Revista Processus de Políticas Públicas e Desenvolvimento Social, Ano 5, n.10, jul.-dez., 2023

(CC BY 4.0) | ISSN 2675-6595

DOI: 10.5281/zenodo.8367336

ARK: 69772/ppds.v5i10.1002

A Lei Geral de Proteção de Dados Pessoais nos Serviços de Saúde Pública[1]

The General Law for the Protection of Personal Data in Public Health Services

Recebido: 04/05/2023| Aceito: 16/19/2023| Publicado: 21/09/2023

Isadora Sousa Lima[2]
https://orcid.org/0009-0001-4275-2310
http://lattes.cnpq.br/0335942627052440
Centro Universitário Processus – UniProcessus, DF, Brasil
E-mail: isadora.isadorasousa.lima@gmail.com

Jonas Rodrigo Gonçalves[3]
https://orcid.org/0000-0003-4106-8071
http://lattes.cnpq.br/6904924103696696
Universidade Católica de Brasília, UCB, DF, Brasil
E-mail: professorjonas@gmail.com

Danilo da Costa[4]
https://orcid.org/0000-0003-1849-4945
http://lattes.cnpq.br/9522717317530051
Universidade Católica de Brasília, UCB, DF, Brasil
E-mail: educadordanilocosta@gmail.com

Resumo

O tema deste artigo é a aplicabilidade da LGPD nos serviços de saúde pública. Investigou o seguinte problema: Como a LGPD pode ser aplicada na coleta de dados nos serviços de saúde pública? Cogitou a hipótese de que o consentimento e a atualização de sistemas de cadastramento seria o meio para garantir a efetividade da LGPD. O objetivo geral é descrever a aplicação da LGPD na coleta de dados. Os objetivos específicos são explicar a relação da LGPD e a saúde, identificar como é feita a coleta de dados e analisar as possíveis mudanças para o cumprimento da Lei. Este trabalho é importante para o operador do Direito devido ao papel desempenhado na compreensão e aplicação das normas da LGPD; para a ciência, pois os dados pessoais são essenciais para a pesquisa científica; agrega à sociedade considerando que milhões de brasileiros fazem uso dos sistemas públicos de saúde. Trata-se de uma pesquisa qualitativa teórica com duração de seis meses.

Palavras-chave: LGPD. Saúde Pública. Aplicabilidade.

[1] Este trabalho foi revisado linguisticamente por Roberta dos Anjos Matos Resende.
[2] Graduanda em Direito pelo Centro Universitário Processus - UniProcessus
[3] Doutor em Psicologia; Mestre em Direitos Humanos (Ciência Política e Políticas Públicas); licenciado em Filosofia, em Sociologia e em Letras (Português e Inglês); Especialista em Direito Constitucional e Processo Constitucional, em Direito Administrativo, em Direito do Trabalho e Processo Trabalhista, entre outras especializações em Educação e Letras. Professor e Pesquisador do UniProcessus (DF) e da Facesa (GO).
[4] Doutorando em Educação; Mestre em Educação. Especialista em Direito Constitucional e Processo Constitucional, em Direito do Trabalho e Processo Trabalhista, e em Direito Administrativo. Licenciado em Geografia.

Abstract
The theme of this article is the applicability of LGPD in public health services. The problem was investigated: How can the LGPD be applied in data collection in public health services? The hypothesis was considered that consent and the updating of registration systems would be the means of guaranteeing the effectiveness of the LGPD. The general objective is to describe the application of the LGPD in data collection. The specific objectives are to explain the relationship between the LGPD and health, identify how data is collected and analyze possible changes to comply with the Law. This work is important for the legal operator due to the role played in terms of understanding and applying the LGPD rules; for science, as personal data is essential for scientific research; adds to society considering that millions of Brazilians make use of public health systems. This is theoretical qualitative research lasting six months.

Keywords: *LGPD. Public health. Applicability*

Introdução

Este estudo se propõe a analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) nos Procedimentos de Coleta de Dados nos Serviços de Saúde Pública. Delimita-se a relação desta lei com a rede de saúde pública em decorrência da utilização de dados sensíveis para o tratamento dos pacientes, de forma que seja criada a relação entre a LGPD (BRASIL, 2018) e a rede pública de saúde.

A *internet,* cada vez mais, acumula todos os tipos de dados pessoais de indivíduos, que inclusive influenciam o cenário econômico e cultural da sociedade. Desta forma, foram necessários estudos sobre a regulamentação da utilização desses dados, garantindo a privacidade dos usuários. Assim, em 14 de agosto de 2018, foi sancionada a Lei n.° 13.709, também chamada de Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Portanto, este artigo se propõe a responder o seguinte problema: Como a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) pode ser aplicada nos serviços de saúde pública? A partir disso, poderá ser analisada de que forma pode ser feita a adequação de tarefas para o total cumprimento do normativo, garantindo ainda a privacidade dos pacientes.

Diante disso, e tratando de todos os meios tecnológicos utilizados pela sociedade em diversas atividades, inclusive na melhoria de tarefas nos serviços de atendimento ao público, visualiza-se a íntima relação entre a proteção de dados pessoais e a população brasileira que usa os mais diversos serviços públicos. Desta forma, a LGPD (BRASIL, 2018) busca a proteção de todos, que possuem informações tratadas por sistema de coletas de dados (LEME; BLANK, 2020, p. 03).

O consentimento é um dos elementos principais na segurança dos dados. Portanto, a hipótese levantada frente ao problema em questão parte do princípio de que a criação de formulários de consentimento disponíveis ao usuário dos serviços de saúde no momento da triagem, bem como a atualização ou a criação de sistemas seguros de cadastramento de dados com a devida capacitação dos servidores, seria o meio para garantir a efetiva aplicação da LGPD (BRASIL, 2018) na rede de saúde pública.

Nessa linha, conforme Faleiros Júnior (2021) a melhor opção para o tratamento de dados considerados sensíveis será, por vezes, o consentimento. Nesse sentido, o capítulo II da Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) traz a necessidade de consentimento do paciente ou seu responsável legal, para que a

unidade de saúde faça a captação de dados para o tratamento do paciente (BARJA; COELHO; HAWRYLISZYN, 2021, p.06).

O objetivo geral do trabalho é descrever como a LGPD pode ser aplicada nos serviços de saúde pública. Com isso, pensando mais especificamente na coleta de dados para a triagem dos pacientes, será possível delimitar a atuação dos serviços públicos em observância da lei e dos fluxos que devem passar por adaptações para garantir a proteção ao usuário.

Vale ressaltar que os dados relacionados com a saúde são classificados como dados sensíveis, que implicam inclusive na continuidade do tratamento do paciente. Considerando que diversos dados sensíveis são coletados para o atendimento, estes devem ser tratados com extrema cautela e com a total garantia de sua privacidade (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Em decorrência do objetivo geral acima mencionado, são estabelecidos os seguintes objetivos específicos: explicar a LGPD e sua ligação com a saúde pública; identificar como é feita a captação de dados nos serviços de saúde pública; analisar quais mudanças devem ser feitas nestes serviços para que haja o efetivo cumprimento da lei. Tais objetivos serão atingidos com a caracterização da Lei, o entendimento de sua relação com a saúde pública, bem como a análise da coleta de dados de pacientes. Ainda foram verificadas as possíveis alterações que devem ser feitas nos sistemas de captação de dados para que haja o efetivo cumprimento da Lei.

Desta forma, resta evidente a necessidade de analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) nos serviços de saúde pública. Foi identificada a necessidade de análise da adequação da Lei aos serviços de saúde, uma vez que as normas que garantiam a segurança do paciente, agora serão aplicadas em conjunto com a nova legislação (BARJA; COELHO; HAWRYLISZYN, 2021, p.05).

Diante do exposto, verifica-se a relevância do tema para os profissionais da área do Direito, considerando que a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) tem sido cada vez mais utilizada, em decorrência inclusive do avanço tecnológico e da crescente utilização de sistemas de informações nos procedimentos de trabalho no Governo Federal. Os profissionais do Direito desempenham um papel fundamental na compreensão e na aplicação dessas normas nos serviços de saúde, e devem estar familiarizados com os princípios da lei, como o Princípio da Finalidade. Além disso, tais profissionais precisam entender as bases legais para o tratamento de dados pessoais na área da saúde, como o consentimento do titular. Eles devem orientar as instituições de saúde sobre como obter o consentimento adequado dos pacientes e como garantir a segurança e a confidencialidade dos dados coletados. Portanto, é fundamental que os profissionais do direito estejam atualizados e capacitados para orientar os serviços de saúde na aplicação correta da Lei.

