agradeço também aos docentes e corpo técnico desta Faculdade pelo aprendizado dentro e fora da sala de aula e pelas lições transmitidas com o intuito de nos conduzirmos da melhor forma a um novo ciclo do campo profissional que poderemos seguir.

Agradeço também aos meus colegas de trabalho e amigos da Gerenciadora HLA, em especial ao Carlos Rocha pela sua compreensão e generosidade em fazer o possível para que eu pudesse cumprir minha jornada extensiva de horas obrigatórias e complementares, sem o qual meu sonho seria consideravelmente postergado.

Agradeço ao meu orientador Fabricio Vasconcelos Oliveira pela ombridade, sinceridade e atenção aos momentos que pude compreender melhor qual caminho estabelecer para apresentar este presente trabalho da melhor forma possível.

Por fim, agradeço a todas as pessoas que direta ou indiretamente contribuíram para que eu chegasse até aqui, o meu muito obrigado!!!

Tente (tente)
E não diga que a vitória está perdida
Se é de batalhas que se vive a vida
Tente outra vez.
Raul Seixas

RESUMO

Esta pesquisa revisou a proteção de dados sensíveis sob a perspectiva da Lei Geral de Proteção de Dados (LGPD), com foco em casos de vazamento no Sistema Único de Saúde (SUS). A abordagem metodológica consistiu em uma revisão bibliográfica baseada em artigos científicos, relatórios institucionais e legislações, publicados entre 2018 e 2024, acessados em bases de dados como Scielo e Google Scholar. Os estudos analisados discutiram falhas no tratamento de informações sensíveis no SUS, como a exposição de mais de 200 milhões de registros no sistema e-SUS Notifica, em 2020, e os impactos de ciberataques sobre instituições terceirizadas. O referencial teórico fundamentou-se na legislação da LGPD e em conceitos de segurança da informação, além de análises sobre ética e privacidade em saúde pública. Os principais resultados indicam que os vazamentos ocorreram devido a fragilidades tecnológicas, como a falta de autenticação multifator e a utilização de sistemas obsoletos, além de lacunas administrativas, como a ausência de políticas eficazes para gestão de dados e treinamento insuficiente dos profissionais. A aplicação da LGPD ainda enfrenta desafios significativos, evidenciados pela ineficácia de medidas preventivas e reativas em evitar novos incidentes. Consequentemente, a confiança do cidadão no SUS é abalada, afetando tanto a coleta de dados precisos quanto a adesão a programas de saúde. A pesquisa conclui que o fortalecimento da governança de dados é essencial para reverter esse cenário. Medidas como auditorias regulares, adoção de tecnologias avançadas e capacitação contínua dos agentes envolvidos são recomendadas para mitigar riscos e garantir a segurança das informações no SUS. A LGPD apresenta o potencial de consolidar uma cultura organizacional voltada para a proteção de dados, desde que sua aplicação seja integrada e efetiva.

Palavras-chave: LGPD; Proteção de Dados; Vazamentos; Saúde Pública.

ABSTRACT

This research reviewed the protection of sensitive data from the perspective of the General Data Protection Law (LGPD), focusing on cases of data leaks in the Unified Health System (SUS). The methodological approach consisted of a bibliographic review based on scientific articles, institutional reports, and legislation published between 2018 and 2024, accessed in databases such as Scielo and Google Scholar. The studies analyzed discussed failures in the treatment of sensitive information in the SUS, such as the exposure of more than 200 million records in the e-SUS Notifica system in 2020, and the impacts of cyberattacks on outsourced institutions. The theoretical framework was based on the LGPD legislation and information security concepts, in addition to analyses of ethics and privacy in public health. The main results indicate that the leaks occurred due to technological weaknesses, such as the lack of multifactor authentication and the use of obsolete systems, in addition to administrative gaps, such as the absence of effective policies for data management and insufficient training of professionals. The application of the LGPD still faces significant challenges, evidenced by the ineffectiveness of preventive and reactive measures in avoiding new incidents. Consequently, citizen trust in the SUS is shaken, affecting both the collection of accurate data and adherence to health programs. The research concludes that strengthening data governance is essential to reverse this scenario. Measures such as regular audits, adoption of advanced technologies and continuous training of the agents involved are recommended to mitigate risks and ensure the security of information in the SUS. The LGPD has the potential to consolidate an organizational culture focused on data protection, as long as its application is integrated and effective.

Keywords: LGPD; Data Protection; Leaks; Public Health.

SUMÁRIO

1. INTRODUÇÃO

A proteção de dados pessoais tornou-se uma questão central na sociedade atual, especialmente devido ao avanço das tecnologias digitais que permitem a coleta, o armazenamento e o compartilhamento de informações de maneira ampla. Embora essas inovações tragam inúmeros benefícios, elas também geram preocupações sobre a privacidade e a segurança das informações dos cidadãos. Nesse contexto, a promulgação da Lei Geral de Proteção de Dados (LGPD), em 2018, representou um marco importante no Brasil, ao estabelecer diretrizes claras para o tratamento e a proteção de dados pessoais (Hawryliszyn et al., 2021).

A LGPD, instituída pela Lei nº 13.709/2018, posiciona o Brasil em sintonia com normas internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. A legislação pátria, inspirada nesse modelo europeu, somou esforços para regulamentar o uso de dados no país. Desde a criação da GDPR, o Congresso Nacional empenhou-se em adaptar essas diretrizes à realidade brasileira, resultando na aprovação da LGPD. Contudo, a efetividade dessa lei, sobretudo no tratamento de dados sensíveis, como informações sobre saúde, religião, orientação sexual e outros aspectos pessoais, merece ser analisada em profundidade (Hawryliszyn et al., 2021).

O tratamento de dados sensíveis é regulado pelos artigos 11 a 13 da LGPD, que exigem medidas específicas e, em geral, o consentimento explícito do titular para a sua utilização. Esses dispositivos destacam a necessidade de práticas rigorosas para proteger a privacidade dos indivíduos. Casos concretos, como o vazamento de dados de pacientes do Sistema Único de Saúde (SUS) em 2020, evidenciam essas fragilidades. Nesse episódio, informações sigilosas de diagnósticos e tratamentos foram expostas online. Além disso, houve a divulgação indevida de dados de vacinação contra a COVID-19, comprometendo não apenas a privacidade dos cidadãos, mas também a confiança no sistema de gestão de dados em saúde pública.

Uma das questões centrais da LGPD é a diferenciação entre dados pessoais comuns e dados sensíveis, sendo estes últimos mais vulneráveis a prejuízos e discriminação em caso de exposição. Ademais, o presente ordenamento jurídico exige consentimento explícito do titular ou prevê exceções, como o cumprimento de obrigações legais ou emergências de saúde pública.

O marco legal supracitado implicou de maneira significativa na proteção de dados pessoais no Brasil. No entanto, sua efetividade depende da aplicação rigorosa

das normas e da conscientização de todos os envolvidos, incluindo organizações e indivíduos. A proteção da privacidade só será plenamente alcançada com o esforço coletivo em respeitar os direitos dos titulares e adotar práticas que assegurem a segurança das informações (Nunes et al., 2021).

O objetivo geral desta pesquisa concentra-se na análise os impactos dos vazamentos de dados sensíveis de usuários do SUS, com ênfase na aplicação da LGPD, considerando suas implicações legais, éticas e de segurança na proteção da privacidade dos cidadãos. Já os objetivos específicos foram:

- Identificar e descrever casos recentes de vazamento de dados sensíveis do SUS;
- Avaliar as medidas de proteção adotadas pelo SUS para evitar novos vazamentos;
- Propor recomendações para melhorar a segurança dos dados sensíveis no contexto do SUS.

A metodologia adotada na pesquisa, a qual explorou os impactos dos vazamentos de dados sensíveis de usuários do Sistema Único de Saúde (SUS) e a aplicação da Lei Geral de Proteção de Dados (LGPD), baseou-se em uma abordagem hipotético-dedutiva. Este método permitiu a formulação de hipóteses sobre o tema e seu teste por meio de uma revisão da literatura científica e de casos práticos. Ademais, a revisão bibliográfica serviu como ferramenta para consolidar e analisar o conhecimento existente, buscando compreender as relações entre os vazamentos de dados e a eficácia da aplicação da LGPD, contribuindo para uma visão mais abrangente e aprofundada do tema.

A escolha pela revisão bibliográfica justificou-se na necessidade de analisar as múltiplas perspectivas sobre a proteção de dados, especialmente no contexto da saúde pública, onde a privacidade dos cidadãos é de extrema relevância. Essa abordagem permitiu identificar lacunas no conhecimento, sintetizar informações e propor interpretações ou recomendações práticas para lidar com as fragilidades na proteção de dados sensíveis no SUS.

Além da revisão bibliográfica, a metodologia incluiu a análise de casos práticos envolvendo incidentes de vazamento de dados no SUS e em instituições parceiras. Foram examinadas circunstâncias específicas que levaram a essas falhas, as consequências para os indivíduos afetados e as medidas tomadas pelas autoridades competentes. Casos emblemáticos, como a exposição de dados de mais de 200

milhões de brasileiros no sistema e-SUS Notifica em, foram analisados para identificar padrões de vulnerabilidade e avaliar a eficácia das respostas às violações.

Após a coleta dos materiais, realizou-se leitura detalhada das fontes, com o objetivo de extrair informações relevantes para compreender os impactos dos vazamentos e as estratégias de mitigação. Esta análise englobou as tendências de pesquisa, os métodos utilizados e as conclusões alcançadas, além de examinar as limitações e possíveis vieses de cada estudo.

A inclusão de casos práticos desempenhou um papel essencial, pois forneceu exemplos concretos das dificuldades enfrentadas na aplicação da LGPD. Ao analisar incidentes de vazamento de dados, foi possível identificar falhas nos processos de tratamento de informações sensíveis e propor soluções práticas para melhorar a segurança e a eficácia da legislação. Esta combinação de revisão e análise permitiu a formulação de diretrizes preventivas e recomendações para evitar novos incidentes, contribuindo para um sistema de proteção de dados mais robusto e confiável no contexto do SUS.

