Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023

Wemerson Gonçalo[1] (Orcid: 0009-0006-8481-8599) (wemerson.goncalo@upe.br)
Maria Clara de Souza[1] (Orcid: 0000-0002-2969-6860) (mariaclara.souza@upe.br)
Wellington Pinheiro dos Santos[2] (Orcid: 0000-0003-2558-6602) (wellington.santos@ufpe.br)
Fábio Henrique Cavalcanti de Oliveira[1] (Orcid: 0000-0002 0181-7624) (fabiohcavalcanti@upe.br)

[1] Faculdade de Ciências Médicas, Universidade de Pernambuco. Recife-PE, Brasil.
[2] Departamento de Engenharia Biomédica, Universidade Federal de Pernambuco. Recife-PE, Brasil.

Resumo: **Objetivo**: Identificar a literatura científica acerca das estratégias de regulação das tecnologias de informação aplicadas na área da saúde para proteção dos dados dos usuários. **Metodologia**: Foi conduzida uma revisão integrativa da literatura, consultando as bases de dados BVS, Scielo e Web of Science, utilizando descritores em português e inglês, delimitando os artigos com ênfase nas tecnologias e LGPD. **Resultados**: A revisão resultou na identificação de 658 artigos, e considerando os critérios de seleção, foram selecionados cinco artigos que se relacionam diretamente com a temática do estudo. As categorias foram sistematizadas e analisadas a partir de três perspectivas: incorporação de inteligência artificial e inovações em saúde; proteção de dados em saúde e seu entrelaçamento com a LGPD; e os aspectos operacionais e governança de informações em saúde. **Conclusões**: A implementação da saúde digital emerge como um desafio importante para a Saúde Coletiva, exigindo discussões sobre seu impacto nas políticas de saúde. A análise ressalta a importância da regulamentação abrangente das TICs na saúde e destaca desafios como a rápida evolução tecnológica, segurança de dados e políticas públicas. Regulamentações como a LGPD se mostram essenciais para proteger a privacidade e segurança dos usuários na saúde digital.

➤ **Palavras-chave:** Proteção de dados. Confidencialidade. Saúde digital. Tecnologias em saúde. Regulação governamental.

Recebido em: 19/03/2024 Revisado em: 09/02/2024 Aprovado em: 04/07/2024

DOI: http://dx.doi.org/10.1590/S0103-73312025350113pt

Editora responsável: Fernanda Mattioni Pareceristas: Maria Cristina Lima e Edmar Galiza dos Santos

Introdução

Nos últimos anos, os avanços tecnológicos têm impulsionado a área da saúde, promovendo melhorias significativas nos cuidados e serviços prestados aos pacientes. A crescente digitalização dos sistemas de saúde traz consigo um imenso potencial para impulsionar a promoção da saúde, enquanto também desempenha papel crucial na transformação dos sistemas de saúde, através de inúmeras estratégias, como o uso de prontuários eletrônicos, telemedicina e aplicativos de monitoramento da saúde (Antunes, 2021; OCDE, 2017).

Mesmo com todo o potencial, a incorporação de tecnologias na área da saúde encontra obstáculos relacionados "à qualidade dos dados, segurança, acessibilidade, privacidade e preocupações regulamentares" (Sharma *et al.*, 2018, p. 2.681). Nesse contexto, a utilização de inteligência artificial, *big data* e internet das coisas na saúde amplia as possibilidades de análise e diagnóstico, mas aumenta a complexidade de assegurar a confidencialidade e integridade dos dados sensíveis. Recomenda-se compreender como as estratégias de regulação podem acompanhar esse cenário em constante evolução e adaptar-se às demandas emergentes (Leme; Blank, 2020).

A proteção de dados é uma questão crucial no contexto da saúde digital, e a regulação das tecnologias de informação é fundamental para garantir a segurança e privacidade das informações dos pacientes, sobretudo por meio da interoperabilidade que pode expor ainda mais os dados particulares (Pelinson, 2022; Hira, 2012). Conforme destacado por Santana *et al*. (2020), a crescente quantidade de dados gerados pelas tecnologias de informação requer abordagens regulatórias sólidas que protejam efetivamente os dados dos usuários, normas de armazenamento e acesso previstos em lei, promovendo a confiança no uso dessas tecnologias na saúde.

A Lei Geral de Proteção de Dados (LGPD) tornou-se um marco regulatório importante no Brasil. A LGPD tem como objetivo principal proteger os direitos fundamentais de privacidade e liberdade dos usuários, impondo obrigações e responsabilidades para as organizações que lidam com dados pessoais. Sua aplicação na área da saúde é essencial para garantir que as informações dos pacientes sejam tratadas de forma ética e segura, protegendo os direitos essenciais da pessoa humana (Brasil, 2018; Leme; Blank, 2020).

Telles *et al.* (2021) destacam que os dados sensíveis dos usuários dizem respeito:

> [...] à intimidade da pessoa e, se revelados, podem gerar discriminação ou perseguição. São relativos à saúde ou à vida sexual, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados genéticos ou biométricos. Contemplam informações diversas, incluindo, tipo sanguíneo, histórico de saúde, doenças pré-existentes, laudo do exame médico admissional no caso de funcionários, entre outros. (p. 14)

O Ministério da Saúde (MS), alinhado com as diretrizes da Organização Mundial da Saúde (OMS), abraçou a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28), orientando o progresso da saúde digital no país. A segunda prioridade da ESD28 destaca a busca por maior confiabilidade e segurança das informações dos pacientes, estabelecendo conexão direta entre a saúde digital e a preocupação com dados particulares. Isso ressalta a importância intrínseca da proteção de dados e a necessidade de estratégias regulatórias sólidas para proteger a privacidade e a segurança das informações dos usuários na área da saúde digital, refletindo o compromisso do MS em impulsionar a inovação digital na saúde ao mesmo tempo que assegura a integridade dos dados sensíveis dos pacientes (Rachid *et al*., 2023; OMS, 2021; Brasil, 2020).

