INTERFACE TECNOLÓGICA

APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NOS SERVIÇOS DE SAÚDE

APPLICABILITY OF GENERAL DATA PROTECTION LAW IN HEALTH SERVICES

Guilherme Garcia – guilherme.garcia1@hotmail.com
Faculdade de Tecnologia de Catanduva – Catanduva – São Paulo – Brasil

Maisson da Silva Fernandes – maaisson@gmail.com
Faculdade de Tecnologia de Catanduva – Catanduva – São Paulo – Brasil

Liriane Soares de Araújo – lirianearaujo@hotmail.com
Faculdade de Tecnologia de Catanduva – Catanduva – São Paulo – Brasil

Ronaldo Rodrigues Martins – ronaldo.martins@fatec.sp.gov.br
Faculdade de Tecnologia de Catanduva – Catanduva – São Paulo - Brasil

DOI: 10.31510/infa.v22i1.2178
Data de submissão: 24/03/2025
Data do aceite: 26/06/2025
Data da publicação: 30/06/2025

RESUMO

Este estudo tem como objetivo avaliar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LGPD) nos serviços de saúde, investigando os princípios, desafios e benefícios dessa lei para a proteção dos dados dos pacientes. A pesquisa aborda a aplicação da LGPD nas instituições de saúde, tanto públicas quanto privadas, identificando as práticas adotadas para garantir a conformidade com a legislação e as lacunas existentes nesse processo. A metodologia utilizada é uma revisão de literatura, com análise de estudos publicados entre 2019 e 2024 sobre a gestão de dados pessoais no contexto da saúde. O estudo revela que, apesar dos avanços promovidos pela LGPD, a aplicação da lei enfrenta desafios significativos, como a adaptação das tecnologias e a capacitação dos profissionais de saúde. Conclui-se que a efetividade da LGPD depende de um esforço contínuo das instituições de saúde para garantir a segurança das informações sensíveis dos pacientes e, assim, fortalecer a confiança no sistema de saúde. Espera-se auxiliar instituições da área de saúde na aplicação da lei em questão, minimizando problemas na utilização da mesma.

Palavras-chave: LGPD, proteção de dados, serviços de saúde, privacidade, aplicação.

ABSTRACT

This study aims to evaluate the applicability of the General Data Protection Law (LGPD) in healthcare services, investigating the principles, challenges, and benefits of this legislation in protecting patient data. The research examines the implementation of the LGPD in both public

and private healthcare institutions, identifying the practices adopted to ensure compliance with the law and the gaps in this process. The methodology used is a literature review, analyzing studies published between 2019 and 2024 on the management of personal data in the healthcare context. The findings reveal that, despite the advances brought by the LGPD, its implementation faces significant challenges, such as technological adaptation and the training of healthcare professionals. It is concluded that the effectiveness of the LGPD depends on continuous efforts by healthcare institutions to ensure the security of sensitive patient information, thereby strengthening trust in the healthcare system. This study aims to assist healthcare institutions in implementing the law, minimizing issues related to its application.

Keywords: LGPD, personal data protection, health services, privacy, application.

1. INTRODUÇÃO

Nos últimos anos, a proteção de dados pessoais tornou-se uma questão central em diversas áreas, especialmente no setor da saúde, onde as informações tratadas são altamente sensíveis. A LGPD, sancionada em 2018, representa um marco importante na regulação da privacidade e segurança de dados no Brasil. Sua aplicabilidade tem gerado discussões sobre os impactos no tratamento das informações dos pacientes, especialmente considerando os desafios que surgem com o uso crescente de tecnologias digitais no setor da saúde. Nesse contexto, a gestão de dados pessoais, como histórico médico, exames e diagnósticos, se torna um ponto crítico, uma vez que a exposição inadequada dessas informações pode gerar sérios danos à privacidade dos indivíduos (Lima; Gonçalves; Costa, 2023).

O problema de pesquisa pode ser formulado pela seguinte pergunta: Como as empresas podem compreender melhor a LGPD para sua aplicação?, complementando com a questão: **Como a LGPD tem sido aplicada nos serviços de saúde, e quais são os principais desafios e benefícios dessa aplicação para a proteção dos dados pessoais dos pacientes?**

Sendo assim, o objetivo principal é apresentar os princípios, desafios e benefícios da LGPD na área de saúde, analisando as práticas adotadas pelas instituições para assegurar a conformidade com a lei e identificar as lacunas existentes.