Ressalta-se ainda a relevância da presente pesquisa para a ciência, pois a coleta e o uso de dados pessoais são essenciais para a pesquisa científica na área da saúde, permitindo avanços significativos no diagnóstico, no tratamento e na prevenção de doenças. É fundamental que essa coleta seja realizada de maneira ética e em conformidade com as normas de proteção de dados.

Em tempo, registra-se a importância do estudo para a sociedade como um todo, visto que a proteção dos dados pessoais é um tema crucial na era digital, na qual a quantidade de informações coletadas e armazenadas cresce cada vez mais. Nesse contexto, considerando ainda que milhões de brasileiros usam os sistemas públicos de saúde, a LGPD (BRASIL, 2018) desempenha um papel fundamental na garantia da privacidade e da segurança dos dados dos indivíduos, assegurando que

suas informações pessoais sejam tratadas de acordo com os princípios estabelecidos pela lei, trazendo benefícios significativos para a sociedade.

Trata-se de uma pesquisa teórica, bibliográfica, fundamentada em artigos científicos e livros acadêmicos, além da análise de lei e de demais normativos vigentes acerca do tema proposto. Com isso, para alcançar os objetivos propostos neste artigo foi realizada uma pesquisa de cunho básico e estratégico, e objetivos descritivos e exploratórios.

Foram selecionados cinco artigos científicos, após buscas realizadas no Google Acadêmico utilizando as seguintes palavras-chave: “LGPD, saúde pública, aplicabilidade”. Além disso, foi utilizada como base a Lei n.° 13.709 de 14 de agosto de 2018, chamada de Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) que aborda a proteção de dados pessoais e a criação da Autoridade Nacional de Proteção de Dados. Na elaboração do desenvolvimento foi verificada a necessidade de inserir ideias de outros autores, de modo a enriquecer a pesquisa, e portanto, os artigos, livros, a legislação e as notícias utilizadas foram essenciais para a fundamentação deste artigo.

Foram determinados alguns critérios de exclusão dos artigos científicos, a partir da seguinte ideia: foram selecionados artigos com até três autores, nos quais pelo menos um seja mestre ou doutor, sendo necessária a publicação do artigo em revista acadêmica com ISSN ou livro com ISBN. O tempo previsto desta pesquisa de revisão de literatura foi de três meses. No primeiro mês foi efetuado o levantamento do referencial teórico, no segundo mês foi realizada a revisão da literatura, e por fim, no último mês, foi feita a elaboração de elementos pré-textuais e pós-textuais que compõem toda a pesquisa.

Foi realizada uma pesquisa qualitativa, caracterizada pela coleta de informações a partir da referência bibliográfica de artigos científicos e/ou livros em que os autores trataram do assunto com a análise dos dados gerados a partir da pesquisa bibliográfica. Foram considerados os aspectos pertinentes levantados pelos autores, de modo a sustentar ou contrapor a hipótese levantada para entender a profundidade do tema.

Nesse sentido, sendo este um artigo de revisão de literatura, a base instrumental utilizada é formada por artigos publicados em revistas com ISSN ou livro com ISBN. Parte-se da pesquisa das palavras-chave que formam a base da busca dos artigos estudados conforme o tema proposto, realizando uma espécie de triagem, selecionando apenas os periódicos e as publicações relativas ao tema (GONÇALVES, 2020, p.98).

A Lei Geral de Proteção de Dados Pessoais nos Serviços de Saúde Pública

As discussões sobre a proteção dos dados pessoais se intensificaram com a crescente utilização de meios tecnológicos nas tarefas diárias e o alcance da *internet* para a transmissão de informações, notícias e outras formas de comunicação. Assim, em 2018 foi criado o Regimento Geral de Proteção de Dados (RGPD) pela União Europeia.

Tal Regimento seria o marco inicial da busca pela proteção de dados pessoais na Europa. Tais estudos, posteriormente, são difundidos para todo o mundo gerando uma série de normas para a proteção dos dados. Contudo, considera-se que o RGPD possui um amplo conjunto de normas em comparação ao normativo brasileiro vigente (ARAGÃO; SCHIOCCHET, 2012, p. 05).

O Brasil não contava com uma legislação específica para essa matéria. Contudo, há a existência da Lei n.° 12.737/2012 (BRASIL, 2012), também chamada

de Lei Carolina Dieckmann em combate aos crimes virtuais, em decorrência do roubo de fotos íntimas da atriz brasileira Carolina Dieckmann. Com isso, houve a alteração do Código Penal para tipificar a conduta do uso ilícito de dados, imagens ou vídeos de uma pessoa sem o seu consentimento.

Em abril de 2014 foi sancionado o Marco Civil da *internet*, Lei n.° 12.965/14 (BRASIL, 2014). Esta Lei buscou a regulamentação da utilização da *internet* no Brasil, estabelecendo o princípio da proteção da privacidade e dos dados pessoais, além de assegurar os direitos do usuário da *internet* como a inviolabilidade e sigilo de comunicações privadas.

Nessa linha, e com base no Regimento Geral de Proteção de Dados da União Europeia, em agosto de 2018 foi sancionada a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.° 13.709/18 (BRASIL, 2018), que conforme seu artigo 1°, visa o tratamento de dados pessoais buscando a proteção de direitos fundamentais de pessoa natural. Além disso, se aplica a entes públicos e privados, compreendendo assim todo o manejo de dados pessoais no Brasil.

Os dados pessoais podem ser conceituados como informações relacionadas a toda pessoa natural, conforme predispõe o artigo 5° da Lei ao elencar pessoa identificada ou identificável. A partir disso, surge a classificação de dados pessoais sensíveis, que possuem íntima relação com o seu titular em razão do seu alto poder discriminatório.

Desta forma, a LGPD (BRASIL, 2018) traz uma proteção ainda maior aos dados sensíveis, por sua intrínseca ligação com a personalidade do indivíduo, dados sobre religião, filiação, dado genético ou biométrico, ou de saúde e vida sexual. Contudo, os dados pessoais são determinados também quanto a sua forma de utilização e o propósito aplicado por meio de seu tratamento (LEME; BLANK, 2020, p. 04).

Assim, fica demonstrada a relevância da LGPD (BRASIL, 2018) no tratamento dos dados pessoais sensíveis que devem passar por um procedimento seguro que garanta os direitos do sujeito. Uma vez violados, os dados sensíveis podem gerar uma série de ofensas, como para a privacidade do indivíduo, gerando lesão a sua honra e dignidade (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Em tempo, identifica-se uma importante atuação do setor público quanto ao tratamento de dados pessoais sensíveis. A Administração Pública possui uma gama de dados captados, motivo pelo qual a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) define regras de controle e regulação garantindo assim a sua eficácia.

Portanto, mesmo um dado considerado comum ou sem relevância, quando transformado em um dado sensível com a utilização de tecnologias, é capaz de gerar grandes impactos na garantia de direitos estabelecidos na norma. Além disso, essa relação é capaz de prever até comportamentos e condutas, ou seja, oportuniza a previsibilidade (LEME; BLANK, 2020, p. 04).

Em uma recente pesquisa realizada pelo Ministério da Saúde com o Instituto Brasileiro de Geografia e Estatística (IBGE) foi constatadoque 71,1% dos brasileiros vão a estabelecimentos públicos de saúde em busca de atendimento (PAULA, 2014). Ainda, de acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), 71,5% dos brasileiros (o que representa mais de 150 milhões de pessoas) não possuem planos médico-hospitalares e a cada 4 brasileiros, 3 dependem exclusivamente do Sistema Único de Saúde (SUS) (ALMEIDA, 2022).

Considerando que os dados pessoais sensíveis são relacionados também aos dados de saúde, estes necessitam de atenção especial. Essa proteção não é apenas para a preservação da intimidade do paciente, mas possui o objetivo de auxiliar as

instituições de saúde pública na gestão dos dados, evitando a exposição.

Principalmente após a crise causada pelo Covid-19, que começou em março do ano de 2020, foram relatadas diversas situações de vazamento de dados sobre a testagem da população e casos positivos para a doença. Assim, vislumbra-se que a saúde seria um dos setores com maior possibilidade de violação de dados, e sua posterior divulgação (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Pode-se afirmar que os vazamentos de dados dizem respeito a uma divulgação de informações anteriormente sigilosas e privadas de pessoas físicas ou jurídicas. Tal ato indica ações criminosas que podem objetivar a obtenção de vantagem por meio das informações logradas, além de ações de negligência diante da real necessidade de proteção desses dados, determinada pela LGPD (BRASIL, 2018).

São comuns as ocorrências de vazamentos de dados como o do Facebook-Cambridge, que fez o uso ilegal dos dados de seus usuários (LUIZ; RODRIGUES, 2018). No caso de dados de saúde, houve vazamento de dados, em 2017, dos pacientes do Cartão Nacional de Saúde. Motivo pelo qual as votações no Senado Federal foram otimizadas para sancionar a Lei Geral de Proteção de Dados Pessoais (LGPD) (BARJA; COELHO; HAWRYLISZYN, 2021, p. 02).