No panorama atual da transformação digital na área da saúde, destaca-se a relevância da atuação da Secretaria de Informação e Saúde Digital (SEIDIGI), estabelecida por intermédio do Decreto nº 11.358/23, como um órgão essencial para tutelar a esfera digital, em colaboração com os princípios norteadores da LGPD, visando proteger as informações e a privacidade dos pacientes. A abordagem estratégica adotada por essa entidade transcende não apenas a conexão e otimização dos serviços de saúde por meio da tecnologia, mas também assume o papel de elo entre as inovações tecnológicas e as necessidades tangíveis do nosso sistema de saúde (Brasil, 2023).

Diante do exposto, a implementação de uma área dedicada à saúde digital em nível nacional tem o potencial de estar associada à melhoria da segurança dos dados pessoais dos cidadãos. Nesse contexto, o objetivo geral deste estudo consiste em identificar a literatura científica acerca das estratégias de regulação das tecnologias de informação aplicadas na área da saúde para proteção dos dados dos usuários. Para isso, busca-se descrever as estratégias de regulação utilizadas para assegurar a proteção de dados e apresentar desafios na regulação das tecnologias.

Metodologia

Esta é uma revisão integrativa da literatura sobre a regulação das tecnologias em saúde para proteção de dados sensíveis dos usuários. A revisão integrativa da literatura utiliza as evidências encontradas dentro da própria literatura visando ao conhecimento científico, com o efeito de qualidade e bom custo-benefício e buscando a avaliação dos resultados (Sobral; Campos, 2012). Sendo assim, a metodologia integrativa se divide em seis partes. Na primeira, formulou-se a pergunta norteadora utilizando o método PICo (P- população; I- Interesse; Co- contexto). Neste trabalho, "P" está relacionado aos usuários do sistema de saúde; "I", proteção de dados sensíveis; e "Co", à regulação das tecnologias em saúde. Levanta-se a seguinte pergunta: "Como as estratégias de regulação das tecnologias podem garantir a proteção de dados sensíveis dos usuários na área da saúde?"

Na segunda parte, ocorreu a pesquisa bibliográfica no Portal de Periódicos da CAPES através do acesso ao CAFe, utilizando três bases de dados digitais: Biblioteca Virtual em Saúde (BVS), Scientific Electronic Library on Line (SCIELO) e Web of Science (WoS). Para tanto, utilizaram-se os descritores disponíveis no DeCS (Descritores em Ciências de Saúde) e suas variações nas línguas portuguesa e inglesa, juntamente com os operadores booleanos AND e OR, que "são usados nas buscas para possibilitar a ampliação ou a restrição (refinamento) dos resultados" (Silva; Menezes, 2001, p. 55). Formou-se, assim, a estratégia de busca, utilizando combinações de descritores: "regulamentação governamental" OR regulação AND confidencialidade OR "*confidentiality*" AND "proteção de dados" OR "*data protection*" AND "sistema único de saúde" OR "*Brazilian health system*" AND "tecnologias em saúde" OR "*health technologies*".

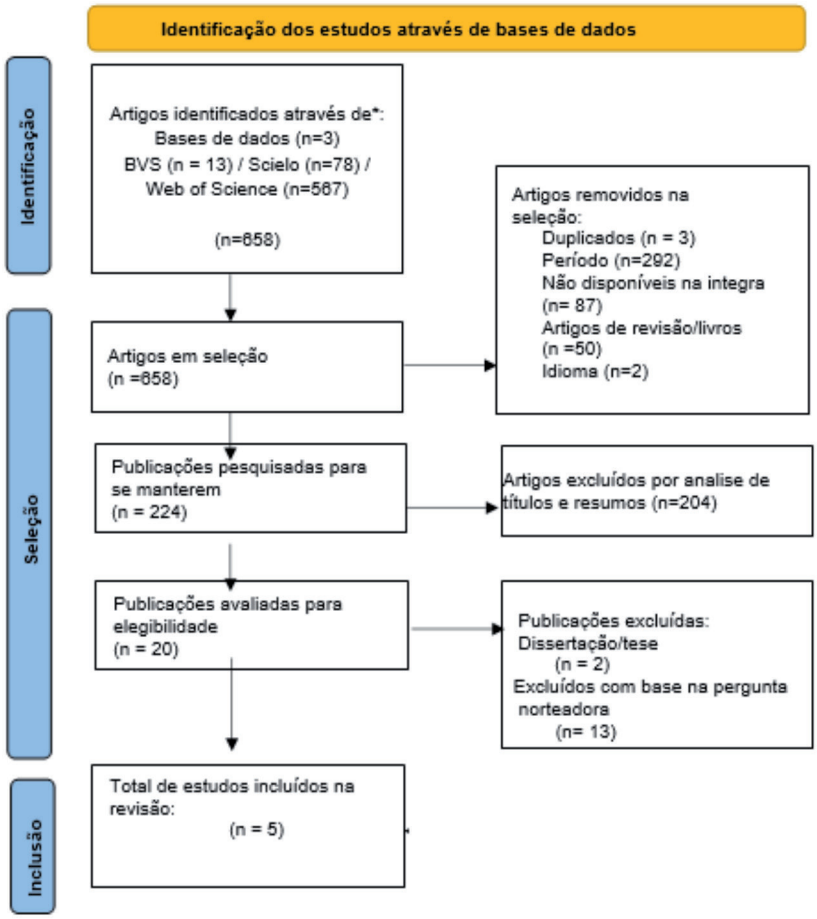
Os fatores de seleção usados para selecionar a amostra foram: estudos dos últimos seis anos, que contenham uma metodologia positiva, levando em consideração as áreas de interesse do tema, sendo textos completos, disponíveis *on-line*. Esse período foi escolhido devido a sua crescente frequência dentro da saúde e à criação da Lei Geral de Proteção de Dados (LGPD) em 2018, que trouxe novos marcos regulatórios na proteção de dados pessoais.