2. A PROTEÇÃO DE DADOS NO BRASIL

Segundo Homci (2023), a evolução da proteção de dados no mundo reflete a crescente preocupação com a privacidade e segurança das informações pessoais em um cenário de desenvolvimento tecnológico e interconectividade global. Desde os primeiros registros de regulamentações até as leis modernas, a proteção de dados tornou-se um elemento essencial na salvaguarda dos direitos dos indivíduos frente ao uso massivo de informações digitais. Tal processo evolutivo, ao longo das décadas, resultou e diversos marcos legais, avanços tecnológicos e mudanças nas expectativas sociais em relação ao tratamento e armazenamento de dados pessoais.

As primeiras iniciativas de proteção de dados surgiram na década de 1970, período em que vários países começaram a adotar legislações específicas para regular o tratamento de informações pessoais. Pioneira, a Alemanha implementou em 1970 a primeira lei de proteção de dados no estado de Hesse, com o objetivo de regulamentar a coleta e o processamento de dados por parte de entidades governamentais e privadas. Essa legislação inspirou outros países europeus e sinalizou a necessidade de criar normas que abordassem a privacidade em um mundo cada vez mais informatizado. Com isso, a Europa consolidou-se como líder na criação de regulamentações nessa área (Homci, 2023).

Na década de 1980, houve uma ampliação significativa das legislações de proteção de dados, especialmente na Europa, onde os países começaram a implementar leis nacionais com base nos princípios fundamentais de privacidade e segurança. Em 1981, o Conselho da Europa adotou a Convenção para a Proteção das Pessoas em relação ao Tratamento Automatizado de Dados Pessoais, conhecida como Convenção 108, que foi o primeiro instrumento legal internacional vinculante sobre o tema. A convenção estabeleceu diretrizes que influenciaram diversos países, promovendo uma abordagem padronizada e estimulando o intercâmbio seguro de informações pessoais entre nações (Polettini, 2020).

Nos anos 1990, com a expansão da internet e o surgimento de novas tecnologias de informação e comunicação, houve um debate global sobre a proteção de dados. O crescimento da coleta e do compartilhamento de informações digitais trouxe à tona preocupações sobre o uso e a segurança dos dados pessoais. Em resposta, a União Europeia promulgou, em 1995, a Diretiva de Proteção de Dados (Diretiva 95/46/CE), estabelecendo normas abrangentes para garantir a privacidade dos cidadãos europeus. A diretiva exigia que os países membros implementassem legislações nacionais alinhadas com seus princípios, promovendo uma harmonização das práticas de proteção de dados no bloco europeu (Polettini, 2020).

No início dos anos 2000, com o aumento das atividades comerciais online e o avanço das redes sociais, as discussões sobre proteção de dados pessoais intensificaram-se em diversas partes do mundo. Empresas multinacionais passaram a coletar e armazenar grandes volumes de dados de usuários, o que gerou preocupações sobre o controle e o uso dessas informações. Em resposta, alguns países começaram a revisar suas leis, enquanto outros, como o Japão e o Canadá, adotaram novas regulamentações baseadas em princípios de proteção de dados. Este período marcou uma fase de transição, na qual o debate sobre privacidade digital passou a ter relevância global (Oliveira, 2022).

A partir de 2010, o fortalecimento da proteção de dados ganhou mais impulso, especialmente com o surgimento de escândalos envolvendo a violação da privacidade dos usuários em grandes plataformas digitais. O caso mais notório foi o escândalo da Cambridge Analytica, em 2018, que expôs o uso indevido de dados de milhões de usuários do Facebook para influenciar processos eleitorais. Esse e outros eventos semelhantes aumentaram a pressão pública e política para uma regulação mais rígida

e abrangente, levando à implementação de leis mais robustas em várias partes do mundo (Oliveira, 2022).

Em 2018, a União Europeia implementou o Regulamento Geral de Proteção de Dados (GDPR), uma das legislações mais rigorosas e abrangentes sobre privacidade e proteção de dados até o momento. O GDPR trouxe uma série de novos direitos para os cidadãos europeus, incluindo o direito ao esquecimento e o direito à portabilidade de dados, além de exigir que as empresas demonstrem conformidade com os princípios de privacidade por design e por padrão. Essa legislação serviu como modelo para muitos países, que adotaram ou revisaram suas próprias leis para refletir as novas exigências do GDPR (Verbicaro; Calandrini, 2022).

Na América Latina, o movimento em direção à proteção de dados pessoais também se intensificou nas últimas décadas, com países como Argentina, Uruguai e Brasil, implementando leis específicas para regulamentar o tratamento de informações pessoais. Em 2020, o Brasil implementou a Lei Geral de Proteção de Dados (LGPD), que seguiu os princípios do GDPR e buscou harmonizar a legislação nacional com as práticas internacionais. Esse avanço colocou o Brasil em um patamar comparável ao de países com leis modernas de proteção de dados, fortalecendo a privacidade dos cidadãos e a segurança jurídica no tratamento de dados (Verbicaro; Calandrini, 2022).

A LGPD representou um avanço significativo, pois trouxe um conjunto de normas específicas para proteger a privacidade dos brasileiros, estabelecendo regras claras sobre a coleta, o armazenamento e o uso de dados pessoais. Este regramento legal foi resultado de anos de discussões entre especialistas, juristas e representantes do setor público e privado, refletindo um esforço coletivo para criar uma legislação moderna e adaptada às demandas da sociedade digital (Efing; Britto, 2021).

Por outro lado, o panorama asiático também refletiu uma crescente adesão à regulamentação de proteção de dados, com países como a Coréia do Sul, Singapura e Índia adotando políticas e leis para assegurar a privacidade dos usuários. Em muitos casos, essas legislações foram influenciadas pelo GDPR e buscavam equilibrar o desenvolvimento econômico com a proteção dos direitos dos cidadãos. A Ásia emergiu como um importante polo de inovação e, paralelamente, enfrentou desafios consideráveis para proteger dados em um cenário de rápido crescimento tecnológico (Basan, 2021).

Atualmente, a proteção de dados é uma preocupação global, e o estabelecimento de normas e regulamentos internacionais está no centro das

discussões sobre privacidade e segurança digital. Organizações e governos buscam colaborar na criação de diretrizes que garantam a privacidade dos indivíduos sem prejudicar o fluxo de informações e o desenvolvimento econômico. Essa colaboração reflete o entendimento de que, em uma economia digitalizada e interconectada, a proteção de dados requer uma abordagem coordenada e o compromisso de todas as partes envolvidas (Basan, 2021).

Machado (2023), destaca que a evolução da proteção de dados no mundo é um processo dinâmico e contínuo, moldado pelas transformações tecnológicas e pelas crescentes demandas sociais por privacidade e segurança. A trajetória dessa evolução demonstra que a proteção de dados é uma questão complexa, que requer regulamentações adaptáveis e cooperação internacional para responder aos desafios impostos por um mundo cada vez mais digital e globalizado. A conscientização dos direitos de privacidade e a adaptação das legislações para acompanhar as inovações tecnológicas são passos essenciais para garantir a segurança e a integridade das informações pessoais em nível global.

Para Efing e Britto (2021), a proteção de dados no Brasil trata-se de um tema que ganhou relevância nos últimos anos, impulsionado pela necessidade de regulamentar o uso crescente de informações pessoais na atual digitalização massiva. Com o advento de tecnologias avançadas e o aumento das interações online, o país viu-se diante de novos desafios no que diz respeito à privacidade e à segurança das informações de seus cidadãos. Esse contexto tornou urgente a criação de uma estrutura legal robusta, capaz de garantir o respeito aos direitos dos indivíduos no tratamento de dados pessoais por empresas e organizações públicas e privadas.

Com efeito, a LGPD estabelece princípios e fundamentos para o tratamento de dados, visando assegurar a transparência e a segurança no manuseio de informações pessoais. Entre os princípios fundamentais, destacam-se a necessidade de consentimento do titular dos dados para seu tratamento, o direito à informação e o princípio da finalidade, que exige que os dados sejam coletados e utilizados exclusivamente para os fins declarados. Além disso, a lei assegura ao titular o direito de acessar, corrigir e excluir seus dados, conferindo maior controle sobre suas informações pessoais e promovendo uma relação de confiança entre consumidores e organizações (Oliveira, 2022).

A criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela fiscalização e regulamentação da LGPD, representou um importante

passo na implementação da legislação. A ANPD é encarregada de orientar empresas e instituições sobre as melhores práticas para o cumprimento da lei, além de ter a função de aplicar sanções em casos de descumprimento. Esse órgão atua como intermediário entre o poder público e a sociedade, promovendo a educação e a conscientização sobre a importância da privacidade e da proteção de dados, além de contribuir para a construção de um ambiente digital mais seguro (Leal, 2021)

A entrada em vigor da LGPD impactou diretamente o setor empresarial, exigindo que as organizações revisassem seus processos de coleta e tratamento de dados para se adequar às exigências legais. Muitas empresas precisaram implementar mudanças estruturais, adotando políticas internas de privacidade, sistemas de segurança digital e treinamentos para seus funcionários. Essa adequação gerou desafios e custos significativos, especialmente para pequenas e médias empresas, que enfrentaram dificuldades para atender aos requisitos da lei. Entretanto, a conformidade com a LGPD trouxe benefícios ao fortalecer a confiança dos consumidores e melhorar a imagem corporativa das empresas comprometidas com a proteção de dados (Verbicaro; Calandrini, 2022).

A proteção de dados no Brasil também reflete uma mudança cultural, na qual os cidadãos estão cada vez mais cientes de seus direitos em relação à privacidade. A LGPD estimulou um processo de conscientização coletiva, onde os brasileiros passaram a valorizar a transparência no uso de suas informações e a exigir responsabilidade das organizações. Essa transformação cultural foi reforçada por campanhas educativas e pela atuação da mídia, que ajudaram a informar a população sobre a importância da proteção de dados e as implicações de seu uso inadequado (Verbicaro; Calandrini, 2022).

