FELIPE ANTÔNIO PARIZOTTO

CONCRETIZAÇÃO DO DIREITO SOCIAL À SAÚDE ATRAVÉS DE INOVAÇÕES TECNOLÓGICAS E AS FRONTEIRAS DO DIREITO À PRIVACIDADE: O CASO DO ASSISTENTE VIRTUAL SARA EM GUARAPUAVA-PR

Londrina

2024

FELIPE ANTÔNIO PARIZOTTO

CONCRETIZAÇÃO DO DIREITO SOCIAL À SAÚDE ATRAVÉS DE INOVAÇÕES TECNOLÓGICAS E AS FRONTEIRAS DO DIREITO À PRIVACIDADE: O CASO DO ASSISTENTE VIRTUAL SARA EM GUARAPUAVA-PR

Dissertação apresentada ao curso de Direito da Faculdades Londrina, como requisito para obtenção do título de Mestre em Direito

Orientador(a): Profa. Dra. Natália Maria Ventura da Silva Alfaya

Londrina

2024

Ficha de identificação da obra

P231c Parizotto, Felipe Antônio
Concretização do direito social à saúde através de inovações tecnológicas e as fronteiras do direito à privacidade: o caso do assistente virtual SARA em Guarapuava-pr / Felipe Antônio Parizotto- Londrina, 2025.
91 f.

Orientador: Natália Maria Ventura da Silva Alfaya.
Dissertação (Mestrado Profissional em Direito, Sociedade e Tecnologias) –Escola de Direito das Faculdades Londrina, 2025.
Inclui bibliografia.

1. Direito à saúde. 2. Inteligência artificial. 3. Privacidade de dados. 4. Assistente virtual SARA. I. Alfaya, Natália Maria Ventura da Silva. II. Faculdades Londrina. III. Título.

CDU: 614.253.83:342.721

Elaborado por: Fernanda Felite Teixeira
Bibliotecária CRB9 2165/O

FELIPE ANTÔNIO PARIZOTTO

CONCRETIZAÇÃO DO DIREITO SOCIAL À SAÚDE ATRAVÉS DE INOVAÇÕES TECNOLÓGICAS E AS FRONTEIRAS DO DIREITO À PRIVACIDADE: O CASO DO ASSISTENTE VIRTUAL SARA EM GUARAPUAVA-PR

Dissertação apresentada ao curso de Direito da Faculdades Londrina, como requisito para obtenção do título de Mestre em Direito.

COMISSÃO EXAMINADORA

Profa. Dra. Natália Maria Ventura da Silva Alfaya
Faculdades Londrina

Profa. Dra. Samia Moda Cirino
Faculdades Londrina

Profa. Dra. Marcella da Costa Moreira de Paiva
Faculdades Londrina

Londrina, 19 de novembro de 2024.

PARIZOTTO, F. A. **Concretização do direito social à saúde através de inovações tecnológicas e as fronteiras do direito à privacidade**: o caso do assistente virtual SARA em Guarapuava-PR. 2024. 90 f. Dissertação (Mestrado em Direito, Sociedade e Tecnologias) – Faculdades Londrina, Londrina, 2024.

RESUMO

O estudo tem como objetivo analisar como as inovações tecnológicas podem efetivar o direito social à saúde no Brasil, preservando a privacidade dos dados dos pacientes. O estudo divide-se em três eixos principais: a situação do direito à saúde no Brasil, a aplicação da tecnologia na saúde pública e os impactos dessas inovações na privacidade dos dados de saúde. A metodologia inclui revisão bibliográfica, documental e estudos de casos no Sistema Único de Saúde (SUS). O trabalho demonstra que as inovações tecnológicas podem melhorar a eficiência e a qualidade dos serviços de saúde, mas ressaltam-se preocupações com a segurança e privacidade dos dados, exigindo uma estrutura regulatória robusta e políticas eficazes de proteção de dados. A dissertação conclui ser possível harmonizar o uso de tecnologias avançadas com a preservação dos direitos fundamentais, desde que medidas adequadas garantam a privacidade e segurança dos dados. A assistente virtual SARA, implantada em Guarapuava-PR, é apresentada como um exemplo concreto de gestão tecnológica aplicada à saúde pública. Implementada inicialmente para enfrentar a demanda por atendimentos durante a pandemia de COVID-19, a SARA demonstrou ser eficaz na triagem, monitoramento e atendimento remoto de pacientes. Posteriormente, a plataforma foi ampliada para incluir monitoramento de pacientes crônicos, como aqueles com diabetes e hipertensão, além de funcionalidades como agendamentos, consultas online, emissão de atestados de vacinação, e suporte via call center. A expansão da SARA também incluiu atendimento a condições de saúde menos graves e a implementação de projetos específicos, como o atendimento a crianças com síndromes gripais e o rastreamento de autismo em crianças. A dissertação destaca a importância da continuidade da pesquisa para explorar os impactos sociais e econômicos dessas inovações e desenvolver mecanismos mais eficazes de proteção de dados.