Em análise, esses vazamentos podem ser gerados pela exposição de senhas ou desvio de informações de *sites* organizacionais. Pode ocorrer o envolvimento dos próprios funcionários responsáveis pela captação de dados dos pacientes, os quais pela falta de conhecimento ou pela negligência fazem o uso indevido ou a divulgação das informações.

Segundo Bertoni (2020), no ano de 2020 o sistema do Ministério da Saúde sofreu uma séria falha de segurança, que expôs dados de 16 milhões de pessoas com diagnóstico suspeito ou confirmado de Covid-19. No mesmo ano, outra falha de segurança causou o vazamento de dados de mais de 200 milhões de brasileiros que fazem uso do Sistema Único de Saúde ou clientes de planos de saúde (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Para visualizar a seriedade relativa ao tema, além do Brasil, que é o foco deste trabalho, há uma dificuldade enfrentada por diversos outros países. Como exemplo, há a notícia divulgada pelo *HIPAA Journal*, que afirma que entre os anos de 2009 e 2020 houve mais de 3.705 violações de dados de saúde, decorrentes de cerca de 500 registros, que foram informados ao Gabinete de Direitos Civis de Saúde e Serviços Humanos dos Estados Unidos da América. Tais violações causaram, dentro outros danos, a exposição e a divulgação ilegal de registros de saúde equivalentes a mais de 81,72% da população dos Estados Unidos (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Após os relatos quanto ao que seria a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018), bem como explicação sobre suas características, e inclusive ocorrências de vazamentos de dados envolvendo a rede de saúde, ficou evidenciada a necessidade de proteção dos dados de pacientes e todos os indivíduos cadastrados na rede pública de saúde. Neste ponto será necessário entender qual é a relação e as possíveis alterações provocadas pela Lei nos procedimentos de captação de dados nos sistemas de cadastramento de pacientes.

Em 2018 foi criada a Autoridade Nacional de Proteção de Dados (ANPD) cuja atuação seria fiscalizar a aplicação da LGPD (BRASIL, 2018). Assim, o Capítulo VIII da Lei informa acerca das sanções administrativas que podem ser aplicadas pela ANPD. Já o Capítulo IX, em complementação, apresenta as responsabilidades do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP). Desta forma, é imprescindível a aplicação da Lei para garantir, além da proteção dos

indivíduos, a não penalização das entidades públicas (BARJA; COELHO; HAWRYLISZYN, 2021 p.07).

Diante disso, a existência da norma não apenas apresenta para a população o que são os dados pessoais sensíveis e sua importância, mas a necessidade de conhecimento, da comunidade e do Poder Público, acerca das consequências do não cumprimento da Lei. Nesse sentido, foi verificado que há uma grande quantidade de dados pessoais sensíveis mantidos pela rede pública de saúde.

Conforme o Ministério da Saúde (2019), além do registro de cadastramento dos usuários, é necessária a atualização periódica dos dados para que os profissionais consigam fazer um atendimento eficaz na marcação de consultas, no envio de resultados de exames, dentre outros serviços. Por isso, é verificado o crescente número de registros de dados sensíveis de saúde nos últimos anos (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Além disso, o Poder Público é receptor de diversos tipos de dados de toda a população, recebidos por órgãos de atendimento distintos. Desta forma, com o uso da inteligência artificial é possível o cruzamento de todos os dados, tornando ainda mais suscetível a exposição dos dados, prejudicando a integridade moral e física dos indivíduos (BARJA; COELHO; HAWRYLISZYN, 2021, p. 04).

Diante das alterações provocadas pela lei e as ocorrências de vazamentos de dados sensíveis, fica evidenciada a necessidade da aplicação das normas nos fluxos de coleta de dados dos serviços de saúde pública. A aplicação das normas de proteção de dados garante a segurança e a privacidade dos pacientes, e fortalece a confiança na utilização dos serviços de saúde pública. Os cidadãos precisam se sentir seguros ao compartilhar suas informações pessoais, sabendo que serão tratadas de forma responsável e de acordo com os princípios estabelecidos pela LGPD (BRASIL, 2018).

A criação de normas e leis de proteção de dados tem uma relação direta com a necessidade de atualização nacional diante dos impactos sociais, econômicos e políticos decorrentes dos avanços tecnológicos, como destacado por Aragão Schiocchet (2012, p. 04). Nesse contexto, a LGPD (BRASIL, 2018) terá um alcance abrangente, afetando praticamente todos os serviços e as instituições integrantes do Sistema Único de Saúde (SUS), incluindo unidades básicas de saúde, pronto atendimentos, hospitais, clínicas, serviços diagnósticos, serviços de reabilitação, serviços de pesquisa e órgãos gestores (ARAGÃO; SCHIOCCHET, 2012, p. 07).

Os vazamentos de dados sensíveis, como registros médicos, informações sobre tratamentos e históricos de saúde, têm se tornado uma preocupação crescente em todo o mundo. Esses incidentes não só expõem a privacidade dos indivíduos, mas podem trazer consequências graves, como a discriminação, a violação de confidencialidade e até mesmo riscos para a integridade física dos pacientes.

Portanto, embora a LGPD (BRASIL, 2018) tenha impacto todos os setores, assume uma importância maior no setor da saúde, devido ao tratamento dos dados pessoais sensíveis. Hospitais, clínicas, laboratórios, operadoras de saúde e consultórios lidam diariamente com informações sensíveis dos pacientes, e a violação desses dados pode acarretar sérios danos aos titulares (BERNARDO; PINZEGHER; SCHUELTER, 2022, p. 04).

Nesse contexto, a aplicação efetiva das normas de proteção de dados nos fluxos de coleta de informações nos serviços de saúde pública se torna indispensável. Isso implica estabelecer medidas robustas de segurança da informação, promover a conscientização sobre a importância da proteção de dados entre os profissionais de saúde e garantir a implementação de políticas e procedimentos que visem a proteção

das informações sensíveis. O Sistema Único de Saúde (SUS) é um dos principais afetados pela aplicação da LGPD (BRASIL, 2018), pois coleta, armazena, processa e acessa diversos tipos de informações de saúde e doença dos usuários, bem como aspectos genéticos, biométricos e até a vida sexual das pessoas. Portanto, a aplicação efetiva da LGPD (BRASIL, 2018) terá uma influência incontestável no SUS (ARAGÃO; SCHIOCCHET, 2012, p. 07).

Posto isso, um dos problemas que a LGPD (BRASIL, 2018) busca solucionar é o acesso descontrolado e o uso indevido dos dados de saúde, também conhecidos como dados clínicos ou informações médicas. O acesso indiscriminado a esses dados e a falta de controle sobre seu destino violam o direito de privacidade do indivíduo. Muitas vezes, as pessoas desconhecem como seus registros são utilizados, o que contribui para a banalização da privacidade (VETIS-ZAGANELLI; BINDA FILHO, 2022).

É fundamental observar que todos os profissionais que lidam com dados sensíveis devem estar envolvidos e engajados na adequação às diretrizes estabelecidas. Desde o momento em que o paciente entra na recepção até a sua alta, quando seu prontuário é encaminhado para fins administrativos, informações sensíveis são manipuladas e processadas.

A proteção desses dados torna-se crucial para garantir a privacidade e a segurança dos indivíduos. A lei estabelece diretrizes específicas para o tratamento adequado dessas informações, incluindo a obtenção de consentimento do titular, a adoção de medidas de segurança, a limitação do acesso apenas para as pessoas autorizadas, entre outros aspectos relevantes (BARJA; COELHO; HAWRYLISZYN, 2021, p. 06).

Portanto, é imprescindível que as instituições de saúde pública obedeçam todas as exigências legais e adotem medidas efetivas para garantir a proteção dos dados sensíveis. A conscientização acerca da importância da privacidade, a implementação de políticas claras de segurança da informação e o investimento em tecnologias apropriadas são passos fundamentais para assegurar a aplicação adequada das normas nos fluxos de coleta de dados nos serviços de saúde pública. A partir disso será possível construir um ambiente confiável e seguro para o tratamento das informações pessoais no contexto da saúde.

Um dos principais desafios da rede de saúde pública é a adaptação dos sistemas de armazenamento e o tratamento de dados para garantir a segurança e a confidencialidade das informações dos pacientes. Isso inclui a implementação de medidas de segurança tecnológicas e a capacitação dos profissionais da área para lidar com os dados pessoais dos pacientes de acordo com as novas regras estabelecidas pela LGPD (BRASIL, 2018).