Foram feitas leituras exploratórias dos títulos e resumo dos artigos, seguidas de leitura flutuantes para verificar se eram adequados ao tema proposto. Em seguida, foi realizada a literatura seletiva, ou seja, uma leitura mais aprofundada do texto

completo do artigo. Dessa literatura foram excluídos os estudos não relacionados ao tema de pesquisa. Em seguida, após determinação da amostra final, foi realizada uma leitura analítica, com o intuito de hierarquizar e resumir as informações contidas nos artigos selecionados em resposta aos objetivos da pesquisa.

Para tanto, foram selecionados 13 artigos na base de dados da BVS, 567 artigos na Web of Science e 78 artigos na Scielo. Foram excluídos 633 artigos, pelos critérios de título, resumo, metodologia, duplicados e tipos de documento, totalizando cinco artigos selecionados para esta pesquisa (Figura 1).

Figura 1. Fluxograma de buscas nas bases de dados



Fonte: Autoria própria.

No que se refere aos critérios de inclusão, participaram desta pesquisa artigos publicados em português e inglês, indexados nas bases de dados nos últimos seis anos (2018-2023), disponíveis na íntegra, descrevendo temas relevantes para a revisão. Para tanto, optou-se pela exclusão de artigos que não abordavam sobre a temática estudada, assim como monografias, dissertações, teses, manuais, revisões da literatura, artigos de opinião, editoriais, artigos de conferência.

Na terceira etapa, a qual visa organizar a coleta dados, utilizaram-se planilhas Excel para a coleta de dados e registro das informações consideradas mais importantes para os objetivos deste estudo. Portanto, a amostra final foi organizada em ordem decrescente de ano de publicação.

Na quarta etapa, foi realizada uma análise crítica dos estudos selecionados, isto é, a análise e síntese de dados extraídos dos artigos de forma descritiva, possibilitando a enumeração, descrição e classificação de dados, a fim de reunir o conhecimento gerado sobre o tema explorado na revisão. A quinta etapa teve como intuito mostrar os principais resultados dos artigos escolhidos para a pesquisa, verificando os dados, comparando e identificando lacunas de sugestões para as próximas pesquisas. Por fim, a sexta etapa caracterizou-se pela apresentação da revisão integrativa e a síntese de conhecimento, com o intuito de avaliar criticamente os resultados. Desta forma, as informações importantes e detalhadas são apresentadas sem omitir qualquer evidência relacionada.

Resultados

Foram selecionados cinco artigos para fazer parte da amostra final da revisão integrativa, após aplicação de todos os critérios e leitura. Para sistematizar e analisar os artigos, foi elaborado um quadro, contemplando os seguintes aspectos, considerados pertinentes: autores; título do artigo; resultados; recomendações/ conclusões (Quadro 1).

Quadro 1. Síntese dos estudos selecionados por ordem decrescente de ano

Autores/Ano	Título do Artigo	Resultados	Recomendações/Conclusões
Dourado & Aith / 2022	A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais	O estudo destaca que são identificados seis princípios-chave para a regulação dos sistemas de Inteligência Artificial (IA) na saúde: autonomia, não-maleficência/beneficência, transparência, responsabilidade, equidade e sustentabilidade. A falta de transparência na IA deve persistir, pelo menos por algum tempo, devido à complexidade e ao custo de projetar sistemas de IA que possam explicar suas previsões. A transparência dos algoritmos é essencial para garantir a proteção da autonomia humana, requisitos regulatórios de segurança e eficácia, e prestação de contas no uso da IA na saúde.	O estudo recomenda que os obstáculos para desenvolver uma IA explicável na saúde sejam reconhecidos e ponderados na construção de mecanismos regulatórios que considerem os limites da explicabilidade e garantam o direito à explicação e à revisão de decisões automatizadas na assistência à saúde. O estudo recomenda que a regulação da IA na saúde no Brasil leve em consideração a LGPD, os princípios éticos, os limites da IA explicável e a necessidade de transparência dos algoritmos, garantindo o direito à explicação e à revisão de decisões automatizadas na assistência.
Bertoni *et al.* / 2022	Internet das Coisas de Saúde: aplicando IoT, interoperabilidade e aprendizado de máquina com foco no paciente	- A adoção de tecnologias digitais na saúde proporciona vantagens como agilidade no acesso às informações, troca de informações com centros especializados. As novas tecnologias em saúde podem ser combinadas para reduzir custos e melhorar a qualidade das intervenções e dos desfechos dos pacientes. - Os sistemas de saúde enfrentam desafios no compartilhamento e integração desses dados. A utilização de modelos distribuídos de interoperabilidade de informações e redes colaborativas de compartilhamento de dados de pacientes podem ser soluções para esse problema.	Garantir a segurança e privacidade dos dados pessoais dos usuários, removendo barreiras de entrada para o compartilhamento constante de dados. Isso inclui o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e o uso de tecnologias como criptografia homomórfica e *blockchain* para proteger as informações dos pacientes.

continua...