Palavras-chave: direito à saúde; inteligência artificial; privacidade de dados; assistente virtual SARA.

PARIZOTTO, F. A. **Concretization of the social right to health through technological innovations and the frontiers of the right to privacy**: the role of the virtual assistant SARA in Guarapuava-PR. 2024. 90 p. Dissertation (Master's degree in Law, Society and Technologies) – Faculdades Londrina, Londrina, 2024.

ABSTRACT

The study aims to analyze how technological innovations can actualize the social right to health in Brazil while preserving patient data privacy. The study is divided into three main areas: the state of the right to health in Brazil, the application of technology in public health, and the impacts of these innovations on the privacy of health data. The methodology includes a literature review, documentary analysis, and case studies within the Unified Health System (SUS). The work demonstrates that technological innovations can improve the efficiency and quality of health services, but concerns about data security and privacy are highlighted, requiring a robust regulatory framework and effective data protection policies. The dissertation concludes that it is possible to harmonize the use of advanced technologies with the preservation of fundamental rights, provided that appropriate measures ensure data privacy and security. The virtual assistant SARA, implemented in Guarapuava, is presented as a concrete example of technological management applied to public health. Initially implemented to address the demand for care during the COVID-19 pandemic, SARA has proven effective in triage, monitoring, and remote patient care. Subsequently, the platform was expanded to include monitoring of chronic patients, such as those with diabetes and hypertension, as well as functionalities like scheduling, online consultations, issuance of vaccination certificates, and call center support. SARA's expansion also included addressing less severe health conditions and implementing specific projects, such as care for children with flu syndromes and autism tracking in children. The dissertation highlights the importance of continued research to explore the social and economic impacts of these innovations and to develop more effective mechanisms for data protection.

Key words: right to health; artificial intelligence; data privacy; virtual assistant SARA.

SUMÁRIO

1 INTRODUÇÃO

A concretização do direito social à saúde no contexto contemporâneo é um desafio complexo impulsionado pelas inovações tecnológicas que moldam e redefinem a sociedade. Este trabalho propõe uma análise da interseção entre o avanço tecnológico e o direito à saúde, focando no panorama brasileiro, na aplicação de tecnologias na saúde pública, na inserção da inteligência artificial e nos impactos na privacidade dos dados de saúde. A metodologia utilizada baseia-se em pesquisa qualitativa, com análise documental, sobretudo legislativa, e revisão bibliográfica, permitindo uma abordagem crítica e aprofundada do tema.

No Brasil, o direito à saúde é um dos pilares fundamentais da cidadania, refletindo a busca por condições dignas de vida e bem-estar. Diante das complexidades do sistema de saúde brasileiro, é essencial explorar como as inovações tecnológicas podem melhorar a qualidade e o acesso aos serviços de saúde.

A aplicação de tecnologia na saúde pública tem potencial para otimizar processos, melhorar diagnósticos e aumentar a eficácia dos tratamentos. A introdução da inteligência artificial promete transformar a abordagem das questões de saúde pública, oferecendo soluções personalizadas e diagnósticos mais rápidos e precisos.

No entanto, esses avanços tecnológicos trazem desafios éticos e jurídicos, especialmente no que se refere à privacidade dos dados de saúde. A coleta, armazenamento e compartilhamento de informações sensíveis devem ser equilibradas para garantir a integridade e a confidencialidade dos dados pessoais, respeitando o direito à privacidade.

Um exemplo significativo de gestão tecnológica na saúde pública é o assistente virtual SARA, implementado em Guarapuava-PR. Inicialmente projetado para atender à demanda durante a pandemia de COVID-19, a plataforma foi expandida para monitorar pacientes crônicos, agendar consultas, oferecer consultas online, emitir atestados de vacinação e fornecer suporte via call center. A SARA também foi utilizada em projetos específicos, como atendimento a crianças com síndromes gripais e rastreamento de autismo.

Este estudo apresentará propostas para aprimorar a proteção de dados, garantindo que os avanços tecnológicos sejam acompanhados por estruturas regulatórias robustas e políticas eficazes de segurança de dados. A aderência do

trabalho ao Mestrado Profissional em "Direito, Sociedade e Tecnologias" evidencia-se pela análise interdisciplinar dos desafios jurídicos e sociais que emergem do uso da tecnologia no setor de saúde. A dissertação explora como as inovações tecnológicas podem ajudar a concretizar o direito à saúde, respeitando ao mesmo tempo as fronteiras do direito à privacidade no contexto dos dados de saúde.