A relevância deste estudo se destaca diante da crescente digitalização dos dados na área da saúde e da complexidade em garantir a privacidade dos pacientes. O impacto da LGPD é crucial para a segurança das informações sensíveis, mas sua aplicação ainda enfrenta obstáculos, como a adaptação das tecnologias e a capacitação dos profissionais da área.

2. A PROTEÇÃO AOS DADOS PESSOAIS NO BRASIL

No Brasil, a proteção de dados pessoais não é expressamente prevista na Constituição, sendo tratada de forma indireta em dispositivos relacionados à intimidade e privacidade. A proteção foi inicialmente fundamentada em normas gerais, como o direito à privacidade e ao habeas data, mas não havia uma legislação específica até a criação da LGPD. Além disso, o Código de Defesa do Consumidor (CDC) e outras leis, como o Marco Civil da Internet (MCI), abordam de forma fragmentada o tratamento de dados, com foco em áreas como cadastros de consumidores e segurança na internet (Nether, 2018).

A legislação brasileira evoluiu ao longo do tempo, com leis como a Lei de Acesso à Informação, o Código de Defesa do Consumidor, e a Lei do Cadastro Positivo. A promulgação da LGPD em 2018 preencheu a lacuna legislativa, estabelecendo normas claras sobre a coleta, uso e proteção de dados pessoais. A questão da privacidade ganhou destaque internacionalmente com casos de vazamento de dados, como o escândalo envolvendo o Facebook e a Cambridge Analytica (Mèlo, 2019).

A proteção à privacidade é garantida pela Constituição Federal de 1988, que, em seu artigo 5º, inciso X, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Esse dispositivo é uma das bases legais para a proteção dos dados pessoais, incluindo aqueles relacionados à saúde. No entanto, garantir a privacidade dos dados de saúde vai além da simples conformidade com a legislação. Como destaca Almeida e Soares (2022), proteger as informações de saúde também significa prevenir o uso indevido desses dados, na qual pode ser realizado por meio de implementação de políticas de segurança da informação, anonimização de dados, controle rigoroso de acesso e aplicação de penalidades em caso de violações. Isto é essencial para evitar discriminação e estigmatização de indivíduos em situação de vulnerabilidade, como pessoas com HIV ou doenças mentais.

A Organização das Nações Unidas (ONU), desde 2005, vem destacando a importância de uma estrutura analítica para o direito à saúde, enfatizando a necessidade de garantir a segurança e proteção de grupos vulneráveis. Nesse contexto, a Organização Mundial da Saúde (OMS) introduziu o conceito de e-Saúde, que se refere ao uso das Tecnologias da Informação e Comunicação (TICs) para mediar o atendimento e a gestão da saúde, incluindo a assistência ao paciente, pesquisa, educação, capacitação da força de trabalho e a monitoração de saúde. No Brasil, um exemplo claro de e-Saúde é o Cartão Nacional de Saúde, que integra o Sistema Único de Saúde (SUS). Esse sistema é uma extensão virtual dos dados pessoais dos pacientes,

funcionando como uma espécie de "avatar" digital que circula nas plataformas de saúde, permitindo o acesso e o compartilhamento de informações entre profissionais e instituições de saúde (Lima; Gonçalves; Costa, 2023).

Além do SUS, a rede privada de saúde no Brasil também adota medidas para garantir a segurança e a privacidade dos dados dos pacientes. A Agência Nacional de Saúde Suplementar (ANS) estabelece normas e padrões obrigatórios para a troca de informações entre operadoras de planos de saúde e prestadores de serviços, regulando o compartilhamento de dados sensíveis e exigindo medidas, como anonimização de dados por exemplo, com o objetivo de proteger a confidencialidade das informações dos pacientes. Essas medidas, embora essenciais, ainda carecem de uma abordagem mais integrada e eficaz para garantir que a privacidade seja respeitada em todas as etapas do processo de cuidado e gestão de saúde (Botelho; Camargo, 2021).

O MCI, sancionado em 2014, também foi fundamental ao tratar de questões como a privacidade e a necessidade de consentimento do usuário para o uso de seus dados. A criação da LGPD representou um marco legal importante para a efetiva proteção de dados no Brasil, com foco na segurança e direitos dos cidadãos no contexto digital (Bioni, 2019). Ele foi instituído pela Lei nº 12.965/2014, e teve como objetivo estabelecer princípios, direitos, garantias e responsabilidades para o uso da Internet no Brasil. A legislação buscou garantir a privacidade dos usuários, proteger os direitos humanos e assegurar a cidadania digital, além de regular a utilização comercial e governamental do ambiente virtual (Nether, 2018).