Autores/Ano	Título do Artigo	Resultados	Recomendações/Conclusões
Camara *et al.* / 2021	Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados	- O Sistema Único de Saúde (SUS) brasileiro vem investindo em tecnologias de Internet das Coisas (IoT) para coletar dados de pacientes. - Ainda existem fragilidades em termos de privacidade do usuário no sistema SUS, sendo necessária uma mudança na estratégia tecnológica e na governança. - A implementação do PDS tem algumas restrições metodológicas em relação aos direitos dos cidadãos ou à eficiência do Estado, mas é um passo em direção ao empoderamento civil e a uma melhoria exigida por lei em relação à privacidade e proteção de dados pessoais.	A solução de armazenamento de dados pessoais (PDS) pode capacitar os usuários, dando-lhes maior controle e transparência sobre o tratamento de seus dados. No entanto, a implementação do PDS em um sistema como o usado pelo Departamento de Informática do Sistema Único de Saúde (SUS) brasileiro pode comprometer a precisão dos dados usados nas políticas públicas, bem como comprometer alguns direitos dos cidadãos.
Donida *et al.* / 2021	Making the COVID-19 Pandemic a Driver for Digital Health: Brazilian strategies	O Brasil implementou várias estratégias digitais de saúde para combater a Covid-19, incluindo a criação do Conecte SUS, uma plataforma para armazenar todos os dados de saúde de um indivíduo ao longo de sua vida, e a Rede Nacional de Dados de Saúde (RNDS) para compartilhar dados de saúde. Assim, a LGPD é importante para garantir que os dados sejam coletados e usados de forma segura, definindo as pessoas como proprietárias exclusivas de seus dados e determinando os dados de saúde como dados confidenciais. No entanto, a divulgação de determinadas informações em benefício da comunidade ou por motivos de saúde pública é permitida, sem prejuízo da intimidade e privacidade do paciente, por meio do anonimato.	O Brasil vem trabalhando para transformar digitalmente o setor de saúde desde o lançamento da estratégia brasileira de saúde digital. A pandemia da Covid-19 acelerou essa transformação e criou enormes desafios para os tomadores de decisão. Ainda há um longo caminho a percorrer antes de alcançar a implementação da saúde digital devido a questões tecnológicas e territoriais, financeiras e éticas.

continua...

Autores/Ano	Título do Artigo	Resultados	Recomendações/Conclusões
Aragão Schiocchet / 2020	Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde	Os principais resultados do artigo indicam que o Sistema Único de Saúde (SUS) no Brasil será significativamente impactado pela Lei Geral de Proteção de Dados (LGPD), particularmente em termos de proteção de dados confidenciais e garantia de boas práticas em segurança da informação.	A conclusão é que o SUS precisará tomar medidas rápidas e diligentes para cumprir a LGPD, a fim de proteger dados confidenciais e garantir boas práticas em segurança da informação. O artigo sugere que o SUS precisará revisar sua estrutura existente e se adaptar às novas exigências para cumprir a lei. Destaca também a necessidade de padronização e normalização dos métodos de coleta de dados no SUS, bem como a importância de obter o consentimento e anonimizar os dados coletados anteriormente.

Fonte: autoria própria.

Discussão

Tecnologias no SUS: incorporação de Inteligência Artificial e inovações em saúde

Nos últimos anos, a interseção entre as Tecnologias da Informação e Comunicação (TICs) e o setor de saúde tem gerado avanços notáveis, impulsionando discussões sobre como incorporar tais inovações de maneira responsável e eficaz. A discussão sobre a incorporação de Inteligência Artificial (IA) e Internet das Coisas (IoT) no Sistema Único de Saúde (SUS) e sua interação com a proteção de dados dos usuários é um tema de crescente relevância e complexidade.

A pesquisa conduzida por Camara *et al*. (2021) explora como a aplicação da IoT e do *blockchain* no SUS pode endereçar a proteção dos dados sensíveis dos pacientes, em conformidade com a Lei Geral de Proteção de Dados (LGPD). A literatura aponta a necessidade de mecanismos confiáveis de armazenamento e compartilhamento de informações sensíveis. Dourado e Aith (2022) ressaltam que a regulação da IA na saúde é um tema intrinsecamente ligado à LGPD, devendo ser cuidadosamente equilibrada entre a inovação tecnológica e a proteção dos direitos dos pacientes.

Nesse contexto, Bertoni *et al*. (2022) discutem a aplicação da IoT e do aprendizado de máquina focados no paciente, realçando como a coleta massiva de dados em tempo real possibilita avanços diagnósticos e terapêuticos. A integração dessas

tecnologias, no entanto, suscita preocupações sobre privacidade e segurança. A obra de Aragão e Schiocchet (2020) amplia a discussão, enfatizando o desafio do SUS em adotar a LGPD, demandando reestruturação dos processos e conscientização dos profissionais de saúde.

O contexto pandêmico também acelerou a necessidade de soluções digitais na saúde. Donida *et al*. (2021) analisam as estratégias brasileiras para saúde digital durante a pandemia de Covid-19. É crucial ressaltar que a transição para tecnologias digitais não deve comprometer a segurança e privacidade dos pacientes. São imprescindíveis políticas inclusivas, esforços de base e liderança efetiva para assegurar aos cidadãos a preservação de sua privacidade e segurança (Pelinson, 2022). A literatura reforça que a proteção de dados deve ser intrínseca ao *design* das soluções tecnológicas.