A LGPD não é apenas uma regulamentação nacional; ela também conecta o Brasil ao cenário internacional de proteção de dados, facilitando a cooperação com outros países e a adesão a acordos globais de segurança digital. Com uma legislação alinhada a padrões internacionais, o Brasil torna-se mais atraente para investimentos estrangeiros, uma vez que empresas globais tendem a priorizar mercados que oferecem segurança jurídica em relação à privacidade. Além disso, a harmonização das normas de proteção de dados facilita o intercâmbio de informações entre o Brasil e outros países, promovendo uma economia digital integrada e segura (Basan; Júnior, 2020).

Os desafios da proteção de dados no Brasil, no entanto, permanecem presentes, especialmente diante do avanço acelerado das tecnologias de inteligência artificial, big data e internet das coisas. A adequação da LGPD a essas inovações tecnológicas é crucial para garantir que a legislação continue relevante e eficaz. O crescimento dessas tecnologias impõe novas demandas, uma vez que elas aumentam a capacidade de coleta e análise de dados, exigindo que o marco legal se adapte para proteger o direito à privacidade em um contexto de mudanças constantes (Basan; Júnior, 2020).

Com o advento da LGPD também houve implicações para o setor público, que precisou adaptar suas práticas de gestão de informações para garantir a conformidade com a legislação. Governos e instituições públicas passaram a ser responsabilizados pelo tratamento dos dados dos cidadãos, o que resultou na criação de políticas de segurança e no fortalecimento dos sistemas de proteção digital. Essa adequação é fundamental para que o setor público desempenhe suas funções com transparência e respeite os direitos dos indivíduos, evitando o uso inadequado ou abusivo de informações pessoais (Pinto; Soares, 2021).

Como bem define Porto e Silva (2021), a proteção de dados no Brasil avançou significativamente com a implementação da LGPD, que marcou um novo paradigma em relação à privacidade e à segurança digital no país. A lei, junto com a atuação da ANPD e a conscientização da população, contribuiu para o fortalecimento dos direitos dos cidadãos e para a construção de um ambiente digital mais seguro e ético. No entanto, o desafio de adaptar a legislação às inovações tecnológicas e garantir sua aplicação efetiva continua exigindo um esforço conjunto entre governo, setor privado e sociedade para consolidar uma cultura de proteção de dados e preservar a privacidade dos brasileiros em um mundo cada vez mais digital.

Por outro lado, é fundamental avaliar as práticas de segurança atualmente adotadas pelo SUS, identificando medidas eficazes e áreas que necessitem de melhorias. Tal abordagem não apenas fortalecerá a proteção de dados, mas também fomentará a criação de uma cultura institucional voltada à segurança das informações sensíveis.

Caldas et al., (2022), define que a proteção de dados no contexto das relações de consumo tornou-se um tema central com o aumento das transações digitais e a intensificação do uso de informações pessoais por parte das empresas. No ambiente contemporâneo, em que o comércio online e o marketing digital se expandem

rapidamente, as informações dos consumidores passaram a ser coletadas, armazenadas e analisadas em grande escala. Esse cenário exige uma atenção especial à proteção dos dados, uma vez que o uso inadequado dessas informações pode comprometer a privacidade dos indivíduos e afetar a confiança nas relações de consumo.

Outrossim, a LGPD foi implementada no Brasil com o objetivo de regulamentar o tratamento de dados pessoais e assegurar os direitos dos consumidores no que se refere à sua privacidade. Essa legislação estabelece diretrizes que obrigam as empresas a serem transparentes em relação à coleta e ao uso de dados, promovendo o direito dos consumidores de conhecer como suas informações são processadas e armazenadas. A LGPD procura, assim, equilibrar os interesses das empresas, que utilizam dados para melhorar sua estratégia de negócios, e os direitos dos consumidores, que buscam proteger sua privacidade (Caldas et al., 2022).

No âmbito das relações de consumo, a proteção de dados está intrinsecamente ligada à criação de um ambiente de confiança entre consumidores e empresas. Ao saber que suas informações são tratadas com responsabilidade, o consumidor tende a sentir-se mais seguro ao realizar transações e compartilhar dados pessoais. A adoção de políticas de privacidade rigorosas e o respeito às normas da LGPD por parte das empresas são elementos que ajudam a fortalecer essa relação de confiança, essencial para o sucesso do comércio digital e das interações comerciais no geral (Costa et al., 2021).

A transparência nas práticas de coleta e uso de dados é outro aspecto fundamental nas relações de consumo. A LGPD estabelece que os consumidores têm o direito de saber quais informações estão sendo coletadas, para quais finalidades e por quanto tempo serão armazenadas. Essa clareza é essencial para que o consumidor tome decisões informadas e tenha controle sobre o uso de seus dados. Com efeito, o respeito a esses direitos amplia a percepção de segurança e reduz os receios relacionados ao uso indevido de informações pessoais, incentivando um consumo mais consciente e seguro (Costa et al., 2021).

Além da transparência, o consentimento também é um dos pilares da proteção de dados nas relações de consumo. A LGPD exige que as empresas obtenham a autorização dos consumidores antes de coletar e utilizar suas informações pessoais, especialmente quando se trata de dados sensíveis, como informações sobre saúde ou orientação sexual. Esse consentimento informado representa uma garantia

adicional para o consumidor e impõe às empresas a responsabilidade de respeitar os limites estabelecidos, assegurando que os dados não sejam usados de forma abusiva ou para finalidades não autorizadas (Pinto; Soares, 2021).

A segurança dos dados é igualmente crucial para proteger as relações de consumo. Vazamentos de informações pessoais, por exemplo, podem gerar impactos profundos para os consumidores, que se tornam vulneráveis a fraudes e invasões de privacidade. A LGPD impõe a necessidade de medidas de segurança adequadas, como criptografia e políticas de restrição de acesso, para proteger os dados contra incidentes de segurança. A implementação dessas práticas aumenta a resiliência das empresas frente a ataques cibernéticos e contribui para preservar a integridade das informações dos consumidores (Verbicaro; Vieira, 2021).

As sanções previstas pela LGPD em casos de descumprimento das normas também desempenham um papel importante na proteção de dados nas relações de consumo. A lei prevê multas e outras penalidades para empresas que não estejam em conformidade com as diretrizes, o que incentiva o cumprimento das regras e a adoção de práticas responsáveis. Essas sanções visam proteger os consumidores de abusos e demonstram o comprometimento do Estado em zelar pelos direitos à privacidade e segurança das informações pessoais (Verbicaro; Vieira, 2021).

A proteção de dados nas relações de consumo também representa um diferencial competitivo para as empresas. Organizações que adotam políticas rigorosas de privacidade e cumprem a LGPD tendem a ser mais valorizadas pelos consumidores, que preferem interagir com marcas que demonstram respeito pela privacidade. Esse compromisso com a proteção de dados fortalece a imagem das empresas e pode influenciar positivamente a fidelidade dos clientes, tornando-se uma vantagem estratégica no mercado cada vez mais consciente da importância da segurança digital (Leal, 2021).

A confiança nas relações de consumo, assegurada pela proteção de dados, é essencial para o desenvolvimento sustentável do comércio digital. A privacidade dos consumidores deve ser preservada não apenas como uma exigência legal, mas como um valor ético que guia as interações comerciais. A proteção de dados contribui para a construção de um mercado mais justo, em que os consumidores podem realizar transações e compartilhar informações sem receio de exposição indevida ou invasão de privacidade, promovendo um ambiente de consumo mais saudável e responsável (Leal, 2021).

A LGPD surge como um marco na busca por equilíbrio entre os interesses comerciais e os direitos dos consumidores, promovendo uma cultura de respeito à privacidade. A implementação de políticas adequadas, a conscientização dos consumidores e o compromisso das empresas com a conformidade à legislação são passos fundamentais para consolidar um cenário de consumo seguro e ético, onde a privacidade dos dados pessoais é efetivamente garantida.

2.1. PRINCÍPIOS FUNDAMENTAIS

A Lei Geral de Proteção de Dados (LGPD) foi criada no Brasil com o propósito de estabelecer normas sobre a coleta, armazenamento e processamento de informações pessoais, assegurando que os direitos de privacidade dos indivíduos sejam respeitados. Dentro desse marco regulatório, os princípios fundamentais da LGPD desempenham um papel crucial, pois orientam as práticas que devem ser adotadas pelas organizações e norteiam o tratamento ético e seguro dos dados pessoais. Esses princípios não apenas delimitam as obrigações legais das empresas, mas também refletem valores sociais e éticos relacionados à privacidade e ao controle sobre informações pessoais (Alves; Souza, 2021).

Um dos princípios mais relevantes da LGPD é o da finalidade, que estabelece que os dados pessoais devem ser coletados e utilizados exclusivamente para propósitos específicos, legítimos e previamente informados ao titular. Esse princípio visa limitar o uso das informações a finalidades claras, evitando que os dados sejam aplicados para objetivos distintos daqueles inicialmente propostos. Essa diretriz assegura transparência no tratamento de dados, permitindo que os indivíduos tenham clareza sobre o propósito para o qual suas informações serão usadas e, assim, possam decidir conscientemente sobre autorizar ou não seu uso (Alves; Souza, 2021).

Outro princípio essencial é o da necessidade, que determina que a coleta de dados deve ser limitada ao mínimo necessário para cumprir com a finalidade informada. Esse princípio se alinha ao conceito de minimização de dados, segundo o qual as organizações devem evitar o acúmulo de informações pessoais irrelevantes ou excessivas. Dessa forma, o princípio da necessidade visa reduzir os riscos associados à exposição de dados e minimizar o potencial de vazamentos e uso indevido das informações pessoais, estabelecendo uma prática que busca equilibrar

a obtenção de dados com a proteção da privacidade do titular (Verbicaro; Calandrini, 2022).