Com o aumento da presença de internautas no Brasil, surgiu a necessidade de regulamentação para lidar com questões como crimes cibernéticos, a proteção da privacidade e a segurança no ambiente virtual. Em resposta, o MCI foi criado para estabelecer uma estrutura legal que abordasse temas como a neutralidade da rede, a retenção de dados de conexão e a responsabilidade das plataformas online. A legislação garante que os direitos dos usuários fossem protegidos de forma clara e eficaz no contexto digital (Mèlo, 2019).

A aprovação do MCI não foi isenta de controvérsias, envolvendo debates sobre a regulação da Internet, a responsabilidade de provedores e o impacto nas liberdades dos usuários. No entanto, a lei trouxe maior clareza sobre a aplicação dos direitos constitucionais no ambiente virtual, especialmente no que diz respeito à privacidade e à proteção de dados pessoais. A legislação também introduziu a ideia de autodeterminação informacional, permitindo que os usuários tivessem mais controle sobre o uso de seus dados pessoais.

Apesar dos avanços trazidos pela Lei 12.965/2014, ainda existem questões em aberto, como os limites da invasão de privacidade, especialmente nas relações de trabalho. A legislação, por não ser capaz de antecipar todos os cenários que surgem no cotidiano, deixa lacunas que precisam ser ajustadas à medida que novas situações e desafios se apresentam. Isso demonstra a complexidade da regulação de um espaço virtual dinâmico e em evolução.

Por fim, o MCI representou um avanço significativo na proteção dos direitos dos usuários da Internet no Brasil, proporcionando um modelo alternativo de governança para a rede. No entanto, ainda há desafios a serem enfrentados, especialmente no que diz respeito à definição clara de responsabilidades e à aplicação de uma proteção de dados mais robusta. A legislação continua sendo um processo em desenvolvimento, refletindo a necessidade de adaptação constante às mudanças tecnológicas e sociais (Bioni, 2019).

Considerando todo esse contexto, pode-se perceber muitas leis, instituições e documentos que possuem o mesmo objetivo, que é garantir a proteção dos dados pessoais e a privacidade dos indivíduos, promovendo segurança jurídica e transparência no uso das informações sensíveis. Como exemplos, destacam-se a LGPD, que estabelece diretrizes claras sobre o tratamento de dados pessoais no Brasil, e o MCI, que regula o uso da internet e reforça os direitos dos usuários no ambiente digital.

3. A LEI GERAL DE PROTEÇÃO DE DADOS

A finalidade da LGPD é a tutela da privacidade, pois neste contexto dominado pelas tecnologias informativas, os riscos de invasão da esfera particular do indivíduo se acentuam, tornando a privacidade mais vulnerável a invasões indevidas e injustificadas (Bioni, 2019).

A questão da titularidade do direito à proteção de dados envolve as pessoas naturais como beneficiárias diretas dessa proteção. No entanto, conforme apontado por Mèlo (2019), outros entes, incluindo os despersonalizados, também têm direito à proteção dos seus dados. A LGPD aplica-se a qualquer operação de tratamento de dados, independentemente do meio ou localização, mas com critérios territoriais, ou seja, abrange operações realizadas no Brasil, ou quando os dados no Brasil são tratados fora do país (Mèlo, 2019).

A LGPD visa criar um sistema de proteção que envolve tanto o Estado quanto a sociedade civil, mas sua efetividade depende do grau de informação que os indivíduos possuem sobre os instrumentos disponíveis para proteger sua privacidade no mundo digital. A proteção prevista pela Lei reflete um direito fundamental, que é a privacidade, e está diretamente ligada à dignidade da pessoa, conforme a teoria de Nether (2018) afirma que a proteção de dados é o

direito mais expressivo da condição humana contemporânea, integrando os direitos fundamentais que sustentam a cidadania no novo milênio.

A eficácia territorial da LGPD, conforme Mèlo (2019), aplica-se a operações de tratamento de dados no Brasil, bem como a operações fora do país, desde que os dados tenham sido coletados no Brasil ou se referem a pessoas localizadas no território brasileiro. A LGPD foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que entrou em vigor em 2018, e possui jurisdição global, obrigando qualquer site que processe dados de cidadãos brasileiros a cumprir suas normas.