Antunes (2021) salienta que a integração de tecnologias proporciona um terreno fértil para o desenvolvimento e utilização de ferramentas inovadoras. Essa transição, entretanto, requer um esforço coordenado e colaborativo para que os sistemas de saúde possam, de fato, aproveitar de maneira eficaz e eficiente esses avanços. Esse empenho entre diferentes sujeitos tem papel crucial para priorizar intervenções na área da saúde, que vão além da prevenção, garantindo que pacientes tenham acesso a serviços de qualidade que sejam capazes de atender às demandas reais da sociedade. Assim, Camara *et al*., (2021) concordando com Bertoni *et al*. (2022), indicam a utilização das tecnologias de *blockchain*, *personal data stores* (PDS) e criptografia como uma abordagem fundamental para preservar a privacidade dos usuários e o controle sobre seus próprios dados, auxiliando os sistemas de saúde na agilidade de captação, acesso e troca de informações em rede.

Dessa forma, a discussão acerca das tecnologias na saúde transcende a simples adoção de inovações. Ela coloca em pauta uma transformação profunda que requer não apenas a compreensão das ferramentas em si, mas também uma visão ampla e sensível sobre as implicações éticas, legais e sociais que permeiam esse cenário em constante evolução (Dourado; Aith, 2022).

A evolução das tecnologias no SUS e a proteção de dados dos usuários representam uma conjuntura desafiadora. A discussão entre a busca por inovação e a manutenção da privacidade é crucial. A convergência entre o avanço das tecnologias de saúde e a proteção dos dados pessoais se torna um elemento vital para prevenir acessos não autorizados e uso indevido de informações sensíveis, preservando a dignidade dos pacientes em meio à revolução digital na saúde.

Proteção de dados em saúde e seu entrelaçamento com a LGPD

Antes da criação da LGPD em 2018, o cenário jurídico brasileiro carecia de um complexo normativo unificado para a proteção de dados pessoais, sendo regulamentado por diversas leis setoriais, como o Marco Civil da Internet, a Lei de Acesso à Informação Pública e outras (Mendes, 2019). Entretanto, essas leis demonstravam fragilidades quanto à proteção do titular dos dados. A LGPD, aliada a outras legislações como a Lei Orgânica da Saúde e códigos éticos, passou a assegurar não apenas a privacidade, mas também a autodeterminação informativa, concedendo a cada indivíduo o direito de gerir seus próprios dados.

A discussão sobre a proteção de dados na área da saúde, especialmente no contexto da LGPD, tem evoluído de maneira complexa e multifacetada, sendo ampliada pela rápida expansão das tecnologias de saúde digital. A interseção entre LGPD, IoT, *blockchain* e IA traz desafios e oportunidades significativas para o campo da saúde. Autores como Camara *et al*. (2021) e Bertoni *et al*. (2022) enfatizam a necessidade de incorporar princípios de privacidade e segurança desde o *design* de soluções de IoT e *blockchain*, visando à conformidade com a LGPD. No entanto, o artigo de Donida *et al*. (2021) destaca como a pandemia de Covid-19 impulsionou a adoção acelerada de tecnologias digitais na saúde, levantando questões urgentes sobre a proteção de dados em momentos de crise.

A LGPD, como um marco regulatório abrangente para a proteção de dados pessoais, assume papel central em moldar a implementação de tecnologias digitais na área da saúde. Obras abordam a complexidade da adaptação do SUS às diretrizes da LGPD, ressaltando a necessidade de garantir a privacidade e a segurança dos dados de saúde no contexto brasileiro (Aragão; Schiocchet, 2020; Dourado; Aith, 2022). A integração com as tecnologias emergentes também é discutida por Santana *et al*. (2020), que destacam a importância de empoderar os pacientes a controlar o uso de suas informações de saúde, alinhando-se com os princípios de autonomia e dignidade.

O aumento da telemedicina e o uso de aplicativos de rastreamento de contatos tornam evidente a necessidade de equilibrar a inovação tecnológica com a privacidade individual. Antunes (2021) ressalta essa dicotomia, enfatizando que a interconexão de dispositivos IoT também aumenta os riscos de ciberataques, destacando a importância da segurança cibernética em paralelo com a proteção de dados, uma vez que o manuseio de informações sensíveis exige protocolos rigorosos para prevenir o vazamento, acesso não autorizado e uso indevido.

O vazamento de dados sensíveis dos usuários pode ter profundas implicações no processo de discriminação, especialmente quando se trata de informações que possuem potencial discriminatório ou lesivo para seus titulares (Doneda, 2010). Isso se torna ainda mais relevante quando se considera a correlação entre o tratamento de dados sensíveis e as normas constitucionais de igualdade (Rodotá, 2003). "O uso inadequado de dados de saúde pode levar à discriminação de grupos historicamente marginalizados, dificultando sua superação de situações prejudiciais, como a recusa de emprego e de acesso a saúde" (Mendes; Marttiuzzo, 2019).

É importante ressaltar, contudo, que os dados pessoais em saúde também exercem função social positiva, como o controle de epidemias e a melhoria do sistema de saúde como um todo. Aragão e Schiocchet (2020) apontam a necessidade de encontrar um equilíbrio entre a proteção da privacidade e a promoção de benefícios para a sociedade, considerando a dinâmica complexa entre dados pessoais, privacidade e informações de saúde. Nesse sentido, a regulação deve criar mecanismos que permitam a utilização responsável dos dados sem comprometer a privacidade e a dignidade dos indivíduos.