Andréa et al., (2020), destaca que o livre acesso é um princípio que assegura aos titulares o direito de obter informações claras e completas sobre o tratamento dos seus dados. Esse princípio representa um avanço em relação ao direito de informação, garantindo que os indivíduos possam solicitar acesso aos seus dados e entender como estão sendo processados, armazenados e compartilhados. Ao promover a transparência, o princípio do livre acesso fortalece a confiança entre consumidores e empresas, pois os titulares dos dados têm a possibilidade de monitorar o uso de suas informações e solicitar correções ou exclusões caso identifiquem irregularidades.

O princípio da qualidade dos dados é igualmente importante na estrutura da LGPD, pois estabelece que as informações pessoais devem ser exatas, claras, relevantes e atualizadas. Esse princípio visa assegurar que os dados mantidos pelas organizações sejam adequados para o cumprimento de suas finalidades, evitando inconsistências e erros que possam prejudicar os titulares. A qualidade dos dados é fundamental para garantir que as informações utilizadas em processos de decisão, tanto empresariais quanto governamentais, sejam precisas e confiáveis, reduzindo riscos de discriminação e outras consequências negativas (Andréa et al., 2020).

Outro aspecto relevante é o princípio da transparência, que complementa os demais princípios ao assegurar que os titulares dos dados tenham plena ciência das práticas adotadas pelas organizações. Esse princípio determina que as políticas de privacidade e os termos de uso devem ser apresentados de forma clara e acessível, permitindo que o titular compreenda os detalhes do tratamento de seus dados. Ao adotar práticas de transparência, as organizações contribuem para a construção de um ambiente de confiança, onde os indivíduos sentem-se mais seguros em compartilhar suas informações pessoais (Andréa et al., 2020).

O princípio da segurança é um dos pilares da proteção de dados, determinando que as organizações devem adotar medidas técnicas e administrativas para garantir a integridade, confidencialidade e proteção dos dados pessoais. Esse princípio é fundamental para prevenir vazamentos de informações, acessos não autorizados e outras formas de uso indevido de dados pessoais. As empresas são responsabilizadas pela adoção de sistemas de segurança eficazes, o que envolve

desde a criptografia de dados até o treinamento de funcionários, visando reduzir vulnerabilidades e promover um ambiente digital mais seguro (Vieira, 2023).

A prevenção é outro princípio que orienta a LGPD, exigindo que as organizações tomem precauções proativas para evitar danos ao titular dos dados. Esse princípio incentiva a implementação de estratégias que antecipem possíveis riscos à privacidade e à segurança das informações, buscando prevenir incidentes antes que eles ocorram. A prevenção reflete uma postura de responsabilidade e respeito pelos direitos dos indivíduos, indo além da simples adequação legal e promovendo uma cultura organizacional focada na proteção dos dados desde a concepção dos processos (Vieira, 2023).

O princípio da não discriminação é especialmente importante na LGPD, pois impede que os dados pessoais sejam utilizados para práticas discriminatórias ou abusivas. Esse princípio reforça o compromisso com a igualdade e a justiça, determinando que o tratamento de dados não pode resultar em desvantagens ou em preconceitos para os titulares. Ao combater o uso discriminatório de informações, a LGPD promove uma sociedade mais inclusiva e protege os indivíduos contra abusos que poderiam prejudicar sua dignidade e seus direitos fundamentais (Gregori, 2020).

O princípio da responsabilização e prestação de contas, por sua vez, exige que as organizações demonstrem a conformidade com a LGPD e assumam a responsabilidade pelo tratamento dos dados pessoais. Esse princípio reforça a necessidade de uma cultura de compliance, onde as empresas e entidades públicas devem adotar práticas de governança e auditoria para comprovar o respeito à legislação. A responsabilização é essencial para garantir que o tratamento de dados seja feito de maneira ética e transparente, proporcionando aos titulares a segurança de que seus direitos estão sendo respeitados (Gregori, 2020).

Segundo Santos et al., (2021), esses princípios fundamentais da LGPD constituem um embasamento ético e legal que visa proteger a privacidade e os direitos dos indivíduos em um contexto de transformação digital. Ao implementar esses valores no tratamento de dados, a legislação brasileira busca equilibrar os interesses econômicos das empresas com os direitos fundamentais dos cidadãos, promovendo um ambiente mais seguro e confiável para a utilização das informações pessoais. A aplicação rigorosa desses princípios é essencial para consolidar a cultura de proteção de dados no Brasil, fortalecendo a confiança entre consumidores e organizações e promovendo um mercado digital ético e sustentável.

Com efeito, a Lei Geral de Proteção de Dados no Brasil representa um avanço significativo na regulamentação sobre o tratamento de informações pessoais, estabelecendo normas claras para a proteção da privacidade dos cidadãos. Sua análise técnica revela uma estrutura normativa detalhada que busca assegurar direitos fundamentais em um contexto de ampla digitalização e constante uso de dados. A lei visa harmonizar práticas de tratamento de informações com os direitos de privacidade, segurança e controle por parte dos indivíduos, proporcionando um arcabouço jurídico moderno e adaptado às demandas da sociedade contemporânea (Silva, 2021).

A LGPD introduz conceitos e terminologias específicas que fundamentam sua aplicação. Termos como "dados pessoais", "dados sensíveis" e "titular" são definidos para esclarecer o escopo da legislação. Dados pessoais abrangem qualquer informação que identifique ou possa identificar um indivíduo, enquanto dados sensíveis referem-se a informações relacionadas a aspectos como saúde, origem étnica, religião ou orientação sexual, que exigem um nível de proteção mais rigoroso. A definição de titular, por sua vez, reforça o direito de controle do indivíduo sobre suas próprias informações, um princípio fundamental da lei (Silva, 2021).

Para Valesi e Aoki (2021), a estrutura normativa da LGPD organiza o tratamento de dados em várias etapas, estabelecendo responsabilidades específicas para as organizações. A lei define o papel do controlador e do operador, sendo o controlador a entidade responsável por tomar decisões sobre o tratamento de dados e o operador aquele que realiza o processamento conforme as instruções do controlador. Essa distinção de papéis é essencial para delimitar responsabilidades e atribuir obrigações, garantindo que todas as etapas do processamento de dados ocorram de acordo com os requisitos legais.

Um aspecto relevante na análise técnica da LGPD é a questão do consentimento, que é considerado a base para o tratamento de dados. A lei exige que o titular seja informado de forma clara e inequívoca sobre as finalidades da coleta de suas informações, e que sua autorização seja dada livremente. O consentimento deve ser específico e explícito, especialmente em casos que envolvem dados sensíveis, garantindo que o titular compreenda os riscos e esteja ciente do uso que será feito de seus dados. Essa exigência reforça a transparência e o controle sobre as informações pessoais (Valesi; Aoki, 2021).

Além do consentimento, a LGPD também prevê outras bases legais para o tratamento de dados, permitindo a coleta e o processamento sem consentimento em situações específicas, como o cumprimento de obrigação legal, a execução de políticas públicas, ou para a proteção da vida e da integridade física. Essas exceções são cuidadosamente delimitadas para assegurar que o tratamento de dados ocorra somente quando absolutamente necessário e justificado, equilibrando a proteção à privacidade com o interesse público e as necessidades operacionais das organizações (Valesi; Aoki, 2021).

A segurança da informação é um ponto fundamental da LGPD, que obriga as empresas a adotarem medidas de proteção adequadas ao tipo e à quantidade de dados tratados. A legislação exige que as organizações implementem controles técnicos e administrativos para prevenir incidentes, vazamentos e acessos não autorizados. A segurança deve ser planejada de forma preventiva, considerando ameaças potenciais e buscando minimizar riscos ao máximo. A implementação de políticas de segurança robustas é, portanto, indispensável para o cumprimento dos requisitos estabelecidos pela LGPD (Korkmaz; Sacramento, 2021).

A atuação da Autoridade Nacional de Proteção de Dados (ANPD) é essencial na supervisão e regulamentação da LGPD, especialmente em sua dimensão técnica. Este órgão tem a responsabilidade de emitir orientações e diretrizes para o cumprimento da lei, além de monitorar e aplicar sanções em casos de infração. A ANPD exerce um papel educativo e punitivo, promovendo a conformidade e a proteção dos direitos dos titulares, bem como contribuindo para a construção de uma cultura de respeito à privacidade nas organizações e na sociedade em geral (Korkmaz; Sacramento, 2021).

Conforme define Basan (2021), a análise técnica da LGPD demonstra que a lei não é apenas uma regulamentação jurídica, mas também um instrumento que promove uma transformação cultural na forma como o tratamento de dados é realizado no Brasil. Ao estabelecer diretrizes e exigências para a coleta, armazenamento, processamento e segurança das informações pessoais, a LGPD reforça a importância da privacidade em uma era digital. Sua implementação requer um compromisso contínuo das organizações com a ética e a transparência, e sua aplicação eficaz depende de uma colaboração ativa entre o Estado, as empresas e a sociedade para proteger os direitos dos indivíduos e fortalecer a confiança no ambiente digital.

Segundo Moribe (2022), a Lei Geral de Proteção de Dados impõe um conjunto de obrigações para as empresas no Brasil, exigindo adaptações significativas em seus processos de coleta, tratamento e armazenamento de informações pessoais. A conformidade com a LGPD implica um esforço abrangente para incorporar práticas de proteção de dados em todas as esferas operacionais das organizações, desde a implementação de políticas de segurança até a criação de uma cultura de privacidade entre os colaboradores. Esse processo, entretanto, representa desafios complexos, especialmente para empresas que ainda não possuem uma estrutura consolidada de governança de dados.

Um dos principais obstáculos para o cumprimento da LGPD está na necessidade de reformulação dos sistemas de TI e das infraestruturas tecnológicas que manipulam informações pessoais. Muitas organizações precisam investir em tecnologias avançadas que garantam o armazenamento seguro e o acesso restrito aos dados, o que pode envolver altos custos iniciais. A necessidade de criptografia, autenticação reforçada e monitoramento constante são alguns dos requisitos técnicos fundamentais para garantir a segurança dos dados pessoais, mas que podem ser de difícil implementação, especialmente para pequenas e médias empresas com recursos limitados (Moribe, 2022).