4. PROCEDIMENTOS METODOLÓGICOS

Este estudo consiste em uma pesquisa bibliográfica, que envolve uma revisão de literatura sobre a aplicabilidade da LGPD nos serviços de saúde. A pesquisa foi realizada a partir da consulta a livros, dissertações e artigos científicos selecionados por meio de buscas em bases de dados acadêmicas, como *Scientific Electronic Library Online* (SciELO), PubMed, Google Acadêmico, Portal de Periódicos da CAPES, entre outras fontes relevantes disponíveis online.

A revisão focou em estudos publicados entre 2019 e 2023, priorizando materiais que abordassem diretamente o impacto e a aplicação da LGPD no setor de saúde. Os idiomas selecionados para a busca foram o português e o inglês. Para localizar os artigos, foram utilizados os seguintes termos: “LGPD”, “serviços de saúde”, “proteção de dados pessoais”, além de seus sinônimos, a fim de ampliar os resultados pertinentes à temática. Os critérios de inclusão foram: estudos que tratassem da aplicação da LGPD nos serviços de saúde, discutindo a gestão de dados pessoais no contexto hospitalar, em clínicas e outros estabelecimentos de saúde.

5. RESULTADOS E DISCUSSÃO

É necessário compreender que o desenvolvimento de novas tecnologias, embora traga avanços significativos na medicina e no acesso à saúde, também acarreta a possibilidade de graves violações de privacidade. Tais problemas são amplificados pela natureza digital dos dados, que podem ser facilmente acessados, copiados e compartilhados sem o devido controle, gerando consequências potencialmente prejudiciais à dignidade e à segurança dos indivíduos (Aragão; Schiocchet, 2020).

A LGPD, sancionada em 2018, surge como uma resposta normativa fundamental a esses riscos. Ela estabelece diretrizes claras para o tratamento de dados pessoais, classificando os dados de saúde como sensíveis e exigindo proteção especial. Entre seus principais dispositivos estão a necessidade de consentimento do titular, a restrição ao uso econômico das informações e a imposição de medidas técnicas de segurança (Costa; Oliveira Rosa, 2021). Apesar disso, a efetivação da lei ainda enfrenta desafios estruturais — como a falta de capacitação dos profissionais e a ausência de políticas robustas de segurança da informação nas instituições.

Há um contraste importante entre os autores: enquanto Aragão e Schiocchet (2020) enfatizam os riscos inerentes à digitalização, Costa e Oliveira Rosa (2021) ressaltam a dificuldade de implementação das normas na prática. Essa diferença de foco revela uma lacuna relevante na literatura: faltam estudos que articulem os aspectos técnicos e normativos com a realidade institucional, considerando as limitações operacionais do setor público e privado.

Adicionalmente, a proteção da privacidade em saúde ainda carece de protagonismo nas políticas públicas. Um exemplo foi a 14ª Conferência Nacional de Saúde (2012), que não incorporou o tema nas diretrizes propostas. Iniciativas posteriores, como o Plano Nacional de Saúde (2016–2019) e a Política Nacional de Informação e Informática em Saúde (PNIIS), buscaram superar essas falhas por meio da criação de políticas de governança, capacitação profissional e reforço da fiscalização (Praça Neto; Gomes; Freitas, 2023), mas ainda enfrentam limitações práticas e estruturais.

Nesse contexto, autores como Martins et al. (2021) apontam que a construção de um sistema de saúde digital seguro e ético depende de uma abordagem integrada. Além da conformidade legal, é necessário promover uma cultura organizacional de proteção de dados, por meio de ações práticas como: (i) capacitação contínua dos profissionais, (ii) adoção de soluções tecnológicas com princípios de “privacy by design” e (iii) criação de estruturas internas de governança de dados.

Portanto, embora o Brasil tenha avançado com a LGPD e políticas setoriais, o enfrentamento dos riscos à privacidade na saúde exige mais que legislação. É preciso alinhar práticas institucionais, formação ética e participação social, garantindo que os direitos dos pacientes sejam preservados frente à crescente digitalização dos serviços de saúde.