2 DO DIREITO À SAÚDE NO BRASIL

As primeiras ações de saúde pública implementadas pelos governantes ocorreram durante o período colonial com a vinda da família real para o Brasil (1808), com o início de um projeto de institucionalização do setor de saúde, assim como a regulamentação da prática médica profissional. Um destaque desse período foi a inauguração, no mesmo ano, da primeira faculdade de medicina do país, conhecida como Escola Médico-Cirúrgica, estabelecida em Salvador, Bahia (Baptista, 2007).

Contudo, durante a Primeira República (1889-1930), a saúde começou a ser objeto de intenso movimento intelectual e político, sendo vista como o "problema vital brasileiro"[1] , resultando em esforços para ampliar o acesso aos serviços médicos, implementar políticas de prevenção de doenças e promover a higiene pública (Lima; Fonseca; Hochman, 2005).

A incorporação da saúde entre os direitos sociais no Brasil foi primordialmente resultado da influência dos movimentos populares durante o período de redemocratização política no final dos anos oitenta. Nesse período marcante da história política brasileira, a mobilização popular desempenhou um papel fundamental na conquista do reconhecimento da saúde como um direito fundamental, refletindo a importância atribuída à garantia do bem-estar coletivo. Essa participação ativa foi crucial para a consolidação da saúde como um direito social, solidificando a base para o desenvolvimento de políticas públicas voltadas para o setor e demonstrando a vitalidade do engajamento cívico na construção das bases fundamentais da sociedade brasileira (Dallari, 2008).

Os direitos fundamentais formam o alicerce de toda sociedade democrática, sendo o conjunto de garantias e liberdades essenciais atribuídas a cada indivíduo. Tais direitos não são meros preceitos normativos; são assegurados como princípios estruturantes da República Federativa do Brasil, permeando todas as esferas da vida social e estabelecendo as bases para uma sociedade justa e igualitária.

Nesse contexto, a Constituição de 1988 (Brasil, 1988) emerge como um documento que estabelece um compromisso duradouro com a proteção dos direitos inerentes a cada cidadão, independentemente de sua posição ou status na sociedade.

[1] Tal expressão foi cunhada pelo escritor paulista Monteiro Lobato (1957).

Na evolução histórica, os direitos fundamentais são classificados originalmente em 3 dimensões. Insta salientar a existência de mais classificações, que não são consenso.

Uma primeira dimensão de direitos fundamentais traz os direitos individuais, também chamados de “liberdades públicas”. Surgiram com as revoluções francesa e americana, e receberam este nome porque foram os primeiros direitos tutelados nas legislações dos povos. O Estado aqui tem uma posição de abstenção com o dever principal de não fazer (não agir, status negativo). Na primeira dimensão encontram-se os direitos civis e políticos.

A segunda dimensão dos direitos fundamentais trata dos direitos sociais, focados na igualdade. O Estado ao invés de abster-se tem o dever principal de fazer, devendo atuar de forma a prover determinadas garantias aos particulares, como condições mínimas para uma vida digna. Aqui estão os direitos econômicos, sociais e culturais.

Na terceira dimensão dos direitos fundamentais buscou-se concretizar a proteção dos direitos transindividuais, abordando questões relacionadas ao bem-estar social, à igualdade, ao acesso à educação, saúde, cultura, moradia e outros aspectos que vão além das liberdades individuais e dos direitos políticos. Os direitos de terceira dimensão já foram utilizados por julgado do STF como parâmetro na defesa ao meio ambiente, mostrando a preocupação solidária e fraterna desta dimensão.

O art. 6º da Constituição Federal de 1988 (Brasil, 1988) inseriu o direito à saúde no contexto dos direitos sociais, de segunda dimensão, exigindo um Estado prestacional para estabelecer uma isonomia substancial e social.

De acordo com Paulo Bonavides (2004):

> Não se pode deixar de reconhecer aqui o nascimento de um novo conceito de direitos fundamentais, vinculado materialmente a uma liberdade “objetivada”, atada a vínculos normativos e institucionais, a valores sociais que demandam realização concreta e cujos pressupostos devem ser “criados”, fazendo assim do Estado um artífice e um agente de suma importância para que se concretizem os direitos fundamentais da segunda geração.

Destaca-se que antes da promulgação da Constituição Federal de 1988 (Brasil, 1988), o direito à saúde no Brasil não era expressamente reconhecido como um direito social na legislação. Em termos legais, o acesso à saúde estava mais vinculado a uma

visão assistencialista, tratado em leis ordinárias e regulamentações específicas, sem uma base constitucional sólida.

Nas palavras de José Afonso da Silva (2008, p. 308), “é espantoso como um bem extraordinariamente relevante à vida humana só agora é elevado à condição de direito fundamental do homem”.