Análise, divulgação e uso de informações em saúde: aspectos operacionais e governança

A qualidade e a gestão das informações em saúde continuam a ser afetadas por desafios significativos, sendo o armazenamento de dados um dos fatores preponderantes. Conforme Camara *et al*. (2021), a crescente preocupação com a segurança das informações e a necessidade de estabelecer uma governança de dados sólida para proteger os dados pessoais emergem como elementos cruciais nesse contexto. Assim, a interligação entre a LGPD, a responsabilidade corporativa e a implementação de uma estrutura de governança de dados robusta desempenham papel central na análise, divulgação e utilização de informações em saúde.

Nesse sentido, o uso de sistemas de informação e outras tecnologias digitais em saúde pode modificar substancialmente a forma como os dados são coletados, tornando-os mais oportunos e permitindo melhor gestão da saúde e do planejamento. Como Dourado (2022) explicita, o exercício do direito à explicação na saúde depende de mecanismos que criem sistemas de inteligência artificial explicáveis e do reconhecimento dos limites da explicabilidade de algoritmos.

O campo da saúde representa um dos segmentos mais vulneráveis a incidentes de divulgação não autorizada de informações. Agentes maliciosos têm a capacidade de empregar técnicas de mineração de dados para identificar informações sensíveis e torná-las públicas (Abouelmehdi *et al*., 2018). Em um exemplo ocorrido em novembro de 2020, uma brecha de segurança no sistema do MS resultou na exposição de dados pertencentes a 16 milhões de indivíduos que receberam diagnóstico suspeito ou confirmado de Covid-19. Além disso, em um incidente subsequente, no espaço de um mês, dados pessoais de mais de 200 milhões de cidadãos brasileiros, incluindo beneficiários do SUS e clientes de seguradoras de saúde, foram inadvertidamente expostos (Bertoni, 2020).

O MS criou a Política Nacional de Informação e Informática em Saúde (PNIIS), com o intuito de orientar o sistema de saúde brasileiro diante da implementação das novas tecnologias para formular um Sistema Nacional de Informação em Saúde (SNIS). Sendo assim, entre os princípios que norteiam o PNIIS, está o princípio da confidencialidade, sigilo e privacidade da informação de saúde pessoal como direito de todo indivíduo que possui ligação direta com a proteção de dados pessoais (Brasil, 2016).

O Brasil deu um grande passo em direção à adoção da saúde digital, criando e implementando iniciativas importantes; no entanto, essas iniciativas ainda não abrangem todo o sistema de saúde (Donida *et al*., 2021). A qualidade dos dados é outra faceta relevante. Bertoni *et al*. (2022) realçam a necessidade de garantir a qualidade dos dados coletados e compartilhados, de modo a sustentar o planejamento e aprimoramento dos serviços de saúde, resultando na criação de uma base legal sólida para a proteção dos dados de saúde.

A importância da governança de dados é abordada por autores como Santos (2020), que salienta a necessidade de se estabelecer uma estrutura regulatória abrangente, abordando aspectos de segurança cibernética, responsabilidade, ética e transparência. Dourado e Aith (2022) contribuem ao destacar a relação entre inteligência artificial na saúde e a LGPD como um marco regulatório inicial para a regulamentação da tecnologia. Ademais, a transparência na comunicação das estratégias de segurança dos dados reforça a importância de estabelecer confiança com os *stakeholders* e o público (Donida *et al*., 2021).

A relevância dos dados anonimizados é abordada por Santos (2020), que destaca a necessidade de uma análise crítica da proteção e promoção de dados de saúde,

mesmo quando são submetidos à anonimização. A autora examina a eficácia dos direitos fundamentais na sociedade da informação, ressaltando a complexidade da relação entre a governança de dados e os dados anonimizados. Essa discussão acrescenta um olhar crítico e reflexivo à aplicação da técnica de anonimização.

A técnica de anonimização de dados ganha destaque nesse contexto, representando uma abordagem fundamental para minimizar os riscos associados à exposição de dados sensíveis. O processo de anonimização envolve a remoção ou transformação de informações que possam identificar diretamente um indivíduo, permitindo que as informações sejam usadas sem que a identidade das pessoas seja comprometida. Esse procedimento é crucial para atender tanto às necessidades de análise de dados quanto à manutenção da privacidade dos pacientes.

A interligação entre a proteção de dados sensíveis e a técnica de anonimização é uma questão multifacetada. Por um lado, a anonimização permite o compartilhamento seguro de informações de saúde entre profissionais, pesquisadores e instituições. No entanto, é vital reconhecer que, apesar dos esforços de anonimização, existem desafios potenciais, como a importância de considerar não apenas as técnicas de anonimização, mas também o enquadramento legal para as práticas de compartilhamento e análise de dados (Camara *et al*., 2021).

Vale mencionar que a anonimização, embora seja uma ferramenta valiosa, não está imune a desafios. Técnicas avançadas de reidentificação, por exemplo, podem comprometer a eficácia da técnica. Portanto, uma abordagem cautelosa e em constante atualização se faz necessária para preservar a segurança dos dados e a privacidade dos indivíduos.

Considerações finais

A instauração da saúde digital apresenta um substancial desafio à área da Saúde Coletiva, demandando a imperativa abertura de discussões acerca dos impactos imediatos das tecnologias digitais nas políticas de saúde. Este trabalho explorou a interseção entre saúde digital e proteção de dados pessoais, investigando as estratégias de regulação das tecnologias de comunicação aplicadas à saúde. A hipótese inicial, de que uma área específica dedicada à saúde digital em nível nacional poderia fortalecer a segurança dos dados pessoais dos cidadãos, foi confirmada ao longo da revisão.