A adequação à LGPD exige também uma revisão minuciosa dos fluxos de trabalho, com o objetivo de identificar quais dados pessoais são processados e para que finalidades. Ademais, as empresas devem mapear todo o ciclo de vida das informações, desde sua coleta até sua eventual eliminação, assegurando que todos os processos estejam em conformidade com os princípios da LGPD, como a finalidade, necessidade e transparência. Esse mapeamento demanda tempo e comprometimento das equipes, além de um conhecimento detalhado sobre as operações internas, o que representa um desafio organizacional significativo (Moribe, 2022).

Além dos ajustes estruturais e operacionais, a LGPD impõe a necessidade de capacitação dos colaboradores para a adequada compreensão e implementação dos conceitos de privacidade e proteção de dados. Os funcionários de diversos setores precisam estar conscientes de suas responsabilidades e das implicações legais do tratamento inadequado de dados pessoais. Essa conscientização e treinamento são fundamentais para minimizar riscos de erros humanos, mas representam um esforço

contínuo que requer recursos financeiros e tempo, além da criação de uma cultura interna de proteção de dados (Barcelos et al., 2021).

O papel do encarregado de proteção de dados, ou Data Protection Officer (DPO), é outra exigência da LGPD que representa um desafio para as empresas. A lei requer que as organizações nomeiem um responsável pela supervisão das práticas de proteção de dados, o que demanda um profissional com conhecimentos jurídicos e técnicos. A contratação de um DPO qualificado é uma necessidade, mas pode ser um desafio financeiro e logístico, especialmente para organizações que possuem estruturas mais enxutas. Em algumas situações, as empresas têm optado por terceirizar esse serviço, mas essa escolha pode envolver desafios relacionados à confiança e ao controle (Barcelos et al., 2021).

A conformidade com a LGPD implica também a implementação de políticas de segurança da informação rigorosas, que sejam capazes de prevenir vazamentos e acessos não autorizados. Com isso, as empresas precisam estabelecer normas e procedimentos internos que assegurem a proteção dos dados pessoais em todas as etapas do processamento. A criação de uma política de segurança eficaz requer planejamento e investimentos constantes em infraestrutura, além de uma fiscalização rigorosa para garantir que as normas sejam seguidas. Esse processo é desafiador e muitas vezes complexo, principalmente em ambientes corporativos que lidam com grandes volumes de informações (Cravo; Joelsons, 2020).

Outro desafio imposto pela LGPD é o de garantir a transparência e o livre acesso dos titulares aos seus dados pessoais. As empresas devem informar claramente aos indivíduos como suas informações estão sendo utilizadas, além de facilitar o acesso, correção e exclusão dos dados quando solicitado. Esse direito à transparência requer que as organizações estejam preparadas para responder rapidamente às solicitações dos titulares, o que pode demandar sistemas eficientes de atendimento e gestão de solicitações. A falta de um processo bem estruturado pode levar a complicações legais e ao desgaste da relação de confiança entre empresa e cliente (Cravo; Joelsons, 2020).

Vigliar (2022), destaca que a comunicação de incidentes de segurança também é uma exigência da LGPD que representa um grande desafio para as empresas. Em casos de vazamento ou acesso indevido, a organização é obrigada a notificar a Autoridade Nacional de Proteção de Dados (ANPD) e, em alguns casos, os próprios titulares dos dados afetados. Esse processo de notificação exige não apenas

transparência, mas também rapidez e clareza nas informações fornecidas. Empresas que não possuem uma estratégia de resposta a incidentes de segurança podem enfrentar dificuldades para cumprir essa exigência de maneira adequada e dentro dos prazos legais.

A conformidade com a LGPD impõe a necessidade de um sistema de auditoria contínua, garantindo que as práticas e políticas de proteção de dados estejam sempre atualizadas e em conformidade com a legislação vigente. As auditorias internas permitem que as empresas identifiquem possíveis vulnerabilidades e façam ajustes preventivos para evitar irregularidades e sanções. No entanto, a realização de auditorias regulares requer investimentos financeiros e a alocação de recursos humanos, tornando-se uma tarefa que exige planejamento estratégico e compromisso por parte da alta administração (Vigliar, 2022).

Ribeiro e Carvalho (2020), definem que a adequação à LGPD não se resume à implementação de medidas técnicas e jurídicas, mas requer uma transformação na cultura organizacional e um compromisso com a proteção da privacidade. Esse processo demanda esforço, investimentos e uma abordagem contínua de aprimoramento. Empresas que conseguem superar esses desafios e se adaptem à legislação são capazes de construir uma relação de confiança com seus clientes e fortalecer sua posição no mercado. A conformidade com a LGPD representa, assim, um diferencial competitivo e uma contribuição para a promoção de um ambiente digital mais ético e seguro.

3. VULNERABILIDADES NO SISTEMA ÚNICO DE SAÚDE (SUS) RELACIONADAS AO TRATAMENTO DE DADOS SENSÍVEIS

O Sistema Único de Saúde (SUS) desempenha um papel crucial no atendimento à saúde de milhões de brasileiros, gerenciando uma vasta quantidade de dados sensíveis que incluem informações pessoais e médicas dos usuários. Contudo, a crescente digitalização e o aumento do uso de tecnologias no setor público têm exposto o SUS a vulnerabilidades significativas no tratamento desses dados. Essas fragilidades, que envolvem aspectos tecnológicos e administrativos, tornam-se preocupações centrais em uma era onde a privacidade e a segurança da informação são cada vez mais valorizadas (Lemes, 2023).

Do ponto de vista tecnológico, o SUS apresenta uma infraestrutura muitas vezes defasada, com sistemas fragmentados e interoperabilidade limitada entre diferentes plataformas. Esse cenário dificulta a adoção de padrões modernos de segurança, como a criptografia avançada e a autenticação multifator, que poderiam proteger os dados armazenados e transmitidos. Além disso, a centralização de informações em bancos de dados acessados por múltiplas instituições aumenta o risco de vulnerabilidades, especialmente quando esses acessos não são monitorados adequadamente (Lemes, 2023).

As falhas administrativas também são notórias no contexto do SUS. A falta de treinamento adequado para os profissionais que lidam com dados sensíveis, aliada à ausência de protocolos claros para o manejo dessas informações, agrava o problema. Muitas vezes, os colaboradores não têm consciência dos riscos associados a práticas inadequadas, como o uso de senhas facilmente descobertas ou o compartilhamento não autorizado de informações, o que contribui para a exposição indevida de dados.

Os vazamentos de dados sensíveis representam riscos severos à privacidade dos indivíduos, com consequências que vão desde discriminação até a recusa de tratamento médico. No caso do SUS, que armazena dados de milhões de brasileiros, a exposição inadequada dessas informações pode ter impactos devastadores, incluindo a perda de confiança no sistema de saúde e a relutância dos cidadãos em fornecer dados precisos ou buscar atendimento por temores relacionados à privacidade.

A LGPD estabeleceu um marco na proteção de dados pessoais no Brasil, definindo diretrizes claras para o tratamento dessas informações. No entanto, sua efetividade ainda enfrenta desafios, especialmente em setores como o da saúde, onde o manejo frequente de dados sensíveis amplia os riscos.

Outrossim, casos emblemáticos de vazamento de informações sensíveis ilustram as consequências dessas fragilidades. Em 2020, uma falha no sistema e-SUS Notifica do Ministério da Saúde expôs dados pessoais e de saúde de mais de 200 milhões de brasileiros. O problema decorreu de configurações inadequadas de segurança, que deixaram informações críticas acessíveis na internet por meses (Aragão; Schiocchet, 2020). Este episódio não apenas revelou a fragilidade dos sistemas utilizados, mas também destacou a insuficiência de medidas preventivas e reativas por parte das autoridades.

Outro incidente significativo ocorreu em 2024, quando um ataque de ransomware à Change Healthcare, empresa que presta serviços ao SUS, resultou na exposição de mais de 100 milhões de registros de saúde. O caso evidenciou como a terceirização de serviços, sem mecanismos robustos de fiscalização e controle, pode ampliar os riscos de violação de dados. A falta de supervisão adequada sobre os fornecedores e parceiros também contribuiu para o agravamento deste caso. Os impactos desses vazamentos são amplos e multifacetados, atingindo não apenas os indivíduos cujas informações foram comprometidas, mas também as instituições responsáveis pela gestão dos dados. Do ponto de vista organizacional, episódios de violação de informações afetam a credibilidade das entidades envolvidas, dificultando a obtenção de financiamento e o desenvolvimento de parcerias estratégicas (Aragão; Schiocchet, 2020). A imagem institucional do SUS, enquanto provedor de saúde pública confiável, também sofre danos significativos.

Os episódios anteriormente citados evidenciam a necessidade urgente de reforçar a aplicação da LGPD no SUS, analisando as falhas nos mecanismos de proteção e investigando como a legislação pode ser aprimorada para atender melhor às demandas por segurança. Além disso, é essencial examinar as implicações jurídicas e éticas desses vazamentos, explorando as interpretações judiciais da LGPD e os precedentes que estão sendo estabelecidos.

No âmbito social, as consequências são ainda mais profundas. Os cidadãos que têm seus dados expostos enfrentam riscos como discriminação, estigmatização e fraudes financeiras. Além disso, a sensação de insegurança em relação à privacidade dos dados pode levar à relutância em fornecer informações precisas ou completas durante o atendimento médico. Essa dinâmica prejudica a coleta de dados confiáveis e impacta diretamente a qualidade dos serviços de saúde oferecidos. A confiança do cidadão no SUS é um elemento fundamental para o funcionamento eficiente do sistema de saúde pública. Contudo, essa confiança é fragilizada cada vez que um incidente de vazamento de dados ocorre (Macedo et al., 2020). A percepção de que as instituições públicas não são capazes de proteger informações sensíveis compromete o relacionamento entre o SUS e a população, criando um ciclo de desconfiança que pode ser difícil de reverter.