Assim, ao ser elevado ao grau de direito social pelo art. 6º da CF/88 (Brasil, 1988), o direito à saúde tornou-se cláusula pétrea, assegurando sua estabilidade e integridade e protegendo-o contra alterações que possam comprometer sua estrutura fundamental.

O Artigo 194 da CF (Brasil, 1988) reconhece a saúde como elemento integrante do sistema de seguridade social. O sistema de seguridade social deve garantir a proteção à saúde, sendo esta reconhecida como um dos pilares essenciais desse sistema, juntamente com a previdência social e a assistência social.

Logo, a inclusão da saúde como componente integral do sistema de seguridade social reflete a compreensão de que a proteção social não se limita apenas à assistência médica, mas abrange um conjunto amplo de ações e serviços que visam garantir o bem-estar e a qualidade de vida da população.

O Artigo 196 da CF (Brasil, 1988) proclama que a saúde é direito de todos e responsabilidade do Estado. Ele destaca a obrigação do Estado em garantir acesso universal e igualitário a serviços de saúde, por meio de políticas sociais e econômicas, visando a promoção, proteção e recuperação da saúde da população.

A disposição constitucional presente no artigo 196 (Brasil, 1988), quando interpretada em conjunto com o cabeçalho do artigo 6º, estabelece uma responsabilidade vinculada a um agente específico: o Estado (União, Estado e Município). Assim, o Estado possui a obrigação de fornecer serviços de saúde de maneira gratuita, universal, equitativa e abrangente a todos os cidadãos (ABREU, 2014).

O art. 197 (Brasil, 1988) desta Constituição reconhece a "relevância pública" das ações e serviços de saúde e estabelece a competência do Poder Público para regulamentá-los, fiscalizá-los e controlá-los.

O art.198 da CF (Brasil, 1988) destaca a organização do sistema de saúde brasileiro com base em diretrizes que incluem a descentralização, a integralidade do atendimento (com ênfase em atividades preventivas) e a participação da comunidade.

Assim, a inclusão do direito à saúde como direito fundamental reflete um compromisso com a dignidade humana e estabelece bases sólidas para a atuação do Estado na promoção de um sistema de saúde acessível, universal e equitativo, consolidando a saúde como elemento central da cidadania e do bem-estar social.

2.1 SISTEMA ÚNICO DE SAÚDE (SUS)

A efetivação do direito à saúde no Brasil envolve a implementação de um sistema de saúde público, universal e integral. O alicerce desta materialização é o Sistema Único de Saúde (SUS), delineado no Artigo 198 da Constituição Federal (Brasil, 1988).

O SUS é amplamente reconhecido como a política pública de maior inclusão social implementada no Brasil, representando, no contexto constitucional, um compromisso político assumido pelo Estado brasileiro em favor de seus cidadãos (Brasil, 2007).

No dia 19 de setembro de 1990, foi promulgada a Lei nº 8.080 (Brasil, 2011), a qual estabeleceu as diretrizes para a promoção, proteção e recuperação da saúde, além de normatizar a organização e o funcionamento dos serviços correlatos, culminando na criação do SUS. Esta legislação, promulgada em meio a um contexto de redemocratização, reafirmou o compromisso do Estado brasileiro com a garantia do direito à saúde como um bem fundamental e inalienável de todos os cidadãos.

Os princípios fundamentais trazidos nessa legislação, como a universalidade do acesso, a integralidade das ações e serviços, a equidade na distribuição de recursos e a descentralização das ações de saúde refletem uma concepção inovadora que buscou superar desigualdades históricas e regionais.

> Universalização: a saúde é um direito de cidadania de todas as pessoas e cabe ao Estado assegurar este direito, sendo que o acesso às ações e serviços deve ser garantido a todas as pessoas, independentemente de sexo, raça, ocupação ou outras características sociais ou pessoais.
>
> Equidade: o objetivo desse princípio é diminuir desigualdades. Apesar de todas as pessoas possuírem direito aos serviços, as pessoas não são iguais e, por isso, têm necessidades distintas. Em outras palavras, equidade significa tratar desigualmente os desiguais, investindo mais onde a carência é maior.
>
> Integralidade: este princípio considera as pessoas como um todo, atendendo a todas as suas necessidades. Para isso, é importante a integração de ações, incluindo a promoção da saúde, a prevenção de doenças, o tratamento e a reabilitação. Juntamente, o princípio de integralidade pressupõe a articulação da saúde com outras políticas públicas, para assegurar uma atuação

> intersetorial entre as diferentes áreas que tenham repercussão na saúde e qualidade de vida dos indivíduos. (Sistema Único de Saúde).