Nesse intento, analisa-se a estratégia brasileira em saúde digital a partir de três perspectivas: incorporação de inteligência artificial e inovações em saúde; proteção de dados em saúde e seu entrelaçamento com a LGPD; e os aspectos operacionais e governança de informações em saúde. Como limitações do estudo, aponta-se que esta pesquisa foi restrita ao recorte histórico de 2018 a 2023, não englobando, portanto, o arcabouço legal anterior à LGPD em seu escopo. Desta forma, abre-se espaço para desenvolvimento de novas pesquisas documentais que abarquem as novas configurações legais decorrentes desta temática.

A análise destaca a importância de uma abordagem cautelosa e abrangente à regulamentação das TICs em saúde. O fortalecimento deste campo na Saúde Coletiva mostra-se necessário para enfrentar os desafios emergentes e garantir que as políticas regulatórias protejam efetivamente os direitos fundamentais de todos. Constata-se a existência de desafios, abrangendo desde a rápida evolução tecnológica até a necessidade de harmonizar as normas regulatórias, garantir a transparência na gestão dos dados, proteger contra ameaças cibernéticas em constante evolução e desenvolver políticas públicas consistentes.

À medida que a saúde digital continua a desempenhar papel cada vez mais central em nosso sistema de saúde, torna-se imperativo que as políticas públicas e as regulamentações acompanhem esse progresso, colaborando de forma sinérgica para criar um ambiente seguro e confiável para todas as partes envolvidas, na competência de supervisionar as atividades das entidades do setor. Evidencia-se que a regulação é fundamental na preservação dos dados dos usuários na esfera da saúde digital. Regulamentações como a LGPD estabelecem o enquadramento legal necessário para resguardar a privacidade e a segurança das informações dos pacientes. Nesse contexto, esta revisão contribui para orientar futuras discussões sobre como moldar o futuro da saúde digital, priorizando a proteção de dados e a segurança dos usuários como elementos centrais.[1]

Agradecimentos

Agradecemos à Faculdade de Ciências Médicas da Universidade de Pernambuco, por fomentar a pesquisa que originou este artigo.

Referências

ABOUELMEHDI, K.; BENI-HESSANE, A.; KHALOUFI, H. Big healthcare data: preserving security and privacy. *Journal of Big Data*, El Jadida, v. 5, n. 1, p. 1-18, 2018. Disponível em: https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-017-0110-7.pdf.

ANTUNES, C. P. A regulação dos dispositivos de recolha e processamento de dados em saúde. Lisboa: Universidade de Lisboa, 2021. Disponível em: <https://repositorio.ul.pt/bitstream/10451/52892/1/MICF_Catarina_Antunes.pdf>. Acesso em: 2 ago. 2023.

ARAGÃO, S. M. de; SCHIOCCHET, T. 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. DOI: 10.29397/reciis.v14i3.2012. Acesso em: 1 ago. 2023.

BERTONI, A. P. S.; RODRIGUES, V. F.; ZEISER, F. A.; *et al*. Internet das Coisas de Saúde: aplicando IoT, interoperabilidade e aprendizado de máquina com foco no paciente. [s.l.: s.n.], 2022. Disponível em: <https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/105/465/738-1?inline=1>. Acesso em: 1 ago. 2023.

BERTONI, E. O novo vazamento de dados na Saúde. E suas consequências. *Nexo*, 2 dez. 2020. Disponível em: https://www.nexojornal.com.br/expresso/2020/12/02/O-novo- vazamento-de-dados-na-Saúde.-E-suas-consequências. Acesso em: 1 ago. 2023.

BRASIL. Lei nº 13709, de 18 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. *Diário Oficial da União*, Brasília, 20 set. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4591.htm. Acesso em: 14 ago. 2023.

BRASIL. Ministério da Saúde. *Estratégia de Saúde Digital para o Brasil 2020-2028*. Brasília: MS, 2020.

BRASIL. Ministério da Saúde. *Portaria GM/MS 1.001*, de 18 de maio de 2021. Altera a Portaria de Consolidação n. 1, de 28 de setembro de 2017, que dispõe sobre o Comitê de Informação e Informática em Saúde - CIINFO/ MS e institui o Comitê Executivo de TIC - CETIC/MS, no âmbito do Ministério da Saúde [Internet]. 2021. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2021/prt1001_24_05_2021.html

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Monitoramento e Avaliação do SUS. *Política Nacional de Informação e Informática em Saúde*. Brasília: Ministério da Saúde, 2016. 56 p. il.

CAMARA, M. A. A. *et al*. Internet das Coisas e *blockchain* no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. *Cadernos Ibero-Americanos de Direito Sanitário*, v. 10, n. 1, p. 93-112, 2021. DOI: 10.17566/ciads.v10i1.657. Acesso em: 1 ago. 2023.

DONEDA, D. A *proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor; Brasília: SDE/DPDC, 2010.

DONIDA, B.; DA COSTA, C. A.; SCHERER, J. N. Making the COVID-19 Pandemic a Driver for Digital Health: Brazilian Strategies. *JMIR Public Health and Surveillance*, v. 7, n. 6, p. e28643, 2021. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8244723/>. Acesso em: 1 ago. 2023.

DOURADO, D. de A.; AITH, F. M. A. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais. *Revista de Saúde Pública*, v. 56, p. art. 80, 2022. Disponível em: https://www.scielo.br/j/rsp/a/k38jGvJdbQSYN4MpzGZpfXw/?format=pdf&lang=pt. Acesso em: 1 ago. 2023.