Para reverter essa situação, é necessário investir em tecnologias modernas e na atualização da infraestrutura digital do SUS. Isso inclui a implementação de sistemas mais seguros, o monitoramento contínuo de acessos e a adoção de medidas

proativas para prevenir vulnerabilidades. Além disso, a criação de protocolos rígidos e a realização de auditorias regulares são passos indispensáveis para garantir a integridade das informações armazenadas.

No plano administrativo, é essencial capacitar os profissionais que lidam com dados sensíveis, promovendo uma cultura organizacional voltada para a segurança da informação. Programas de treinamento e conscientização podem ajudar a reduzir comportamentos de risco e melhorar a adesão a boas práticas no manejo de informações (Macedo et al., 2020). A implementação de uma política de segurança robusta, com penalidades claras para violações, também pode atuar como fator dissuasório.

A relação entre fragilidades tecnológicas e administrativas destaca a necessidade de uma abordagem integrada para resolver os problemas de proteção de dados no SUS. Sem uma estratégia coordenada que aborde ambas as dimensões, qualquer esforço para mitigar os riscos estará incompleto. As lições aprendidas com incidentes passados devem servir como guia para evitar novas ocorrências e reforçar a segurança do sistema. Além disso, é crucial que o SUS fortaleça a fiscalização sobre empresas terceirizadas que manuseiam dados sensíveis. Isso envolve a exigência de padrões mínimos de segurança, o monitoramento das atividades realizadas por esses fornecedores e a responsabilização em caso de falhas. Contratos que contemplem cláusulas rigorosas de proteção de dados são essenciais para evitar lacunas na gestão de informações sensíveis (Rattes, 2020).

A aplicação da Lei Geral de Proteção de Dados no contexto do SUS é um recurso que pode contribuir para mitigar as vulnerabilidades identificadas. No entanto, a simples existência de uma legislação não é suficiente; é preciso garantir sua implementação efetiva, com mecanismos claros de fiscalização e sanção.

A Autoridade Nacional de Proteção de Dados (ANPD) tem um papel crucial no processo de mitigação de vazamento de dados, assegurando que as normas sejam cumpridas. O fortalecimento da proteção de dados no SUS não é apenas uma questão técnica, mas também ética e social. Garantir a segurança das informações sensíveis é fundamental para preservar a dignidade e os direitos dos cidadãos (Rattes, 2020). Ao investir na proteção dos dados, o SUS poderá reforçar a confiança da população, contribuindo para um sistema de saúde pública mais eficiente, seguro e confiável.

4. IMPLICAÇÕES ÉTICAS E JURÍDICAS DOS VAZAMENTOS DE DADOS SENSÍVEIS EM SAÚDE PÚBLICA

Os vazamentos de dados sensíveis em saúde pública representam uma questão de extrema relevância ética e jurídica, principalmente aos contextos em que a privacidade do indivíduo é essencial para a garantia de direitos fundamentais. A saúde, como área que lida diretamente com informações altamente confidenciais, demanda uma abordagem cuidadosa e rigorosa no tratamento dessas informações, a fim de assegurar a dignidade e a proteção dos cidadãos. O direito à privacidade, consagrado em legislações nacionais e internacionais, reforça a necessidade de mecanismos robustos para evitar a exposição indevida de dados, especialmente em sistemas públicos como o SUS (Furtado et al., 2022).

Em contextos de saúde pública, a proteção de dados pessoais assume um papel central para preservar a confiança dos cidadãos nas instituições. O respeito à privacidade desses dados não é apenas uma obrigação legal, mas um imperativo ético, visto que reflete o compromisso das instituições com os direitos dos indivíduos (Furtado et al., 2022).

Os vazamentos de dados em saúde pública acarretam consequências éticas significativas para as entidades responsáveis. O não cumprimento de padrões adequados de proteção de informações demonstra uma falha em honrar a relação de confiança estabelecida entre a instituição e os pacientes. Além disso, compromete princípios fundamentais, como a beneficência e a justiça, que orientam o trabalho nas áreas de saúde e administração pública (Furtado et al., 2022). Essa negligência pode impactar negativamente a percepção pública sobre o sistema de saúde, fragilizando sua credibilidade.

Do ponto de vista jurídico, os vazamentos de informações sensíveis configuram violações claras às legislações que regulamentam a proteção de dados. No Brasil, a Lei Geral de Proteção de Dados estabelece diretrizes rigorosas sobre o tratamento de informações pessoais, especialmente quando envolvem dados considerados sensíveis. O descumprimento dessas normas pode gerar penalidades administrativas, ações civis e, em casos extremos, responsabilidade criminal para os agentes envolvidos. Portanto, a legislação busca assegurar que as instituições implementem mecanismos de segurança adequados e adotem boas práticas de governança (Lima; Bandeira, 2024).

A responsabilidade das instituições envolvidas em vazamentos vai além do cumprimento das normas legais. Há uma expectativa social de que elas adotem uma postura proativa, tanto na prevenção de incidentes quanto na reparação de danos. Isso inclui a transparência na comunicação com os afetados, a implementação de medidas corretivas e a disponibilização de recursos para mitigar as consequências do vazamento. Por outro lado, a falha em atender essas expectativas pode amplificar os danos reputacionais, além de agravar as implicações jurídicas. Com efeito, os indivíduos afetados por vazamentos enfrentam um conjunto de desafios que variam de acordo com a gravidade da exposição de suas informações. Consequências como fraudes financeiras, uso indevido de dados para discriminação e prejuízos emocionais são comuns em situações desse tipo. A dificuldade de acessar mecanismos de reparação ou obter respostas adequadas das instituições responsáveis agrava ainda mais os impactos sobre as vítimas, gerando desconfiança e sentimentos de vulnerabilidade (Lima; Bandeira, 2024).

As implicações éticas dos vazamentos também se refletem nas relações interpessoais e sociais dos indivíduos prejudicados. A exposição de dados de saúde pode desencadear estigmatização, afetar oportunidades de emprego e comprometer relações familiares e profissionais. Tais danos, muitas vezes imensuráveis, evidenciam a importância de medidas preventivas e da responsabilização rigorosa das instituições. No que diz respeito à eficácia das sanções aplicadas em casos de vazamento, é necessário avaliar se as penalidades impostas têm um caráter educativo e dissuasório. Multas financeiras, embora necessárias, podem ser insuficientes para promover mudanças estruturais nas instituições responsáveis (Galvão et al., 2024). A imposição de obrigações específicas, como a revisão de políticas de segurança e a implementação de auditorias regulares, pode ter um impacto mais duradouro na melhoria da proteção de dados.

Decisões judiciais e regulatórias desempenham um papel crucial na definição de precedentes que orientam as práticas das instituições de saúde. Casos emblemáticos ajudam a estabelecer parâmetros para a interpretação das leis e a aplicação de sanções. Contudo, ainda há desafios relacionados à uniformidade e à celeridade desses processos, que muitas vezes não acompanham a urgência dos danos sofridos pelas vítimas. A ausência de medidas corretivas eficazes pode perpetuar a sensação de impunidade e fragilidade no sistema de proteção de dados. Em contraste, respostas rápidas e adequadas aos vazamentos podem contribuir para

restaurar a confiança do público nas instituições (Galvão et al., 2024). Isso reforça a necessidade de uma articulação eficiente entre as autoridades reguladoras, as entidades de saúde e o sistema judiciário.

Além das sanções, é fundamental promover uma cultura organizacional que priorize a segurança da informação e o respeito à privacidade dos cidadãos. Essa transformação requer investimentos em tecnologia, capacitação de profissionais e a adoção de princípios éticos que permeiem todas as atividades relacionadas ao tratamento de dados sensíveis. Os vazamentos em saúde pública também levantam questões sobre a responsabilidade compartilhada entre os diversos agentes envolvidos no tratamento de dados. Instituições públicas, empresas terceirizadas e fornecedores de tecnologia têm papéis complementares nesse ecossistema, e falhas em qualquer etapa do processo podem resultar em incidentes graves. Isso demanda maior supervisão e coordenação para garantir que todos os agentes cumpram suas responsabilidades de maneira eficaz (Gunther et al., 2020).

A regulação mais rigorosa das práticas de tratamento de dados sensíveis é um passo necessário, mas insuficiente. É imprescindível que as instituições desenvolvam estratégias preventivas que incluam a identificação precoce de vulnerabilidades e a mitigação de riscos potenciais. A prevenção de vazamentos deve ser vista como uma prioridade, e não como uma resposta reativa após a ocorrência de incidentes.

As implicações éticas e jurídicas dos vazamentos de dados sensíveis em saúde pública reforçam a necessidade de um compromisso conjunto entre os diferentes atores envolvidos. Apenas com esforços integrados será possível garantir a proteção dos direitos dos cidadãos e a construção de um sistema de saúde mais seguro e confiável (Gunther et al., 2020). A busca por soluções efetivas deve ser contínua, reconhecendo que a proteção da privacidade é fundamental para a dignidade e o bem-estar da população.

5. CONCLUSÃO

Em 2020, uma falha no sistema e-SUS Notifica, mantido pelo Ministério da Saúde do Brasil, resultou na exposição de dados pessoais de mais de 200 milhões de brasileiros. Essa vulnerabilidade decorreu da inserção inadvertida de credenciais de

acesso no código-fonte do site, permitindo que informações sensíveis ficassem acessíveis na internet por pelo menos seis meses. Entre os dados expostos, estavam informações pessoais de cidadãos cadastrados no Sistema Único de Saúde (SUS) e clientes de planos de saúde.

A exposição prolongada dessas informações evidenciou fragilidades significativas na segurança dos sistemas de saúde pública. A presença de credenciais no código-fonte indica falhas nos procedimentos de desenvolvimento e revisão de software, além de uma possível ausência de práticas robustas de segurança da informação. Tais lapsos comprometem a confidencialidade dos dados e expõem os cidadãos a riscos como fraudes e roubos de identidade.