Três meses após a aprovação da Lei 8.080 veio a Lei 8.142/90 (Brasil, 1990), promulgada em 28 de dezembro de 1990, a qual dispõe sobre a participação da comunidade na gestão do SUS e sobre as transferências intergovernamentais de recursos financeiros na área da saúde.

Entre os pontos mais importantes da Lei 8.142/90 (Brasil, 1990), estão: a) necessidade de conselhos e conferências de saúde para garantir a representatividade e o envolvimento da sociedade na definição de políticas e no controle social das ações de saúde; b) destinação de recursos para a saúde, estabelecendo percentuais mínimos de gastos dos municípios, estados e União, garantindo uma base financeira para a manutenção e expansão do SUS.

Não obstante a Lei 8.080 ter sido aprovada em 1990, apenas com o Decreto 7.508 (Brasil, 2011), de 28 de Junho de 2011, houve sua regulamentação. Entre as disposições principais do decreto, destaca-se a ênfase na regionalização da saúde e na criação de regiões de saúde, visando uma distribuição equitativa e eficiente dos serviços. Além disso, o decreto aborda a organização das redes de atenção à saúde, a necessidade de pactuação entre os entes federativos (União, Estados, Municípios e Distrito Federal), bem como aspectos essenciais relacionados à participação ativa da comunidade nos processos de decisão.

Destaca-se também a Lei Complementar 141, de 13 de Janeiro de 2012 (Brasil, 2012), que regulamenta o § 3o do art. 198 da Constituição Federal. Esta lei especifica as aplicações mínimas de recursos em ações e serviços públicos de saúde, define critérios para a elaboração de planos de saúde e estabelece mecanismos para a fiscalização e controle de recursos destinados à saúde. Ainda, reforça a necessidade de transparência nas informações sobre o financiamento e a execução das ações de saúde.

A administração das ações e dos serviços de saúde deve ser caracterizada pela solidariedade e participação conjunta dos três níveis federativos: União, Estados e municípios. A rede que integra o SUS é extensa e engloba tanto ações quanto serviços de saúde (abarcando a atenção primária, média e alta complexidade), os serviços de urgência e emergência, a atenção hospitalar, as atividades das vigilâncias epidemiológica, sanitária e ambiental, bem como a assistência farmacêutica.

Assim, o percurso de pouco mais de 30 anos do Sistema Único de Saúde brasileiro se caracterizou por importantes mudanças na atenção à saúde da população. Ao longo das últimas décadas, observou-se um notável aumento e diversificação na oferta de estabelecimentos de saúde, com especial destaque para o aumento significativo de postos de saúde públicos. Paralelamente ao aumento da infraestrutura, houve uma expansão notável no número de profissionais de saúde no país, sendo que a maioria significativa de médicos e enfermeiros mantém vínculos com o SUS (Viacava. 2018).

Portanto, o SUS no Brasil é de fundamental importância para o controle de doenças, imunização, educação em saúde, vigilância epidemiológica e acesso à serviços de saúde, destacando-se a recente Política Nacional de Saúde Bucal incluída no âmbito do SUS pela Lei 14.572, de 8 de Maio de 2023 (Brasil, 2023).

2.2 PAPEL DO PODER JUDICIÁRIO NO ACESSO AO DIREITO À SAÚDE

Com a expansão dos direitos conferidos aos cidadãos e a imposição da obrigação de pronta observância desses direitos pela Constituição de 1988 (Brasil, 1988), cujas normas adquiriram aplicabilidade direta e imediata, emergiu a responsabilidade do Poder Judiciário na efetivação do direito fundamental à saúde.

Nesse contexto, a jurisdição passou a desempenhar um importante papel ao corrigir a inércia do legislador e/ou administrador, incumbindo-se de ordenar a implementação das medidas necessárias para concretizar as políticas públicas delineadas pelo artigo 196 da Carta Magna.

O acesso à saúde pela via judicial está na necessidade percebida pelos indivíduos de obter, por meio de decisões judiciais, aquilo que não conseguem de maneira adequada pelo Sistema Único de Saúde (SUS).

As demandas judiciais pelo direito à saúde tiveram início no país nos anos 1990, com a ocorrência de ações judiciais que pleiteavam tratamentos para indivíduos portadores do vírus HIV. As decisões favoráveis aos pacientes representaram um avanço significativo na garantia do acesso universal e integral aos serviços e insumos de saúde. Desde então, as demandas passaram por uma diversificação e multiplicação (Vieira, 2023).

Destaca-se também o período da pandemia de COVID 19, onde as medidas adotadas nacionalmente mostraram-se descoordenadas, fragmentadas, mal

direcionadas e negligenciaram as potencialidades do SUS, e diante desse cenário, o Poder Judiciário teve que intervir de forma proativa para garantir a efetividade dos direitos fundamentais (Lucca, 2021).