Além disso, a LGPD (BRASIL, 2018) também trouxe mudanças na forma como os pacientes autorizam o uso de seus dados pessoais. Agora, os pacientes devem ser informados de forma clara e objetiva sobre como seus dados serão tratados e terão o direito de consentir ou não com o uso desses dados. É necessária a adaptação para garantir que os pacientes sejam informados adequadamente e possam exercer seu direito de escolha.

No âmbito do Sistema Único de Saúde (SUS), é evidente a existência de uma infinidade de dados que ainda não foram anonimizados (dados originalmente relativos a uma pessoa, mas que passaram por um procedimento de desvinculação) ou pseudonimizados (procedimento que substituição de dados de identificação de um indivíduo por uma identificação artificial). Esses dados são compartilhados tanto por meio de sistemas digitais quanto em formato físico entre instituições de todas as

esferas governamentais.

Essa situação se torna problemática, especialmente em municípios ou grupos populacionais de menor porte, nos quais a quantidade restrita de titulares desses dados amplia os riscos de identificação dos indivíduos. Em cenários nos quais o número de pessoas envolvidas é reduzido, a possibilidade de associação direta ou indireta de informações pessoais sensíveis torna-se mais relevante e preocupante (ARAGÃO; SCHIOCCHET, 2012, p. 10).

A proteção da privacidade e a segurança dos dados pessoais no contexto da rede pública de saúde não são apenas questões éticas, mas um imperativo legal. É essencial que os responsáveis pelo tratamento dessas informações adotem medidas rigorosas para garantir a conformidade com a legislação, bem como para proteger a confidencialidade e a integridade dos dados dos cidadãos.

Além de uma mera adequação à legislação, é fundamental destacar que o respeito aos dados dos pacientes envolve aspectos ainda mais valiosos, relacionados ao sigilo, privacidade e confidencialidade no âmbito da assistência em saúde. Esses valores éticos indispensáveis não podem ser negligenciados (VETIS-ZAGANELLI; BINDA FILHO, 2022).

É fundamental que a rede de saúde pública se adapte a essa nova realidade, garantindo que os pacientes sejam devidamente informados sobre o uso de seus dados e tenham a oportunidade de consentir ou não com o seu compartilhamento. Isso implica o desenvolvimento de procedimentos de obtenção de consentimento que sejam transparentes, acessíveis e que forneçam todas as informações relevantes para que os pacientes possam tomar a decisão.

A autodeterminação informativa do paciente é um dos fundamentos da LGPD (BRASIL, 2018), como previsto no art. 2º, II da Lei. Tal princípio tem como início o preenchimento do termo de consentimento esclarecido e informado, um documento exigido para procedimentos cirúrgicos, intervenções médicas e a realização de pesquisas. Esses atos envolvem a necessidade de dados de saúde, e os termos de consentimento devem conter informações sobre a confiabilidade dos exames, alertas sobre possíveis riscos, consequências fisiológicas e complicações, além dos objetivos e benefícios dessa intervenção (VETIS-ZAGANELLI; BINDA FILHO, 2022).

É essencial que os pacientes compreendam claramente para quais finalidades seus dados serão utilizados, se haverá compartilhamento com terceiros, quais medidas de segurança serão adotadas e como poderão exercer seus direitos de acesso, retificação e exclusão dos dados. Essas informações devem ser apresentadas de forma simples e compreensível, evitando o uso de linguagens técnicas que possam dificultar a compreensão, como a própria Lei de Acesso à Informação já indica.

No capítulo II da LGPD (BRASIL, 2018) é despendida atenção ao consentimento do paciente ou seu responsável legal, de modo que o hospital colete e trate os dados, visando o cuidado do paciente. É importante que o hospital informe a necessidade da obtenção desses dados e de que maneira serão utilizados durante o tratamento do paciente. Além disso, o paciente tem o direito de exigir a exclusão de suas informações no prontuário a qualquer momento. É fundamental demonstrar que todas as informações disponibilizadas no prontuário estão devidamente protegidas (BARJA; COELHO; HAWRYLISZYN, 2021, p. 06).

A rede de saúde pública também deve garantir que os pacientes tenham autonomia para consentir ou não com o uso de seus dados. Isso significa que a autorização não pode ser imposta como uma condição para o acesso aos serviços de saúde. Os pacientes devem ter a liberdade de escolher se desejam ou não

compartilhar seus dados pessoais e essa decisão deve ser respeitada.

Atualmente, cada serviço vinculado ao SUS tem autonomia para desenvolver seu próprio modelo de consentimento e assentimento informado para consultas, exames e procedimentos. No entanto, na maioria dos casos, não há itens específicos relacionados com a coleta e o tratamento dos dados, padronização, nem a exigência de requisitos mínimos a serem contemplados nesses documentos (ARAGÃO; SCHIOCCHET, 2012, p. 09).

Além disso, é importante que as instituições de saúde pública implementem mecanismos efetivos para o gerenciamento e o armazenamento seguro dos dados pessoais dos pacientes. Isso inclui a adoção de medidas de segurança da informação, como por exemplo a criptografia, controle de acesso, o monitoramento e a auditoria dos sistemas. Dessa forma, será possível garantir a proteção dos dados, minimizar os riscos de vazamentos ou acessos não autorizados e fortalecer a confiança dos pacientes na utilização dos serviços de saúde pública.

As imposições para o tratamento desses dados são mais rigorosas, uma vez que é exigido o consentimento expresso, em documento separado e para uma finalidade específica, de acordo com o artigo 11 da LGPD (BRASIL, 2018). Conforme o inciso II deste artigo, somente é permitido o tratamento dos dados sensíveis sem o consentimento do titular em situações em que for indispensável (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Em resumo, a LGPD (BRASIL, 2018) trouxe mudanças significativas na autorização e no uso de dados pessoais na área da saúde. A transparência, a clareza e o respeito à autonomia dos pacientes são fundamentais para estabelecer uma relação de confiança e proteger a privacidade e os direitos individuais no contexto da saúde.

Nessa linha, resta evidente a necessidade de adaptação de fluxos de captação de dados que envolve o cadastramento de pacientes e todos os cidadãos que usam a rede pública de saúde. Os dados solicitados devem passar pela etapa de consentimento, além da necessidade de armazenamento em sistemas seguros, e profissionais treinados para garantir a segurança das informações e a integridade física e moral do indivíduo.

As tecnologias desenvolvidas no campo da saúde têm uma ampla utilização de dados pessoais, especialmente os dados sensíveis, como dados biométricos e indicadores fisiológicos. Outros contextos além do médico-hospitalar também lidam com inúmeros dados sensíveis. Portanto, é importante garantir a proteção da privacidade desde a concepção do produto, conforme exigido pela Lei Geral de Proteção de Dados Pessoais (BERNARDO; PINZEGHER; SCHUELTER, 2022, p. 05).

Além disso, é necessária a implementação de práticas de governança de dados, incluindo políticas claras de privacidade, procedimentos de consentimento informado e ações de treinamento para profissionais envolvidos no manuseio dessas informações. Ao adotar uma abordagem proativa para a proteção da privacidade desde o início, as organizações de saúde podem fortalecer a confiança dos pacientes e usuários, ao mesmo tempo em que cumprem com as obrigações legais e éticas de privacidade e proteção de dados.

No Brasil, historicamente, a experiência de tratamento de dados em saúde tem sido acompanhada pela implementação de vários sistemas de informação com diversos objetivos. Como exemplo, podemos citar os sistemas vinculados ao DATASUS, como o Departamento de Informática do SUS, como o Sistema de Informações Hospitalares (SIH), Sistema de Informação de Mortalidade (SIM), Sistema de Informação de Atenção Básica (SIAB), Sistema de Cadastramento de

Usuários (CADSUS) e outros sistemas de abrangência nacional. Além disso, existem sistemas com a possibilidade de serem desenvolvidos e implantados localmente por Estados e Municípios (ARAGÃO; SCHIOCCHET, 2012, p. 08).

Esses sistemas são adaptados conforme as necessidades específicas de cada localidade, permitindo um acompanhamento mais detalhado e personalizado da saúde da população em nível regional, são essenciais para o planejamento e a gestão eficientes do sistema de saúde pública no Brasil. Eles fornecem dados valiosos para subsidiar políticas públicas, identificar tendências, avaliar a qualidade dos serviços e orientar a tomada de decisões estratégicas.

Na área da saúde, é crucial que toda e qualquer tecnologia considere a potencial coleta e o tratamento de dados sensíveis, o que demanda uma atenção especial para garantir a segurança em cada etapa de submissão dos dados,(BERNARDO; PINZEGHER; SCHUELTER, 2022, p. 11). No entanto, para alcançar isso é necessária a adequação dos sistemas de informação e a adoção de novas abordagens, a fim de evitar violações de informações confidenciais e outros tipos de incidentes de segurança, possibilitando um uso eficaz dos grandes volumes de dados de saúde (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Para isso, é fundamental investir em sistemas de informação robustos, que adotem medidas de criptografia, controle de acesso, monitoramento contínuo e a capacitação dos profissionais envolvidos. Além disso, a conscientização sobre a importância da proteção dos dados deve ser disseminada entre todos os atores envolvidos, desde os desenvolvedores de tecnologias até os profissionais de saúde e os pacientes.