HIRA, A. Y. *Saúde Digital*: novo paradigma da convergência das tecnologias de informação para a área da saúde. São Paulo, 2012.

LEME, R. S.; BLANK, M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. *Cadernos Ibero-Americanos de Direito Sanitário*, v. 9, n. 3, p. 210-224, jul-set. 2020. http://dx.doi.org/10.17566/ciads.v9i3.690. Acesso em: 14 ago. 2023.

MENDES, L. S. A lei geral de proteção de dados pessoais: um modelo de aplicação em três níveis. *Revista dos Tribunais*, ed. esp. LGPD 2019, p. 35-56.

MENDES, L. S.; MARTTIUZZO, M. Discriminação algorítmica: conceito, fundamento legal e tipologia. Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias. *RDU*, Porto Alegre, v. 16, n. 90, p. 39-64, 2019.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *Health ministerial meeting*. The next generation of health reforms. Oecd 57 [Internet].2017;(January):1-17. Disponível em: http://www.oecd.org/health/ministerial/ministerial-statement-2017.pdf. Acesso em: 14 ago. 2023.

PELINSON, S. C. Os Desafios na troca de informação em Saúde (Interoperabilidade) em um ambiente organizacional de Cooperativas Médicas. *FGV Repositório Digital*, 2022. Disponível em: bibliotecadigital.fgv.br/dspace/handle/10438/32189. Acesso em: 6 ago. 2023.

RACHID, R. *et al.* Saúde digital e a plataformização do Estado brasileiro. Ciência & Saúde Coletiva [online]. v. 28, n. 7, p. 2143-2153. <https://doi.org/10.1590/1413-81232023287.14302022>. Acesso em: 14 ago. 2023.

RODOTÁ, S. Democracia y protección de datos. *Cuadernos de Derecho Público*, n. 19-20, mayo-diciembre 2003.

SANTANA, A. P. de; SANTANA, J. D. L. C.; SILVA, P. C. da. A influência da tecnologia da informação no tratamento de dados na área da saúde seguindo as normas da Lei Geral de

Proteção de Dados (LGPD), *Repositório Anima e Educação*, disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/32418/1/20222_%20ECP_JDLCS_%20APS.pdf>. Acesso em: 2 ago. 2023.

SANTOS, S. P. *A eficácia dos direitos fundamentais na sociedade da informação*. Uma análise acerca da proteção e promoção de dados em matéria de saúde. Disponível em: <http://repositorio.undb.edu.br/bitstream/areas/442/1/SAMANDA%20PEREIRA%20SANTOS.pdf>. Acesso em: 6 ago. 2023.

SHARMA, A. *et al*. Using Digital Health Technology to Better Generate Evidence and Deliver Evidence-Based Care. *J Am Coll Cardiol*., v. 71, n. 23, p. 2680-90, 2018.

SILVA, L. S.; MENEZES, E. M. *Metodologia da pesquisa e elaboração de dissertação*. Manual de orientação. Florianópolis, 2001. Disponível em: <http://www.scribd.com/doc/2367267/DA-SILVA-MENEZES-2001-Metodologia-da-pesquisa-e-elaboracao-de-dissertacao> Acesso em: 5 ago. 2023.

SOBRAL, F. R.; CAMPOS, C. J. G. Utilização de metodologia ativa no ensino e assistência de enfermagem na produção nacional: revisão integrativa. *Revista da Escola de Enfermagem da USP*, v. 46, n. 1, p. 208-218, 2012.

TELLES, E. T. G.; MARUCO, F. O. R.; DA SILVA, V. D. A implementação da Lei Geral de Proteção de Dados no Exercício Profissional na Área da Saúde. *Revjur*, São Paulo 2021. Disponível em: https://revista.unisal.br/lo/index.php/revdir/article/view/1535. Acesso em: 14 ago. 2023.

WORLD HEALTH ORGANIZATION. *Global strategy on digital health 2020-2025*. Geneva: WHO; 2021.

Nota

[1] W. Gonçalo e M. C. de Souza: participaram de todas as etapas de planejamento e construção da pesquisa, análise e interpretação dos dados e aprovou a versão final do manuscrito. W. P. dos Santos: contribuiu para a revisão crítica do conteúdo e aprovou a versão final do manuscrito. F. H. C. de Oliveira: participou de todas as etapas de planejamento e construção da pesquisa, análise e interpretação dos dados, revisão crítica do conteúdo e aprovou a versão final do manuscrito.

Abstract

Regulatory approaches to health data protection: an integrative review from 2018 to 2023

Objective: To identify scientific literature on regulatory strategies for information technologies applied in the health sector to protect user data. **Methodology**: An integrative literature review was conducted, consulting the databases BVS, Scielo, and Web of Science, using descriptors in Portuguese and English, focusing on articles related to technologies and LGPD. **Results**: The review identified 658 articles, and considering the selection criteria, 5 articles directly related to the study's theme were selected. Categories were systematized and analyzed from three perspectives: incorporation of artificial intelligence and innovations in health; protection of health data and its intertwining with LGPD; and operational aspects and governance of health information. **Conclusions**: The implementation of digital health emerges as a significant challenge for Public Health, requiring discussions about its impact on health policies. The analysis highlights the importance of comprehensive regulation of ICTs in health and underscores challenges such as rapid technological evolution, data security, and public policies. Regulations like LGPD are essential to protect the privacy and security of users in digital health.

➤ **Keywords:** Data protection. Confidentiality. Digital health. Health technologies. Government regulation.