Atualmente, as demandas judiciais para a efetivação do direito à saúde no Brasil refletem a complexidade e a abrangência do SUS, bem como as falhas e desafios enfrentados pelo sistema público de saúde. Essas demandas são variadas e podem ser classificadas em várias categorias, cada uma com suas particularidades e implicações legais e sociais.

Uma das principais categorias de demandas judiciais no campo da saúde é a solicitação de medicamentos e tratamentos não fornecidos gratuitamente, geralmente envolvendo medicamentos de alto custo, tratamentos experimentais ou terapias que não estão incluídas nas listas oficiais do SUS. Os pacientes que não conseguem acesso a esses medicamentos ou tratamentos recorrem ao Judiciário para garantir seu fornecimento.

Outra categoria significativa de demandas envolve pedidos de realização de procedimentos cirúrgicos e exames diagnósticos, onde os pacientes enfrentam longas filas de espera no SUS para cirurgias essenciais ou exames críticos, como ressonâncias magnéticas e tomografias. As ações judiciais visam obter ordens judiciais que obriguem o Estado a realizar esses procedimentos em tempo hábil.

Demandas relacionadas à internação hospitalar e ao acesso a unidades de tratamento intensivo (UTI) também são comuns, onde os pacientes buscam ordens judiciais para garantir leitos hospitalares adequados e cuidados intensivos, especialmente quando há superlotação nos hospitais públicos.

Além dos medicamentos e cirurgias, há demandas judiciais para obtenção de tratamentos específicos e terapias avançadas, como tratamentos para doenças raras, terapias genéticas e outros avanços médicos recentes.

Recentemente, observou-se um aumento significativo de pedidos judiciais requerendo o medicamento canabidiol. Esse aumento está diretamente relacionado ao reconhecimento crescente das propriedades terapêuticas do medicamento, especialmente no tratamento de condições médicas como epilepsia refratária, ansiedade, dor crônica e outras doenças neurológicas.

Dessa maneira, a atuação judicial não se limita apenas à resolução de litígios, mas também se estende à promoção da justiça social e à tutela efetiva dos direitos fundamentais no campo da saúde. A imposição de medidas por meio de decisões

judiciais visa suprir as deficiências na implementação das políticas públicas de saúde, garantindo a observância integral dos preceitos constitucionais voltados à proteção da vida e da dignidade humana.

No entanto, cabe salientar que a judicialização excessiva pode também desorganizar o planejamento e a gestão das políticas públicas de saúde. As decisões judiciais muitas vezes são tomadas sem uma visão geral do sistema de saúde, levando a uma fragmentação das políticas e dificultando a implementação de soluções integradas e sustentáveis.

Convém destacar que o Supremo Tribunal Federal (STF) definiu recentemente os parâmetros para a concessão judicial de medicamentos registrados na Agência Nacional de Vigilância Sanitária (Anvisa), mas não incorporados ao Sistema Único de Saúde (SUS), independentemente do custo. Este entendimento foi consolidado no Recurso Extraordinário (RE) 566471, Tema 6 da Repercussão Geral, julgado em março de 2020 e finalizado em 20 de setembro de 2023 (Brasil, 2023).

O julgamento concluiu que, como regra geral, o fornecimento judicial de medicamentos registrados na Anvisa e não incluídos nas listas do SUS (Rename, Resme e Remune) deve ocorrer de forma excepcional. Para o deferimento, o autor da ação precisa demonstrar, cumulativamente, a falta de recursos para aquisição, a imprescindibilidade do medicamento para o tratamento, a ausência de alternativas no SUS, e comprovar a eficácia do medicamento com base em evidências científicas robustas. A decisão, quando favorável, requer comunicação aos órgãos competentes para avaliação da incorporação do medicamento no SUS.

Três premissas sustentam essa tese: 1) a limitação dos recursos públicos; 2) a igualdade de acesso aos serviços de saúde e 3) o respeito pela expertise técnica embasada em evidências. Os ministros Gilmar Mendes e Luís Roberto Barroso ressaltaram que a judicialização excessiva beneficia indivíduos, mas pode comprometer a eficiência e a universalidade do sistema de saúde. Assim, as concessões judiciais devem estar fundamentadas na medicina baseada em evidências, destacando que somente órgãos técnicos detêm o conhecimento adequado para avaliar segurança, eficácia e custo-benefício de medicamentos.

Os requisitos definidos pelo STF exigem, além da negativa administrativa para o fornecimento do medicamento, a demonstração de que a Conitec não incorporou o fármaco ou que há atraso em sua avaliação, bem como a impossibilidade de substituição por medicamentos disponíveis no SUS. Também é necessário

comprovar, por meio de ensaios clínicos randomizados e revisões sistemáticas, a eficácia e segurança do medicamento e apresentar laudo médico fundamentado, demonstrando a imprescindibilidade do tratamento.