Ao adotar essas medidas, é possível fazer um uso eficaz dos grandes volumes de dados de saúde disponíveis. A análise dessas informações pode gerar percepções essenciais para o desenvolvimento de políticas de saúde, aprimoramento de diagnósticos, além de contribuir para a pesquisa científica e a inovação tecnológica na área da saúde.

A crescente utilização dos recursos da Tecnologia da Informação e Comunicação na área da saúde amplia a necessidade de atenção com a segurança dos dados. O volume dessas informações é significativo, e nem sempre há uma organização adequada, o que aumenta os desafios de proteção e gerenciamento dos dados sensíveis. A implementação de recursos como prontuário eletrônico do paciente (PEP), telemedicina e troca de informações entre instituições requer uma abordagem sólida de segurança para garantir a confidencialidade e a integridade dos dados em trânsito e armazenados (BARJA; COELHO; HAWRYLISZYN, 2021, p. 05).

Visto isso, a proteção dos dados sensíveis na área da saúde é um desafio. Por meio do desenvolvimento de novos sistemas de informação e da adoção de abordagens atualizadas de segurança é possível garantir a confidencialidade e a integridade dos dados, possibilitando um uso eficaz dessas informações para o benefício de pacientes, profissionais e do sistema de saúde como um todo.

Quando ocorrem violações de registros médicos e vazamentos de dados, o dever da confidencialidade é desrespeitado. Assim, é necessário responsabilizar aqueles que deveriam garantir a segurança do armazenamento dos dados, de acordo com a LGPD (BRASIL, 2018), sendo considerados agentes de tratamento (VETIS-ZAGANELLI; BINDA FILHO, 2022).

É importante ressaltar que a responsabilidade pela segurança desses dados não recai apenas sobre os profissionais de saúde, mas sobre as instituições, empresas e prestadores de serviços que lidam com essas informações. Todos os agentes de tratamento de dados são responsáveis pela adoção de medidas de

segurança adequadas para proteger a privacidade e a integridade das informações pessoais.

Nesse sentido, há a necessidade de cumprimento da confidencialidade. Este é um dever intrínseco da relação entre o médico e o paciente, previsto ainda em diversos códigos de ética auxiliando o cumprimento das normas de proteção dos dados pessoais sensíveis e evitando diversas situações de violação (VETIS-ZAGANELLI; BINDA FILHO, 2022).

É importante ressaltar que a conformidade com a LGPD (BRASIL, 2018) não é apenas uma questão de evitar sanções, mas promover a confiança dos titulares de dados e manter a reputação e a integridade da instituição. Ao garantir a segurança e a privacidade dos dados, as instituições demonstram o seu compromisso com a proteção dos direitos dos indivíduos.

As medidas de segurança e os padrões estabelecidos são elementos essenciais para garantir a proteção dos dados pessoais e o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018). É fundamental que as instituições compreendam e estejam em conformidade com tais medidas, a fim de evitar multas e sanções aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) (BARJA; COELHO; HAWRYLISZYN, 2021, p. 09).

Para garantir a segurança dos dados, as instituições devem adotar políticas e procedimentos claros, alinhados com os princípios e os requisitos estabelecidos pela LGPD (BRASIL, 2018). Isso inclui a implementação de medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, perdas, alterações ou divulgações indevidas.

A ANPD, como órgão responsável pela fiscalização e a aplicação da LGPD (BRASIL, 2018), tem o poder de impor multas e sanções em caso de não conformidade com a lei. Portanto, as instituições devem estar cientes de suas obrigações e investir em boas práticas de proteção de dados para evitar consequências adversas. Além disso, é fundamental que realizem ações periódicas para monitorar a adequação das medidas de segurança e revisar os processos existentes (BARJA; COELHO; HAWRYLISZYN, 2021, p. 07).

Primeiramente, é necessário concentrar os esforços na compreensão das normas estabelecidas pela Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), avaliando seus impactos e alcance sobre a estrutura da tecnologia da informação do Sistema Único de Saúde (SUS). Isso envolve revisar o modelo de governança existente e identificar as instituições, que serão afetadas pelas novas exigências. Após esse procedimento, será possível avançar para a implementação dos componentes do modelo de governança de proteção de dados delineado nas fases anteriores. Isso implica alinhar adequadamente as camadas do sistema e a tecnologia da informação do SUS para garantir um desempenho eficiente e maior capacidade operacional (ARAGÃO; SCHIOCCHET, 2012, p. 12).

A falta de padronização e normalização na coleta de dados dentro da rede pública de saúde pode gerar lacunas na proteção da privacidade e no cumprimento das exigências legais. Para superar esses obstáculos será necessário realizar um mapeamento abrangente dos diferentes modelos de coleta de dados em uso, identificando possíveis vulnerabilidades e lacunas na conformidade com a LGPD (BRASIL, 2018).

Uma das principais dificuldades enfrentadas pela rede pública de saúde na sua adequação está relacionada com a grande variabilidade de modelos e métodos de coleta de dados não padronizados e não normalizados. Essa diversidade de abordagens dificulta a implementação de medidas de segurança e privacidade de

forma consistente em toda a estrutura da rede (ARAGÃO SCHIOCCHET, 2012, p. 10).

Além disso, é importante destacar a existência de milhares de *bytes* de dados já coletados e armazenados nos equipamentos do SUS para os quais não foi solicitado o consentimento dos indivíduos. Isso representa uma questão desafiadora em termos de conformidade com a LGPD (BRASIL, 2018), que exige a obtenção de consentimento explícito e informado para o tratamento de dados pessoais.

A Lei do Marco Civil da *Internet*, promulgada em abril de 2014, estabelece diretrizes e princípios para o uso da *internet* no Brasil para garantir a proteção dos direitos dos usuários, incluindo a segurança dos dados pessoais. Embora seu foco principal seja a regulamentação da *internet* como um todo, alguns de seus princípios e disposições têm implicações diretas para o campo da saúde.

Em âmbito sanitário, são realizados esforços no sentido de padronizar e formular normas elucidativas sobre a proteção de dados em saúde. A Lei n.° 12.965/2014 (BRASIL, 2014), conhecida como Lei do Marco Civil da Internet, desempenhou um papel importante ao introduzir princípios fundamentais de segurança dos dados nesse contexto (VETIS-ZAGANELLI; BINDA FILHO, 2022).

Ademais, é importante ressaltar que a proteção de dados em saúde não se restringe apenas ao ambiente digital, mas abrange os meios físicos de armazenamento e transmissão de informações. É necessário estabelecer medidas de segurança abrangentes, considerando os aspectos tecnológicos e os processos e procedimentos adotados nas instituições de saúde.

A crescente disponibilidade e acessibilidade aos dados gerados no contexto da saúde têm impulsionado avanços significativos na área. A coleta, o armazenamento e a análise de dados permitem que os profissionais de saúde identifiquem padrões, tomem decisões embasadas em evidências e personalizem o atendimento aos pacientes.

Conforme mencionado por Nybo (2019), atualmente é quase impossível conceber uma solução no campo da saúde que não envolva a utilização de dados pessoais. Vivemos em uma era conhecida como “dataísmo”, na qual a realidade passou a ser interpretada e compreendida por meio dos dados (BERNARDO; PINZEGHER; SCHUELTER, 2022, p. 08). O “dataísmo” se baseia na ideia de que os dados são uma ferramenta fundamental para a compreensão do mundo ao nosso redor. Os avanços tecnológicos e a interconectividade permitem a geração contínua de dados em diferentes formatos e escalas.

Nesse ponto, é importante registrar que o DATASUS, departamento de informática do Sistema Único de Saúde, em seu Plano Diretor de Tecnologia da Informação 2019/2021, menciona a necessidade de preparação para *compliance*, de modo que auxilie a implementação da LGPD (BRASIL, 2018) no Ministério da Saúde (ARAGÃO; SCHIOCCHET, 2012, p. 11).

Para garantir a efetiva implementação desses princípios é essencial revisar constantemente os pontos de privacidade em cada etapa do desenvolvimento. Isso inclui a análise da coleta e do armazenamento de dados, a definição de políticas claras de privacidade, a adoção de medidas de segurança adequadas e a garantia de conformidade com as regulamentações aplicáveis, como a LGPD (BRASIL, 2018) no Brasil.