5.1 Lei Geral de Proteção de Dados Aplicada à Saúde

O setor da saúde é um dos campos que mais lida com dados sensíveis, cuja violação pode resultar em danos significativos aos indivíduos. A LGPD específica claramente os tipos de informações que são tratadas nesse setor, como disposto no Art. 5º e Art. 11º, definindo dados relacionados à saúde, à vida sexual, genéticos ou biométricos como dados sensíveis. Portanto, qualquer entidade que manipule tais dados, como históricos médicos e produtos de cuidado à saúde, deve tratá-los com precauções especiais, dada a sua natureza sensível (Lima; Gonçalves; Costa, 2023).

Além dos dados diretamente relacionados à saúde, organizações de saúde também gerenciam informações como registros financeiros, seguros de saúde, resultados de exames e dados biométricos, o que torna essencial para essas entidades adequarem-se às exigências da LGPD. Um ponto relevante da LGPD diz respeito à relação com fornecedores terceirizados, como no caso da telemedicina, onde os dados sensíveis dos pacientes podem ser transferidos para outros países e acessados por profissionais de fora (Eroud; Bon Vecchio; Vecchio, 2022).

Outro aspecto complexo é o uso de dados sensíveis, uma vez que a LGPD exige que qualquer tratamento de dados seja realizado com o consentimento do titular. No entanto, no setor da saúde, muitas vezes os dados inicialmente coletados para uma finalidade específica podem ser necessários para outras aplicações, complicando a gestão do consentimento. A lei permite que o titular revogue seu consentimento a qualquer momento, o que exige que as organizações desenvolvam sistemas para garantir a revogação imediata e o cessar do tratamento dos dados (Botelho; Camargo, 2021).

A LGPD prevê algumas exceções em que dados sensíveis podem ser tratados sem o consentimento do titular, como no caso de procedimentos realizados por profissionais de saúde para tutelar a saúde do paciente, conforme o Art. 7º, inciso VIII. Em situações críticas de vida ou morte, dados sensíveis podem ser utilizados sem consentimento, desde que sejam indispensáveis para o tratamento. A lei também autoriza o tratamento sem consentimento para cumprir obrigações legais, realizar estudos de pesquisa, ou proteger a vida e a integridade física do titular ou de terceiros, como previsto nos incisos II, IV e VII do Art. 7º (Almeida; Soares, 2022).

Além disso, a Agência Nacional de Saúde Suplementar (ANS) regula casos específicos relacionados ao tratamento de dados sensíveis no setor de saúde. Ela pode estabelecer diretrizes para o tratamento de dados com foco em riscos para seguros de saúde, como doenças pré-existentes e tendências patológicas. Contudo, a LGPD exige a anonimização dos dados para

fins de pesquisa, excluindo a maioria das empresas de saúde suplementar que atuam com fins lucrativos e não com finalidades institucionais de pesquisa (Martins *et al*., 2021).

A questão do tratamento de dados sensíveis também envolve a proteção contra discriminação, como estabelecido no Art. 6º, inciso IX, da LGPD. Isso implica que as operadoras de planos de saúde não podem discriminar ou abusar de dados pessoais para fins de mensuração de riscos. Essa regulamentação pode impactar diretamente os modelos de negócios das operadoras de planos de saúde, especialmente no cálculo de contraprestações e na definição de coberturas, evitando discriminação abusiva (Costa; Rosa, 2021).

A LGPD também restringe o compartilhamento de dados sensíveis, proibindo sua comunicação entre controladores de dados com o intuito de obter vantagem econômica, exceto em situações de prestação de serviços de saúde. O compartilhamento é permitido, mas deve ocorrer com o consentimento do titular e estar de acordo com as autoridades competentes. O ponto de controvérsia recai sobre o significado da frase "obter vantagem econômica", o que pode gerar discussões sobre as intenções da lei e a aplicação de suas diretrizes, uma vez que a redação não é completamente clara (Praça Neto; Gomes; Freitas, 2023).

5.2 Garantia da Privacidade e Prevenção do Uso Indevido de Dados.

Para garantir essa privacidade e minimizar riscos, diversas estratégias podem ser adotadas como técnicas de criptografia, controle de acessos restritos e monitoramento contínuo. A governança de dados também é uma peça-chave para evitar o uso indevido de informações sensíveis, bem como, políticas institucionais bem definidas, treinamento contínuo dos profissionais de saúde e conscientização sobre a importância da proteção de dados são estratégias fundamentais para assegurar que as diretrizes de segurança sejam seguidas adequadamente (Lima; Gonçalves; Costa, 2023).