A tese de repercussão geral fixada também estabeleceu que as decisões judiciais que deferirem medicamentos fora das listas do SUS devem considerar, obrigatoriamente, a posição técnica do Núcleo de Apoio Técnico do Judiciário (NATJUS) ou de outros especialistas. A decisão não pode se basear exclusivamente em prescrições médicas do autor da ação, e deve incluir a análise do ato administrativo de não incorporação do medicamento pelo SUS.

Assim, é essencial o diálogo constante entre o Judiciário, os gestores de saúde e os formuladores de políticas. É necessário que as decisões judiciais sejam informadas por evidências científicas e pelo conhecimento técnico dos impactos sistêmicos, para assim garantir que a judicialização contribua positivamente para a saúde pública, sem comprometer a eficiência e a sustentabilidade do sistema.

3 SAÚDE DIGITAL: TECNOLOGIAS E INTELIGÊNCIA ARTIFICIAL APLICADAS NA SAÚDE PÚBLICA

No cenário contemporâneo, a tecnologia assume um papel indispensável na metamorfose da saúde pública, disponibilizando ferramentas e soluções inovadoras destinadas a abordar os desafios inerentes a essa esfera.

A aplicação da tecnologia no âmbito da saúde tem se expandido globalmente, abrangendo diversas áreas, como o aprimoramento de procedimentos cirúrgicos e estéticos, assim como a otimização da realização de exames médicos.

Destaca-se também que a realidade imposta pela pandemia do coronavírus (Covid-19), com o elevado risco de transmissão do vírus e com a cura ainda em fase de pesquisa, fez com que a demanda por mecanismos tecnológicos que facilitassem a comunicação entre o médico e o paciente afetado pela doença fosse implementada.

Com o advento das novas tecnologias, também surgem oportunidades para assegurar o direito à saúde por meio da aplicação da inteligência artificial e do uso de *chatbots*.

Ressalta-se que a compreensão do conceito de inteligência artificial é desafiadora, uma vez que não existe consenso e nem uma definição acadêmica universalmente aceita. No entanto, de maneira abrangente, a inteligência artificial pode ser caracterizada como a habilidade das máquinas de operarem de maneira análoga aos seres humanos: aprender, discernir e tomar decisões racionais diante de situações específicas. Não se exige que a máquina possua consciência de sua própria existência ou da realidade ao seu redor, mas sim que ela seja capaz de executar tarefas que anteriormente eram consideradas exclusivamente humanas.

Os *chatbots*, sistemas de assistência digital, são produtos da inteligência artificial e desempenham uma função decisiva na concretização do direito à saúde. Essa tecnologia, viabilizada pelos avanços em linguagem natural, possibilita que sites, aplicativos móveis e quaisquer dispositivos externos sejam capazes de falar com pessoas como humanos (Quedevez, 2022).

A criação de sistemas baseados em decisões humanas constitui um mi dos principais desafios no campo da Inteligência Artificial, encontrando aplicação frequente na área da Medicina por meio de Sistemas Especialistas (SE). Os softwares aplicados na área da saúde possuem um desenvolvimento inteligente utilizando Sistemas Especialistas para fornecer respostas a questionamentos específicos. Esses

sistemas operam por meio de inferências baseadas no conhecimento contido em uma base de conhecimento especializado. Uma característica fundamental desses sistemas é a capacidade de explicar de maneira transparente ao usuário suas conclusões e o raciocínio que levou a essas conclusões (Guarizi; Oliveira, 2014).

Por meio do Decreto nº 11.358, de 1º de janeiro de 2023, foi criada a Secretaria de Informação e Saúde Digital (SEIDIGI), com a incumbência de desenvolver políticas públicas direcionadas para a administração da saúde digital.

O estabelecimento da SEIDIGI marca um avanço significativo no progresso da saúde digital no Brasil. A secretaria é responsável por coordenar as ações do governo federal em diversas áreas da saúde digital, desde a implementação de sistemas de informação em saúde até a proteção de dados e a capacitação de profissionais.

Essas atribuições são essenciais para o desenvolvimento da saúde digital no país. O uso de tecnologias digitais pode melhorar o acesso, a eficiência e a equidade do atendimento, mas é preciso garantir que essas tecnologias sejam seguras e que os profissionais de saúde estejam preparados para usá-las.

A SEIDIGI tem o potencial de promover uma transformação significativa na saúde no Brasil, e está trabalhando para implementar a Estratégia de Saúde Digital para o Brasil 2020-2028, que visa a melhorar a qualidade, a eficiência e a equidade do atendimento, por meio do uso de tecnologias digitais.