A proteção de dados pessoais é um aspecto crucial que deve ser considerado desde o início de qualquer projeto. É fundamental incorporar os princípios do *Privacy by Design* (Privacidade desde a Concepção) e *Privacy by Default* (Privacidade por Padrão) em todas as etapas de desenvolvimento (BERNARDO; PINZEGHER; SCHUELTER, 2022, p. 10).

O *Privacy by Design* aborda a incorporação de medidas de privacidade e proteção de dados desde a concepção do produto ou sistema. Isso significa que a privacidade deve ser uma consideração central durante o planejamento, a arquitetura e a implementação da solução. Ao adotar essa abordagem, busca-se garantir a privacidade dos dados pessoais desde o início, em vez de tentar corrigir problemas de privacidade posteriormente.

Já o *Privacy by Default* envolve a configuração padrão de um produto ou serviço para que as configurações de privacidade mais restritivas sejam aplicadas automaticamente. Isso significa que as configurações devem ser pré-definidas para oferecer o nível máximo de privacidade aos usuários, permitindo que façam ajustes que posteriormente desejem.

Assim, a proteção de dados pessoais deve ser uma prioridade desde o início de qualquer projeto. A abordagem *Privacy by Design* e *Privacy by Default* garante que os requisitos de privacidade sejam considerados e implementados em todas as fases do desenvolvimento. Revisões periódicas e a participação de especialistas em privacidade são fundamentais para garantir a conformidade e a proteção efetiva dos dados pessoais dos usuários.

Além dos princípios que devem ser observados desde a concepção de novas soluções de saúde, é fundamental considerar as orientações técnicas fornecidas pelas ISOs (normas que buscam um melhor e mais eficaz direcionamento de processos por meio da criação de condutas e padrões, associadas com as práticas da Associação Brasileira de Normas Técnicas-ABNT). Essas normativas oferecem um conjunto de diretrizes e boas práticas para o desenvolvimento de produtos e serviços que preservem a privacidade e a segurança dos dados pessoais, complementando os princípios básicos estabelecidos. Ao adotar essas abordagens combinadas é possível construir soluções eficazes e confiáveis, que supram as necessidades dos usuários e estejam em conformidade com as exigências regulatórias.

Durante a concepção de novas soluções no âmbito da saúde é fundamental observar os princípios que regem a proteção de dados pessoais. No entanto, é importante destacar que esses princípios não são as únicas boas práticas que devem ser adotadas nesse contexto. Existem diversas orientações adicionais que podem complementá-los para garantir a preservação da privacidade dos titulares dos dados pessoais. Nesse contexto, a família de normas ISO 27000 desempenha um papel relevante. Essas normas estabelecem diretrizes e requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI). Elas fornecem um conjunto abrangente de práticas recomendadas para proteção da informação, incluindo a privacidade dos dados pessoais (BERNARDO; PINZEGHER; SCHUELTER, 2022, p. 07).

Destaca-se a questão do livre compartilhamento de informações entre instituições de rede pública de saúde, que requer uma abordagem cuidadosa, equilibrando a necessidade de acesso às informações para assegurar os direitos dos pacientes com a proteção da privacidade e a confidencialidade dos dados pessoais. A criação de regulamentações específicas e diretrizes claras para o intercâmbio de informações pode contribuir para um ambiente mais seguro e transparente, garantindo a continuidade do cuidado, a promoção da saúde e o cumprimento dos direitos dos usuários da rede de saúde pública.

Até o momento, não existe uma regulamentação clara sobre a troca de dados entre as diversas entidades da rede pública de saúde. Isso pode gerar desafios, especialmente nos casos em que as solicitações de informações são feitas por órgãos judiciais, Defensorias Públicas e Ministérios Públicos, frequentemente procurados por

pacientes que buscam garantir o direito à saúde (ARAGÃO; SCHIOCCHET, 2012, p. 10).

A ausência de diretrizes específicas para o compartilhamento de informações entre instituições relacionadas ao SUS pode criar incertezas e obstáculos na troca de dados relevantes para a continuidade e a qualidade do atendimento aos pacientes. A falta de uma clara regulamentação nesse sentido pode resultar em dificuldades para garantir o acesso adequado às informações necessárias para a tomada de decisões médicas e o planejamento de políticas de saúde.

A falta de uma regulamentação específica para o compartilhamento de informações entre todas as instituições de saúde pública gera incertezas e obstáculos no fluxo de dados relevantes para a continuidade e a qualidade do atendimento aos pacientes. A ausência de orientações claras nesse sentido dificulta o acesso adequado às informações necessárias para a tomada de decisões médicas e o planejamento de políticas de saúde.

Nesse sentido, a Fundação Vanzolini, por meio de seu guia de implantação, informou que ao implementar um sistema de gestão, contendo processos, pessoas e tecnologia, que perpassa por todas as áreas de trabalho, a organização tornará possível o atendimento contínuo de maneira sustentável dos requisitos da LGPD (BRASIL, 2018) (BARJA; COELHO; HAWRYLISZYN, 2021, p. 07).

Ao se adequar à LGPD (BRASIL, 2018), as instituições de saúde têm a oportunidade de rever suas práticas e implementar medidas robustas de proteção de dados. Isso inclui a adoção de políticas de privacidade claras, o estabelecimento de mecanismos de consentimento adequados, a implementação de sistemas de segurança da informação e a capacitação dos profissionais envolvidos.

O respaldo jurídico é um elemento fundamental quando se trata da proteção de dados pessoais no contexto da LGPD (BRASIL, 2018). Além disso, é essencial que cada instituição reconheça as ações necessárias para estar em conformidade com a legislação. A LGPD (BRASIL, 2018) não deve ser vista apenas como uma exigência legal, mas como um estímulo para impulsionar processos tecnológicos e informacionais nas instituições, visando proporcionar maior segurança e privacidade aos pacientes (BARJA; COELHO; HAWRYLISZYN, 2021, p. 10).

O uso do *big data (*conjunto de dados com alto volume e complexidade) na área da saúde oferece oportunidades promissoras. Com a quantidade crescente de dados disponíveis, provenientes de registros médicos eletrônicos, dispositivos médicos, aplicativos móveis e outros sistemas de informação, os profissionais de saúde têm acesso a uma riqueza de informações que podem ser exploradas.

Além disso, com o passar dos anos foi possível verificar um crescimento significativo do uso do *big data* em todas as áreas da saúde. O *big data*, a análise e a utilização de conjuntos de dados massivos e complexos, têm desempenhado um papel cada vez mais importante na tomada de decisões e na melhoria dos cuidados de saúde (LEME; BLANK, 2020, p. 04).

Uma das principais vantagens do *big data* na saúde é sua capacidade de identificar padrões e tendências que podem auxiliar no diagnóstico precoce de doenças, no desenvolvimento de tratamentos personalizados e na previsão de surtos epidemiológicos. Como exemplo, os algoritmos de aprendizado de máquina podem analisar grandes volumes de dados de pacientes para identificar fatores de risco e padrões de sintomas que possam indicar a ocorrência de determinadas condições médicas.

Além disso, o *big data* possibilita a análise de dados em tempo real, permitindo uma resposta mais rápida a eventos críticos, como epidemias ou emergências de

saúde pública. Isso é especialmente relevante em situações de crise, quando a agilidade na coleta, na análise e no compartilhamento de informações pode salvar vidas.

No contexto do *big data* é comum a coleta massiva de dados pessoais para alimentar algoritmos e análises complexas. No entanto, a LGPD (BRASIL, 2018) estabelece que esse processo deve ocorrer de forma transparente e com consentimento do titular dos dados. Além disso, a Lei impõe a necessidade de garantir a segurança e a privacidade dessas informações, protegendo contra acessos não autorizados, vazamentos ou uso indevido.

Ao observar os princípios da LGPD (BRASIL, 2018) no contexto do *big data*, é possível assegurar que o tratamento dos dados seja realizado de maneira ética e responsável. Isso significa que as organizações que fazem uso do *big data* devem adotar medidas de segurança robustas, implementar políticas claras de privacidade, fornecer informações claras sobre o tratamento dos dados e obter o consentimento adequado dos indivíduos.

Dessa forma, a LGPD (BRASIL, 2018) terá um grande impacto no *big data*, visto que a obtenção de informações pessoais por meio do tratamento de dados, sem que sejam observados os paradigmas ali instituídos, poderá gerar danos aos indivíduos, ferindo gravemente a privacidade, a liberdade e a autonomia dos mesmos (LEME; BLANK, 2020, p. 05).

É importante destacar que o uso do *big data* na saúde traz desafios e preocupações. A privacidade e a segurança dos dados pessoais são questões cruciais, especialmente quando se trata de informações sensíveis de saúde. É essencial garantir que as medidas adequadas sejam implementadas para proteger a privacidade dos indivíduos e garantir a conformidade com regulamentações, como a LGPD (BRASIL, 2018).