Em 2024, a Change Healthcare, subsidiária da UnitedHealth, sofreu um ataque de ransomware que resultou no comprometimento de dados pessoais e de saúde de mais de 100 milhões de indivíduos. O ataque, atribuído ao grupo de ransomware ALPHV/BlackCat, destacou a vulnerabilidade de grandes empresas de tecnologia da saúde a ciberataques sofisticados. A invasão causou interrupções significativas nos serviços de processamento de reivindicações médicas e pagamentos, afetando a continuidade dos cuidados de saúde.

A análise destes incidentes revela padrões comuns de vulnerabilidade, incluindo a dependência de tecnologias obsoletas, práticas inadequadas de segurança cibernética e falta de treinamento adequado dos funcionários. No caso da Change Healthcare, a utilização de tecnologias obsoletas amplificou o impacto do ataque e dificultou os esforços de recuperação. Além disso, a ausência de autenticação multifator e a exploração de credenciais comprometidas facilitaram o acesso dos invasores aos sistemas.

As respostas institucionais a estas violações variaram em eficácia. No incidente do e-SUS Notifica, embora o problema tenha sido corrigido após a denúncia, a exposição prolongada dos dados sugere uma resposta inicial lenta e a falta de monitoramento contínuo da segurança dos sistemas. Para no caso da Change Healthcare, a empresa efetuou o pagamento de um resgate de US$ 22 milhões em Bitcoin para recuperar os dados, uma decisão controversa que levanta questões sobre a eficácia de ceder às demandas de criminosos cibernéticos.

Com base na análise desses casos destaca-se a necessidade urgente de fortalecer as medidas de segurança cibernética nas instituições de saúde. A implementação de autenticação multifator, a atualização de sistemas legados e a

realização de auditorias regulares são passos essenciais para mitigar riscos. Além disso, o treinamento contínuo dos funcionários em práticas de segurança da informação pode reduzir a probabilidade de erros humanos que comprometam a integridade dos dados.

A proteção de dados sensíveis no Sistema Único de Saúde (SUS) é uma necessidade urgente, considerando os riscos associados a vazamentos de informações pessoais e médicas. Para enfrentar esse desafio, é essencial adotar estratégias abrangentes que combinem soluções tecnológicas e administrativas. A implementação de medidas preventivas e corretivas robustas pode reduzir significativamente as vulnerabilidades, protegendo a privacidade dos usuários e fortalecendo a confiança no sistema público de saúde (Falcão et al., 2024).

Com efeito, uma das estratégias tecnológicas mais eficazes na proteção de dados sensíveis é o uso da criptografia. Essa técnica, que transforma informações legíveis em um formato inacessível sem a chave de decriptação, é fundamental para garantir a segurança dos dados tanto em repouso quanto em trânsito. Além disso, a autenticação multifator oferece uma camada adicional de proteção, exigindo que os usuários forneçam mais de uma forma de verificação para acessar sistemas que armazenam dados sensíveis (Falcão et al., 2024).

Os controles de acesso são outro componente essencial na proteção da informação no SUS. Restringir o acesso aos dados apenas a profissionais autorizados, com base em suas funções e responsabilidades, reduz significativamente o risco de exposição indevida. Além disso, o monitoramento contínuo de acessos e atividades nos sistemas de saúde permite identificar rapidamente possíveis anomalias e agir de forma preventiva contra ameaças. A realização de auditorias regulares nos sistemas de informação é indispensável para avaliar a eficácia das medidas de segurança implementadas. Tais procedimentos ajudam a identificar falhas e vulnerabilidades, permitindo a correção antes que possam ser exploradas. Além disso, as auditorias promovem a transparência e a responsabilidade, demonstrando o compromisso das instituições de saúde pública com a proteção dos dados dos cidadãos (Andrade et al., 2024).

Incidentes internacionais mostram como iniciativas bem-sucedidas podem ser adaptadas ao contexto brasileiro. No Reino Unido, o National Health Service (NHS) implementou uma série de medidas de segurança, incluindo a adoção de padrões avançados de criptografia e a realização de treinamentos regulares para seus

funcionários. Essas ações reduziram significativamente a ocorrência de vazamentos de dados e fortaleceram a confiança pública no sistema de saúde. No Brasil, algumas instituições públicas e privadas têm adotado boas práticas que poderiam servir de modelo para o SUS. A utilização de tecnologias baseadas em blockchain, por exemplo, tem sido explorada para registrar e proteger dados médicos de forma descentralizada e altamente segura (Andrade et al., 2024). Essa inovação tecnológica oferece um nível adicional de proteção contra acessos não autorizados e alterações indevidas nos registros.

Além das medidas tecnológicas, é essencial implementar estratégias administrativas que promovam uma cultura organizacional voltada à segurança da informação. Isso inclui a capacitação contínua de profissionais, garantindo que estejam cientes dos riscos associados ao manuseio inadequado de dados sensíveis e das práticas que devem ser seguidas para mitigá-los. A conscientização é uma ferramenta poderosa para reduzir comportamentos de risco no ambiente de trabalho. A criação de políticas claras e abrangentes de proteção de dados é outra medida fundamental. Essas políticas poderão estabelecer diretrizes específicas para o tratamento de informações sensíveis, incluindo procedimentos para coleta, armazenamento, compartilhamento e descarte seguro de dados. Além disso, devem prever sanções para o descumprimento das normas, reforçando a importância de sua aplicação (Brandão et al., 2024).

A seu modo, a liderança institucional desempenha um papel crucial na promoção da segurança da informação. Gestores e administradores devem liderar de forma exemplar, demonstrando compromisso com a proteção de dados e incentivando práticas seguras em todos os níveis da organização. A alocação de recursos financeiros e humanos para a implementação de medidas de segurança também é essencial para o sucesso das iniciativas. A integração entre diferentes sistemas de informação utilizados no SUS é um desafio que precisa ser abordado para melhorar a proteção dos dados. A interoperabilidade segura entre plataformas facilita o compartilhamento de informações essenciais sem comprometer a privacidade dos usuários (Brandão et al., 2024). Essa integração deve ser acompanhada por mecanismos de segurança robustos para evitar brechas.

Parcerias entre o SUS e empresas especializadas em segurança da informação podem acelerar a implementação de soluções inovadoras. Empresas de tecnologia têm experiência e recursos para desenvolver sistemas avançados de proteção, que

podem ser adaptados às necessidades específicas do sistema público de saúde. Essas colaborações devem ser baseadas em contratos claros que garantam a confidencialidade dos dados. Ademais, a transparência na comunicação com os cidadãos também é fundamental para fortalecer a confiança no SUS. Informar os usuários sobre as medidas de segurança adotadas, bem como sobre os direitos que possuem em relação ao tratamento de seus dados, cria um ambiente de maior transparência e respeito à privacidade. Essa prática é essencial para promover o engajamento e a colaboração do público (Labres et al., 2021).

A implementação de um sistema de governança em segurança da informação pode consolidar as iniciativas de proteção de dados no SUS. Esse sistema deve envolver a criação de comitês responsáveis por monitorar e avaliar continuamente as estratégias adotadas, garantindo sua atualização em face de novas ameaças e tecnologias emergentes. A governança eficaz assegura que a proteção dos dados seja um processo contínuo e dinâmico. A combinação de estratégias tecnológicas, administrativas e culturais é essencial para a proteção de dados sensíveis no SUS. A adoção de boas práticas e a incorporação de exemplos bem-sucedidos de outros contextos podem transformar o sistema público de saúde em um modelo de segurança da informação (Labres et al., 2021). Ao investir em medidas de proteção robustas, o SUS não apenas preserva a privacidade dos cidadãos, mas também fortalece a confiança e a eficiência de seus serviços.

A análise da proteção de dados sensíveis sob a ótica da Lei Geral de Proteção de Dados (LGPD), com foco em casos de vazamento no Sistema Único de Saúde (SUS), evidencia fragilidades significativas na gestão e segurança das informações pessoais. A exposição de dados, como nos episódios do e-SUS Notifica, em 2020, e outros incidentes similares, revela um cenário preocupante de insuficiência nas medidas preventivas e reativas implementadas. Esses casos destacam a necessidade de ações mais rigorosas e coordenadas para proteger as informações sensíveis de milhões de brasileiros.

A investigação demonstrou que, embora a LGPD represente um marco regulatório importante, sua aplicação prática enfrenta desafios substanciais. Lacunas na infraestrutura tecnológica, ausência de protocolos adequados e a falta de capacitação dos profissionais que lidam com esses dados são fatores que contribuem para a ocorrência de vazamentos. Além disso, a resposta tardia das autoridades em

algumas situações comprometeu ainda mais a confiança do público no sistema de saúde pública, ressaltando a importância de estratégias mais proativas.

Os impactos dos vazamentos vão além das consequências imediatas, como o uso indevido de informações pessoais. Eles afetam diretamente a relação de confiança entre os cidadãos e o SUS, prejudicando a adesão a programas de saúde e a coleta de dados precisos para o planejamento de políticas públicas. Além disso, as instituições responsáveis enfrentam danos reputacionais e riscos jurídicos que poderiam ser mitigados com uma governança de dados mais robusta.

A pesquisa também aponta a relevância de investir em tecnologias modernas, como criptografia avançada e autenticação multifator, além de promover uma cultura organizacional voltada para a segurança da informação. A implementação de auditorias regulares, políticas de transparência e capacitação contínua para os profissionais que manejam dados sensíveis são medidas essenciais para minimizar vulnerabilidades e garantir a proteção das informações pessoais.

Em suma, a proteção de dados sensíveis no SUS é um desafio que exige esforços conjuntos entre governo, instituições de saúde e sociedade. A adoção de práticas preventivas e a aplicação rigorosa da LGPD são cruciais para reverter o cenário atual e fortalecer a segurança da informação no Brasil. Somente com ações integradas e uma abordagem ética será possível preservar os direitos dos cidadãos e assegurar a confiabilidade do sistema de saúde pública.