Sendo assim, a Segurança da Informação desempenha um papel essencial na proteção dos dados sensíveis na área da saúde, prevenindo acessos indevidos, vazamentos e usos não autorizados dessas informações. Para isso, medidas como controle de acesso baseado em níveis de permissão, criptografia de ponta a ponta e monitoramento contínuo de atividades devem ser implementadas para garantir a integridade e a confidencialidade dos dados dos pacientes (Martins *et al*., 2021). Além disso, a criação de planos de resposta a incidentes e auditorias regulares são fundamentais para mitigar riscos e assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD) (Lima; Gonçalves; Costa, 2023). Nesse contexto, investir na capacitação dos profissionais de saúde para a correta manipulação de informações digitais

torna-se indispensável, pois a segurança dos dados não depende apenas de tecnologia, mas também da conscientização e responsabilidade dos indivíduos envolvidos no tratamento dessas informações (Botelho; Camargo, 2021).

Além disso, a implementação de ferramentas que permitam a gestão de consentimento dos pacientes, garantindo que estes tenham controle sobre o uso de seus dados, é um passo essencial na conformidade com a LGPD (Hawryliszyn; Coelho; Barja, 2021). Exemplos dessas ferramentas são os Sistemas de Informação em Saúde, que desempenham um papel crucial ao organizar e armazenar dados de forma estruturada, viabilizando a interoperabilidade e a proteção da informação (Coelho Neto; Chioro, 2021). Para reforçar a segurança, esses sistemas incorporam mecanismos como, autenticação multifator, registros de auditoria e controle de acessos, elementos essenciais para minimizar riscos de violações de dados (Chaves; Miranda, 2023). Assim, a implementação dessas ferramentas não apenas protege as informações dos pacientes, mas também fortalece a governança digital na saúde, garantindo conformidade com a LGPD e promovendo maior confiança na gestão dos dados sensíveis.

Casos reais como o vazamento de informações do Cartão Nacional de Saúde já citado anteriormente, demonstram a urgência da aplicação de medidas rigorosas para evitar acessos indevidos. Diante desse cenário, instituições de saúde, tanto públicas quanto privadas, devem investir em um planejamento estratégico de segurança da informação, que inclua a adoção de auditorias regulares e a atualização constante de protocolos de proteção (Lima; Gonçalves; Costa, 2023).

Portanto, a privacidade e a segurança da informação no setor da saúde devem ser tratadas como prioridade, integrando boas práticas de governança, tecnologias de proteção e ações educacionais. A conformidade com a LGPD não apenas reduz riscos e penalidades legais, mas também fortalece a confiança dos pacientes e aprimora a qualidade dos serviços de saúde prestados.

6. CONCLUSÃO

O presente estudo buscou responder às seguintes questões: Como as empresas podem compreender melhor a LGPD para sua aplicação? e Como a LGPD tem sido aplicada nos serviços de saúde, e quais são os principais desafios e benefícios dessa aplicação para a proteção dos dados pessoais dos pacientes?

Considerando tais perguntas, a análise realizada ao longo deste trabalho permitiu concluir que a compreensão da LGPD pelas empresas exige a adoção de uma abordagem

estruturada, que inclui a implementação de políticas de governança de dados, investimentos em capacitação profissional e o uso de tecnologias de segurança. No setor da saúde, a aplicação da LGPD ainda enfrenta desafios significativos, como a necessidade de adequação tecnológica, a padronização de práticas de compartilhamento de informações e a conscientização dos profissionais sobre a importância da proteção dos dados pessoais. No entanto, os benefícios são claros: a LGPD contribui para maior transparência no uso das informações, reforça a segurança dos dados sensíveis e fortalece a confiança dos pacientes nas instituições de saúde.

Dessa forma, é possível compreender que a proteção de dados na área da saúde é um tema de grande relevância, exigindo esforços contínuos por parte das instituições para garantir conformidade com a legislação. Observou-se que a LGPD trouxe avanços importantes ao estabelecer diretrizes para o tratamento de dados pessoais, mas sua implementação ainda enfrenta desafios práticos, especialmente no que diz respeito à adaptação tecnológica e à capacitação dos profissionais.