No contexto atual, em que a tecnologia desempenha um papel fundamental em todos os setores, a proteção das informações tornou-se uma preocupação central para as organizações. Dados sensíveis e confidenciais são constantemente coletados, armazenados e compartilhados, tornando-se alvos potenciais para ameaças cibernéticas e violações de privacidade.

Nesse sentido, o desenvolvimento de um planejamento adequado para o gerenciamento de riscos é essencial. É preciso identificar e avaliar os riscos associados às informações, sejam vazamentos, acessos não autorizados, falhas de segurança ou outras vulnerabilidades. Com base nessa análise, medidas de segurança e protocolos de proteção podem ser implementados de forma proativa. Assim, para garantir a confidencialidade, a integridade e a segurança das informações, é indispensável o desenvolvimento do planejamento e do gerenciamento de riscos (LEME; BLANK, 2020, p. 08).

O desenvolvimento de um planejamento e um gerenciamento de riscos eficaz envolve tanto aspectos técnicos quanto organizacionais. É necessário estabelecer políticas claras de segurança da informação, promover a conscientização e o treinamento dos colaboradores, realizar avaliações regulares e constantes atualizações das melhores práticas e regulamentações vigentes.

No geral, empresas que exploram a inteligência artificial e as tecnologias semelhantes estão impulsionando a inovação na área da saúde. Essas soluções têm o potencial de transformar a forma como recebemos cuidados médicos, tornando-os mais acessíveis, eficientes e personalizados. Mas, é importante encontrar um equilíbrio entre a tecnologia e o cuidado humano, garantindo que a saúde seja tratada com a devida sensibilidade e a atenção necessária.

Uma empresa em destaque é a *Babylon*, que tem como missão disponibilizar um serviço de saúde acessível para todos. Com o avanço da tecnologia e a inteligência artificial desempenhando um papel cada vez mais importante na área da saúde, a *Babylon* desenvolveu um aplicativo inovador que utiliza Inteligência Artificial para fornecer assistência médica acessível para milhões de pessoas. Com base nos dados fornecidos pelos usuários e nas respostas obtidas durante a anamnese virtual, a inteligência artificial é capaz de realizar uma análise criteriosa e propor um provável diagnóstico (LEME; BLANK, 2020, p. 10).

A iniciativa da *Babylon* representa um avanço importante no campo da saúde digital, ao utilizar a inteligência artificial para democratizar o acesso aos cuidados médicos. Ao disponibilizar um serviço acessível a todas as pessoas do planeta, a empresa pretende reduzir as barreiras geográficas e financeiras, garantindo que mais indivíduos recebam orientações médicas confiáveis e busquem o tratamento adequado.

No entanto, é importante destacar que a utilização de dados pessoais sensíveis, como informações médicas e sintomas, levanta questões de privacidade e proteção desses dados. É fundamental que a empresa, ou no caso, os sistemas utilizados pela Administração Pública, estejam em conformidade com as leis e regulamentações de proteção de dados, garantindo a segurança e a confidencialidade das informações dos usuários.

A cultura da organização representa um desafio para a adequação das instituições de saúde à LGPD (BRASIL, 2018). Assim, se a conduta não estiver baseada na lei, sendo aplicada em todas as rotinas do paciente, podem existir dúvidas e até dificuldades no controle das informações (BARJA; COELHO; HAWRYLISZYN, 2021, p. 10).

A implementação de treinamentos e programas de capacitação sobre a LGPD pode ajudar a disseminar o conhecimento e a compreensão das melhores práticas de proteção de dados. Além disso, é essencial estabelecer políticas claras de privacidade e segurança da informação, bem como mecanismos de monitoramento e controle para garantir o cumprimento das diretrizes estabelecidas pela LGPD (BRASIL, 2018).

Uma cultura organizacional sólida e baseada na LGPD (BRASIL, 2018) é essencial para assegurar que as informações dos pacientes sejam devidamente controladas e acessadas apenas por profissionais autorizados. Isso contribui para a construção de uma relação de confiança com os pacientes, fortalece a reputação da instituição de saúde e, acima de tudo, protege os direitos fundamentais de privacidade e segurança dos dados pessoais.

Por todo o exposto, é possível entender que o processo de adaptação ao novo cenário exigirá uma estreita colaboração entre gestores, técnicos e a sociedade civil. Caso ocorram violações ou descumprimentos, a sociedade terá o respaldo legal para buscar sanções e reparação pelos danos causados. Essa possibilidade de responsabilização das instituições de saúde em caso de descumprimento da LGPD (BRASIL, 2018) é um incentivo para que elas se adaptem conforme as exigências da legislação (ARAGÃO; SCHIOCCHET, 2012, p. 14).

As penalidades previstas podem ser severas e incluem multas expressivas, além de outros tipos de sanções. Diante disso, é do interesse tanto das instituições quanto da sociedade civil que a adaptação ao novo cenário ocorra de forma efetiva. Além disso, no contexto da rede pública de saúde, que lida diariamente com um volume significativo de informações sensíveis, é essencial que sejam estabelecidas medidas e procedimentos adequados para proteger esses dados.

Para alcançar a conformidade com a LGPD (BRASIL, 2018), a rede de saúde

pública precisa adotar uma abordagem abrangente, considerando da coleta até o armazenamento e o compartilhamento de dados. Serão necessárias políticas claras de privacidade e segurança da informação, além de investimentos em tecnologia e capacitação dos profissionais envolvidos.

Portanto, embora o caminho de revisão e readequação seja desafiador, ele é inevitável para as organizações que fazem o atendimento de milhares de pessoas estejam nos termos determinados pela lei. A revisão da estrutura existente implica analisar cuidadosamente os processos, as políticas e as práticas organizacionais para identificar possíveis lacunas e ineficiências. É necessário questionar se a estrutura atual está alinhada de acordo com as necessidades e demandas do ambiente em que a organização opera (ARAGÃO; SCHIOCCHET, 2012, p. 12)

Com uma abordagem cuidadosa, planejamento estratégico e o envolvimento de todos os membros da organização, é possível superar esses desafios e construir uma estrutura e cultura organizacional adaptadas aos novos moldes, prontas para enfrentar os desafios e fornecer os cuidados físicos a partir de um atendimento de qualidade, garantindo a proteção dos dados de todos os indivíduos envolvidos.

Nessa linha, a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) requer esforços abrangentes e coordenados, envolvendo tanto a conscientização individual quanto o comprometimento institucional. Portanto, os desafios da adequação à LGPD (BRASIL, 2018) exigem esforços em diferentes frentes. A conscientização das pessoas é o primeiro passo para criar uma cultura de proteção de dados. O planejamento estratégico é necessário para identificar as medidas adequadas de conformidade. E, por fim, os investimentos são indispensáveis para implementar as mudanças necessárias e garantir a segurança dos dados pessoais (BARJA; COELHO; HAWRYLISZYN, 2021, p. 10).

Assim, com um esforço conjunto envolvendo a participação ativa de profissionais, gestores, órgãos reguladores e a sociedade em geral, será possível superar esses desafios e construir um ambiente em que a privacidade e a segurança dos dados sejam resguardadas, promovendo uma sociedade mais consciente e protegida na coleta e no tratamento de informações pessoais.

Considerações Finais

Este artigo de revisão de literatura abordou a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) nos procedimentos de coleta de dados dos serviços de saúde pública. Através da análise de diversos estudos e pesquisas foi possível compreender a relevância e os desafios da implementação dessa legislação nesse contexto específico.

Foi possível verificar que os principais desafios enfrentados pelas instituições de saúde pública abordam a conscientização e a capacitação dos profissionais envolvidos, bem como a implementação de políticas e medidas de segurança da informação. Portanto, para a aplicação da LGPD (BRASIL, 2018) nos procedimentos de coleta de dados nos serviços de saúde pública é necessário promover a cultura de proteção de dados e estimular a adoção de práticas seguras em todas as etapas do processo de coleta, armazenamento e uso dessas informações, além da adaptação de fluxos de tarefas atendendo ao critério do consentimento do paciente com as devidas atualizações ou criações de sistemas de informações mais seguros e eficazes.

Os resultados obtidos indicam que a LGPD (BRASIL, 2018) desempenha um papel fundamental na proteção da privacidade e dos dados pessoais dos indivíduos envolvidos nos serviços de saúde pública. Com a crescente digitalização e

armazenamento de informações sensíveis é essencial que as instituições adotem medidas adequadas para garantir a conformidade com os princípios e requisitos estabelecidos pela lei.