REFERÊNCIAS

ALVES, Giselle Borges; SOUZA, Rodrigo Teixeira de. Comércio digital e proteção de dados: a era do Big Data. Revista da Defensoria Pública do Distrito Federal, v. 3, n. 1, 2021.

ANDRADE, Thael Rhian Alves et al. Responsabilidade culposa pelo vazamento de dados: a inteligência artificial como agravante no estelionato digital. Revista Filosofia Capital-ISSN 1982-6613, v. 20, n. 26, p. e548-e548, 2024.

ANDRÉA, Gianfranco Faggin Mastro et al. Proteção dos dados pessoais como direito fundamental: A evolução da tecnologia da informação e a lei geral de proteção de dados no Brasil. Revista de Direito Constitucional e Internacional, v. 121, p. 115-139, 2020.

ARAGÃO, Suéllyn Mattos; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do sistema único de saúde. Revista Eletrônica de Comunicação, Informação & Inovação em Saúde, v. 14, n. 3, 2020.

BARCELOS, Ana Karollina et al. A lei geral de proteção de dados e o papel do DPO. Revista Projetos Extensionistas, v. 1, n. 2, p. 87-92, 2021.

BASAN, Arthur Pinheiro. A Lei Geral de Proteção de Dados Pessoais e a tutela dos direitos fundamentais nas relações privadas. Revista Jurídica Eletrônica da UFPI, v. 8, n. 1, p. 9-36, 2021.

BASAN, Arthur Pinheiro. Publicidade digital e proteção de dados pessoais: o direito ao sossego. Editora Foco, 2021.

BASAN, Arthur Pinheiro; JÚNIOR, José Luis de Moura Faleiros. A proteção de dados pessoais e a concreção do direito ao sossego no mercado de consumo. Civilistica. com, v. 9, n. 3, p. 1-27, 2020.

BRANDÃO, Sonia Darque; DE FREITAS, João Paulo Bezerra; DIB, Rebeca Dantas. Regulação de dados pessoais na era digital e os desafios no setor público de saúde. REVISTA DELOS, v. 17, n. 62, p. e3203-e3203, 2024.

CALDAS, Roberto Correia da Silva Gomes et al. Análises preliminares sobre a responsabilidade civil na lei geral de proteção de dados pessoais. Administração de Empresas em Revista, v. 2, n. 28, p. 414-461, 2022.

COSTA, Paula Martins da Silva et al. A proteção nas relações de consumo decorrentes de uso de tecnologias disruptivas em moedas virtuais. Brazilian Journal of Development, v. 7, n. 2, p. 17613-17631, 2021.

CRAVO, Daniela Copetti; JOELSONS, Marcela. A importância do CDC no tratamento de dados pessoais de consumidores no contexto de pandemia e de vacatio legis da LGPD. Revista de Direito do Consumidor, v. 131, p. 111 - 145, 2020.

EFING, Antonio Carlos; BRITTO, Melina Carla de Souza. A reafirmação dos direitos do consumidor virtual brasileiro e a Lei Geral de Proteção de Dados. Argumenta Journal Law, Jacarezinho–PR, Brasil, n. 35, p. 93-121, 2021.

FALCÃO, Matheus Zuliane et al. POR UMA AGENDA DA SOCIEDADE CIVIL EM DADOS E SAÚDE. Angélica Baptista Silva Francisco José Aragão Pedroza Cunha, p. 205.

FURTADO, Isabela Crispim Brito et al. Ecossistemas digitais na saúde: transformações na pandemia e a implementação do Conecte SUS. Universidade Federal de Minas Gerais - UFMG, 2022.

GALVÃO, Heideivirlandia Leite et al. Incidentes de Segurança: Regulação e Prática de Vazamento de Dados Pessoais Frente à LGPD. ID on line. Revista de psicologia, v. 18, n. 72, p. 179-197, 2024.

GREGORI, Maria Stella. Os impactos da lei geral de proteção de dados pessoais na saúde suplementar. Revista de Direito do Consumidor, v. 127, n. 01, p. 171-196, 2020.

GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho; RODRIGUES, Luciano Ehlke. A Proteção e o Tratamento dos Dados Pessoais Sensíveis na Era Digital e o Direito à Privacidade: os limites da intervenção do Estado. Relações Internacionais no Mundo Atual, v. 2, n. 27, p. 25-41, 2020.

HAWRYLISZYN, Larissa Oliveira; COELHO, Natalia Gavioli Souza Campos; BARJA, Paulo Roxo. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): O DESAFIO DE SUA IMPLANTAÇÃO PARA A SAÚDE. **Revista Univap**, *[S. l.]*, v. 27, n. 54, 2021.

HOMCI, JANAINA VIEIRA. A proteção dos dados pessoais no consumo digital. Editora Thoth, 2023.

KORKMAZ, Maria Regina Rigolon; SACRAMENTO, Mariana. Direitos do titular de dados:: potencialidades e limites na Lei Geral de Proteção de Dados Pessoais. Revista Eletrônica da PGE-RJ, v. 4, n. 2, 2021.

LABRES, Bruno H.; GRÉGIO, André; SILVA, Fabiano. Análise Exploratória de Atributos Textuais em Bases de Dados para Identificação de Campos Sensíveis. In: Anais Estendidos do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. SBC, 2021. p. 98-109.

LEAL, José Geraldo Alves. A lei geral de proteção de dados e a banalização no uso de dados pessoais no meio empresarial. Ponto de Vista Jurídico, p. 63-79, 2021.

LEMES, Delwin. Lei Geral De Proteção De Dados Pessoais (LGPD): o setor público e vazamentos de dados pessoais. REVISTA EIXO, v. 12, n. 2, p. 109-118, 2023.

LIMA, Glenna Farias; DE OLIVEIRA BANDEIRA, Leonardo Silva. A (im) possibilidade do reconhecimento do dano presumido por vazamento de dados pessoais. Revista Contemporânea, v. 4, n. 10, p. e6145-e6145, 2024.

MACEDO, Crislaine Santos et al. Você já protege seus dados?. Caderno de Graduação-Ciências Exatas e Tecnológicas-UNIT-SERGIPE, v. 6, n. 1, p. 171-171, 2020.

MACHADO, Daniel Carlos. Contratos Eletrônicos de Consumo: Formação Válida e Proteção de Dados Pessoais. Editora Thoth, 2023.

MORIBE, Gabriela Tiemi. A proteção de dados pessoais na Secretaria Nacional do Consumidor (2019-2021). 2022. Tese de Doutorado.

NUNES, Caroline Castro; MA, Stephane; TEIXEIRA FILHO, Marcelo Silveira. Armazenamento Descentralizado no Sistema Único de Saúde Brasileiro (SUS) Usando Interplanetary File System (IPFS) e Blockchain. Revista de Direito, v. 13, n. 01, p. 01-25, 2021.

OLIVEIRA, Jordan Vinícius de. Vazamento de dados pessoais e responsabilização civil: compatibilidades e conflitos entre o Código de Defesa do Consumidor e a lei geral de proteção de dados. Revista Brasileira de Direito Civil, v. 31, n. 01, p. 17-17, 2022.

PINTO, Laryssa Carolyne Oliveira; SOARES, Douglas Verbicaro. A proteção de dados do consumidor no comércio eletrônico (e-commerce): análises da lei n. 13.709/2018 nas relações de consumo virtuais. Revista Ilustração, v. 2, n. 3, p. 7-24, 2021.

POLETTINI, Márcia Regina Negrisoli Fernandez. A LGPD e os impactos nas relações de consumo. Revista JurisFIB, v. 10, n. 2, 2020.

PORTO, Antônio José Maristrello; E SILVA, Maria Eduarda Vianna. Lei Geral de Proteção de Dados Pessoais: uma análise econômica sobre o seu regime de responsabilidade. Economic Analysis of Law Review, v. 12, n. 3, p. 283-300, 2021.

RATTES, ARISTEU. Lei Geral de Proteção de Dados-Lei 13.709/2018. TCC's Direito, p. 19-19, 2020.

RIBEIRO, Micaela Mayara; CARVALHO, Thomaz Jeferson. Lei Geral de Proteção de Dados: consequências jurídicas da violação da privacidade para obtenção de dados. X mostra interna de trabalhos de iniciação científica, v. 10, p. 1-4, 2020.

SANTOS, Camila Ferrão dos et al. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. Revista Eletrônica da PGE-RJ, v. 4, n. 3, 2021.

SILVA, Diogo Osmidio Reis da. A proteção de dados pessoais como direito fundamental autônomo. p. 17-36, 2021.

VALESI, Raquel; AOKI, Mayra Yakari. O direito à privacidade e à proteção de dados pessoais nas relações de consumo. Revista de Estudos Jurídicos UNA, v. 8, n. 1, p. 205-226, 2021.

VERBICARO, Dennis; CALANDRINI, Jorge. A proteção da confiança do consumidor e a base do legítimo interesse na Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). Revista de Direito do Consumidor, v. 139, n. 31, p. 78, 2022.

VERBICARO, Dennis; CALANDRINI, Jorge. Nudges na proteção de dados pessoais no ciberespaço: um empurrão para incentivar decisões racionais dos consumidores. Revista de Direito do Consumidor, São Paulo, v. 142, p. 185-214, 2022.

VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. Revista de Direito do Consumidor, v. 134, p. 195-226, 2021.

VIEIRA, Lucas. Conceito, objeto e autonomia do direito da proteção de dados pessoais. Revista de Direito e as Novas Tecnologias, São Paulo, v. 18, 2023.

VIGLIAR, José Marcelo Menezes. LGPD e a Proteção de Dados Pessoais na Sociedade em Rede: Dados de Crianças e Adolescentes na Internet; Tratamento de Proteção de Dados no Comércio Eletrônico. Editora Almedina Brasil, 2022.