A partir desta análise, percebe-se que a privacidade e a segurança dos dados são fundamentais para a construção de um ambiente digital confiável, em que tanto os profissionais quanto os pacientes possam ter segurança no armazenamento e no compartilhamento de informações. A adoção de boas práticas de segurança da informação, como criptografia, controle de acessos e auditorias regulares, mostrou-se essencial para assegurar a confidencialidade e a integridade dos dados no setor da saúde.

Por fim, este estudo reforça a importância da LGPD como um marco regulatório necessário para garantir a proteção dos dados pessoais e a privacidade dos cidadãos. A conformidade com a legislação não apenas reduz riscos jurídicos, mas também aprimora a gestão da informação e assegura a proteção dos direitos dos indivíduos. No entanto, o sucesso da aplicação da LGPD dependerá do compromisso contínuo das instituições de saúde em adotar medidas que promovam um tratamento de dados seguro, ético e eficiente.

REFERÊNCIAS

ALMEIDA, Siderly Carmo Dahle; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, p. 26-45, 2022. Disponível em: https://doi.org/10.1590/1981-5344/25905. Acesso em: 15 mar. 2025.

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. Disponível em: https://doi.org/10.29397/reciis.v14i3.2012. Acesso em: 15 mar. 2025.

BOTELHO, Marcos César; CAMARGO, Elimei Paleari. A aplicação da Lei Geral de Proteção de Dados na saúde. **Revista de Direito Sanitário**, v. 21, p. e0021-e0021, 2021. Disponível em: https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023. Acesso em: 15 mar. 2025.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**. Rio de Janeiro: Forense, Editora, 2019.

CHAVES, Midiã Marcelina Pereira; MIRANDA, João Luiz. Sistemas de Informação em Saúde: desafios encontrados durante a operacionalização e compartilhamento de dados. **Revista Eletrônica Acervo Saúde**, v. 23, n. 3, 2023. Disponível em: https://doi.org/10.25248/reas.e11712.2023. Acesso em: 16 mar. 25.

COSTA, Jeferson Morais; OLIVEIRA ROSA, Stefan. Lei Geral de Proteção de Dados Aplicada à Saúde. **Humanidades & Inovação**, v. 8, n. 45, p. 136-143, 2021. Disponível em: https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/4183. Acesso em: 15 mar. 2025.

COELHO NETO, Giliate Cardoso; CHIORO, Arthur. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil?. **Cadernos de Saúde Pública**. v. 37, n. 7, 2021. Disponível em: https://doi.org/10.1590/0102-311X00182119. Acessado em: 16 mar. 2025.

EROUD, Aicha Andrade; BON VECCHIO, Fabrizio; VECCHIO, Fabiana Guerra. O Consentimento da LGPD na Prestação de Serviços da Saúde. **Revista Percurso**, v. 1, n. 42, 2022. Disponível em: https://revista.unicuritiba.edu.br/index.php/percurso/article/download/6216/371374154. Acesso em: 15 mar. 2025.

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**, v. 27, n. 54, 2021. Disponível em: https://doi.org/10.18066/revistaunivap.v27i54.2589. Acesso em: 16 mar. 2025.

LIMA, Isadora Sousa; GONÇALVES, Jonas Rodrigo; COSTA, Danilo. A Lei Geral de Proteção de Dados Pessoais nos Serviços de Saúde Pública. **Revista Processus de Políticas Públicas e Desenvolvimento Social**, v. 5, n. 10, p. 58-78, 2023. Disponível em: https://doi.org/10.5281/zenodo.8367336. Acesso em: 15 mar. 2025.

MARTINS, Marcela; *et al*. A Aplicação da LGPD nos Hospitais Privados e o Direito Fundamental à Saúde e Proteção de Dados Pessoais. In: **VII Seminário Internacional de Direitos Humanos e Empresas**, p. 70, 2021. Disponível em: https://homacdhe.com/wp-content/uploads/2021/01/Anais-do-VII-Semin%C3%A1rio-Internacional.pdf#page=70. Acesso em: 15 mar. 2025.

MÈLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019.

NETHER, Nicholas Augustus Barcellos. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018.

PRAÇA NETO, Antonio Arão; GOMES, Thamires Gabriele Silva; FREITAS, Gisela Carvalho. Lei Geral de Proteção de Dados Pessoais: os impactos no setor de saúde. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 5, p. 3834-3846, 2023. Disponível em: https://doi.org/10.51891/rease.v9i5.10177. Acesso em: 15 mar. 2025.