Além disso, foi demonstrado que a parceria entre os serviços de saúde pública e os pacientes desempenha um papel importante. É fundamental informar os indivíduos sobre seus direitos em relação aos seus dados pessoais, fornecendo transparência e consentimento informado em todas as etapas do processo. A criação de mecanismos de participação e controle social pode fortalecer ainda mais a proteção dos dados e promover a confiança dos usuários nos serviços de saúde pública.

O artigo demonstrou a relevância do tema aos operadores do Direito, de modo que a análise do normativo e o estudo das exigências sejam agentes na adequação dos procedimentos das instituições de saúde. Foi possível observar a intrínseca relação entre a sociedade usuária e beneficiária dos serviços, que é atuante ao conhecer os seus direitos e exigir seu cumprimento. E a ciência, que a partir do seu desenvolvimento e trabalho em conjunto com a sociedade e profissionais do Direito será alvo de grandes avanços contribuindo e tornando cada vez mais efetivo o tratamento dos pacientes.

Portanto, a aplicabilidade da LGPD (BRASIL, 2018) nos procedimentos de coleta de dados dos serviços de saúde pública é essencial para garantir a privacidade, a segurança e a integridade das informações pessoais. A conscientização, a capacitação dos profissionais, a implementação de políticas e as medidas de segurança com a participação ativa dos pacientes são elementos-chave para o sucesso dessa implementação. A contínua avaliação e a atualização das práticas de proteção de dados serão necessárias para acompanhar os avanços tecnológicos e as demandas da sociedade, assegurando a proteção dos direitos individuais no contexto da saúde pública.

Referências

ALMEIDA, Lucilene. **Crescimento anual no número de usuários do SUS chama atenção e reforça a importância da rede pública para os brasileiros**. 14 de dez. de 2022. Disponível em: <https://newslab.com.br/crescimento-anual-no-numero-de-usuarios-do-sus-chama-atencao-e-reforca-a-importancia-da-rede-publica-para-os-brasileiros/>. Acesso em: 07 maio 2023.

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: Desafios do Sistema Único de Saúde. **Revista Eletrônica de Comunicação, Informação e Saúde**. Vol. 14, n° 3, p. 692-708. jul.- set, 2020. Disponível em: <https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2012/2391>. Acesso em: 06 mar. 2023.

BARJA, Paulo Roxo; COELHO, Natalia Gavioli Souza Campos; HAWRYLISZYN, Larissa Oliveira. Lei Geral de Proteção de Dados (LGPD): O Desafio de Sua Implantação para a Saúde. **Revista UNIVAP**. Vol. 27, n° 54. 2021. Disponível em: <http://revista.univap.br/index.php/revistaunivap/article/view/2589>. Acesso em: 15 mar. 2023.

BERNARDO, Taynara Rodrigues; PINZEGHER, Igor Pacheco; ILHASCHUELTER, Patrícia. Lei de Proteção Geral de Dados em Saúde: Protegendo a Saúde, o Usuário

e o Profissional. **Livro Desenvolvimento de Tecnologias em Pesquisa e Saúde: Da Teoria à Prática**. Ed. Científica Digital. Vol. 1, n° 1, Cap. 9, p. 138-149. 2022. Disponível em: <https://downloads.editoracientifica.com.br/articles/220408594.pdf>. Acesso em: 09 mar. 2023.

BERTOTTI, Barbara Mendonça; BLANCHET, Luiz Alberto. Public foment for innovation in artificial intelligence: An assessment based on technological data from patents. **International Journal of Digital Law**. Belo Horizonte. vol. 2, n°. 3. set./dez, 2021. Disponível em: <https://journal.nuped.com.br/index.php/revista/article/view/v2n3bertotti2021>. Acesso em: 24 mar. 2023.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Dispõe sobre a Proteção dos Dados Pessoais. Brasília, DF: Diário Oficial da União, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 20 mar. 2023.

DANTAS, Eduardo. A Responsabilidade Civil Pelo Manuseio e Tratamento de Dados Pessoais Sensíveis em Saúde - Apontamentos em Razão da LGPD. **REVISTA DE DIREITO MÉDICO E DA SAÚDE: doutrina, legislação, jurisprudência**. Brasília: VEM MAIS EDITORAÇÃO. n. 24. set. 2021. p.27-41. Disponível em: <https://anadem.org.br/wp-content/uploads/2023/02/Revista-de-Direito-Medico-e-da Saude-24a-Edicao_web-1-1.pdf#page=27>. Acesso em: 25 mar. 2023.

DUARTE,S.V.; FURTADO, M.S.V. Trabalho de conclusão de curso (TCC) em ciências sociais aplicadas. São Paulo: **Saraiva, 2014. E-book Kindle**. Paginação irregular. Acesso em: 10 abr. 2023.

FALEIROS JÚNIOR, José Luiz de Moura . Reflexões Sobre as Bases Legais Para o Tratamento de Dados Pessoais Relativos à Saúde na Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Médico e da Saúde: doutrina, legislação, jurisprudência**. Brasília: Vem Mais Editoração. n. 24. set. 2021. p.11-26. Disponível em: <https://anadem.org.br/wp-content/uploads/2023/02/Revista-de-Direito-Medico-e-da Saude-24a-Edicao_web-1-1.pdf#page=11>. Acesso em: 21 maio 2023.

GONÇALVES, Jonas Rodrigo. Como elaborar uma resenha de um artigo acadêmico ou científico. **Revista JRG de Estudos Acadêmicos**. Vol. 3, n. 7, p. 95–107, 2020. DOI: 10.5281/zenodo.3969652. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/41>. Acesso em: 03 abr. 2023.

GONÇALVES, Jonas Rodrigo. Como escrever um artigo de revisão de literatura. **Revista JRG de Estudos Acadêmicos**. Vol. 2, n. 5, p. 29–55, 2019. DOI: 10.5281/zenodo.4319105. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/122>. Acesso em: 03 abr. 2023.

GONÇALVES, Jonas Rodrigo. Como fazer um projeto de pesquisa de um artigo de revisão de literatura. **Revista JRG de Estudos Acadêmicos**. Vol. 2, n. 5, p. 01–28, 2019. DOI: 10.5281/zenodo.4319102. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/121>. Acesso em: 05 abr. 2023.

GONÇALVES, Jonas Rodrigo. Escolha do tema de trabalho de curso na graduação em Direito. **Revista Coleta Científica**. Vol. 5, n. 9, p. 88–118, 2021. DOI: 10.5281/zenodo.5150811. Disponível em: <http://portalcoleta.com.br/index.php/rcc/article/view/58>. Acesso em: 05 abr. 2023.

INSTITUTO, Nacional de Traumatologia e Ortopedia. **O que são Dados Pessoas Sensíveis?**. Disponível em: <https://www.into.saude.gov.br/lista-servicos/219-perguntas-frequentes/perguntas-lgpd/790-como-faco-para-atualizar-meu-cadastro-no-into-8#:~:text=Assim%2C%20s%C3%A3o%20dados%20pessoais%20sens%C3%ADveis,quando%20vinculado%20a%20um%20indiv%C3%ADduo>. Acesso em: 15 abr. 2023.

LEME, Renata Salgado; BLANK, Marcelo. Jurisprudência e Legislação Sanitária Comentadas Lei Geral de Proteção de Dados e Segurança da Informação na Área da Saúde. **Cadernos Ibero-Americanos de Direito Sanitário**. Vol. 9, n°3. 2020. Disponível em: <https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690/770>. Acesso em: 21 mar. 2023.

LGPD Brasil.com.br. Adequação da LGPD na Saúde: Entenda mais. Disponível em: <https://www.lgpdbrasil.com.br/lgpd-na-saude/>. Acesso em: 05 maio 2023.
MINISTÉRIO, da Saúde. **Profissionais de Saúde, Vamos Cadastrar a População?** 21 out. 2019. Disponível em: <https://aps.saude.gov.br/noticia/5994>. Acesso em: 06 maio 2023
PAULA, Patrícia de**. 71% dos brasileiros têm os serviços públicos de saúde como referência**. Disponível em: <https://bvsms.saude.gov.br/71-dos-brasileiros-tem-os-servicos-publicos-de-saude-como-referencia/> Acesso em: 09 abr. 2023.

Tribunal de Justiça do Distrito Federal e Territórios. Marco Civil da Internet. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet>. Acesso em: 15 abr. 2023.

VETIS-ZAGANELLI, Margareth; BINDA FILHO, Douglas Luis.A Lei Geral de Proteção de Dados e Suas Implicações na Saúde: As Avaliações de Impacto no Tratamento de Dados no mbito Clínico-Hospitalar. **Revista de Bioética y Derecho**. Vol. 1, n° 54, p. 215-232. 2022. Disponível em: <https://scielo.isciii.es/scielo.php?script= sci_arttext & pid=S1886-58872022000100013 & lng= es\ nrm= iso & tlng=pt>. Acesso em: 20 mar. 2023.