O Ministério da Saúde também vem buscando introduzir inovações tecnológicas no âmbito do Sistema Único de Saúde (SUS), onde uma das ideias é incorporar a inteligência artificial (IA) nos serviços de atendimento à população. Isso seria feito por meio do programa SUS Digital, que ainda está em fase de estudos, e teria como propósito ampliar o acesso da população a um serviço de saúde pública que seja simultaneamente universal, eficiente e de elevada qualidade (CRUZ, 2023).

De acordo com Egues (2023):

> Em nosso sistema de saúde a IA poderia auxiliar na triagem de casos, acompanhamento de pacientes, como aquelas com diabetes, pressão alta ou até mesmo gestantes e puérperas. Em exames clínicos, a inteligência artificial se mostrou bastante eficaz no rastreio de anomalias em exames laboratoriais, sejam os de sangue ou de pesquisa genético.
>
> Em UTIs, sua utilização seria no monitoramento, previsão de fatores de risco e chances de agravo. Obviamente, todos os processos da IA, seja de diagnóstico, previsão, bancos da dados e afins, estariam sob supervisão humana.

> Novamente, é uma preocupação dos pesquisadores, que a IA aprenda de acordo com a sua área de implementação, pois cada região de nosso país, possui particularidades que precisam ser avaliadas individualmente.
>
> A IA pode ser uma ferramenta robusta para todos os níveis de atenção em saúde do SUS. Na atenção primária, impactaria na agilidade de marcação de consultas com especialistas, por exemplo. Mas ela não substitui a força humana dos profissionais dessa área.
>
> Portanto, é de suma importância que o governo capacite seus profissionais, dando incentivo para a continuidade e aprimoramento do seu conhecimento.Isso impactará de forma significando não apenas na manutenção da qualidade de nosso serviço gratuito de saúde, mas também na garantia de respeito aos princípios do SUS, melhorando como um todo a vida de nossa população

Cabe destacar o recente Plano Brasileiro de Inteligência Artificial (PBIA), denominado “IA para o Bem de Todos”, que prevê um investimento significativo de R$ 23 bilhões entre 2024 e 2028 e busca promover o desenvolvimento, a disponibilização e o uso ético da inteligência artificial no Brasil. Especificamente para o setor de saúde, o PBIA propõe iniciativas que visam otimizar processos e melhorar o atendimento à população, e entre as mais de 30 ferramentas previstas, destacam-se o desenvolvimento de sistemas de IA para suporte à decisão na compra de medicamentos, bem como para a otimização de diagnósticos no Sistema Único de Saúde (SUS), incluindo o diagnóstico de câncer, pneumonia e tuberculose.

3.1 PLANO DE AÇÃO SAÚDE DIGITAL

O plano de Ação Saúde Digital para o Brasil (Brasil, 2020) 2020-2028 delineia um conjunto de atividades e os recursos requeridos para efetivar a Visão de Saúde Digital, seguindo etapas evolutivas. Este planejamento foi concebido com base em três grandes eixos de ação e sete prioridades que, ao serem devidamente atendidas, conduzirão progressivamente à realização da referida Visão.

O primeiro eixo de ação diz respeito às ações do Ministério da Saúde para o SUS, reconhecendo e valorizando o Programa Conect SUS, tendo entre as principais ações a serem desenvolvidas: fortalecer a Rede Nacional de Dados em Saúde (RNDS), ampliando sua presença para todos os estados e municípios; Intensificar as ações do Informatiza APS para promover a conexão de todas as unidades de saúde à Rede Nacional de Dados em Saúde (RNDS); Ampliar e consolidar os serviços do

SUS, integrando de forma colaborativa a saúde pública com a privada e a suplementar.

Já o segundo eixo diz respeito à definição de diretrizes para colaboração, reconhecendo a importância de expandir e consolidar a governança e os recursos organizacionais essenciais para sustentar a Estratégia de Saúde Digital. Dentre as principais ações deste eixo estão a exploração de oportunidades de colaboração entre atores como suporte ao Conect SUS, bem como Identificar e suprir as demandas de recursos humanos na área da Saúde Digital. Além disso, mapear iniciativas de inovação em curso no país, abrangendo áreas como Internet das Coisas (IoT), Big Data, dados abertos e startups, assim como explorar colaborações internacionais e fortalecer parcerias já estabelecidas.

O terceiro e último eixo aborda a implantação do espaço de colaboração da Estratégia de Saúde Digital. Esse espaço tem como objetivo facilitar a colaboração entre todos os participantes da Saúde Digital, fornecendo definições claras de expectativas, papéis e responsabilidades. A colaboração proposta vai além do aspecto tecnológico, abrangendo modelos, serviços, métodos e conhecimentos otimizados pelo uso da Saúde Digital.

As iniciativas a serem implementadas foram cuidadosamente escolhidas com base na identificação de 7 prioridades estratégicas e fundamentais para a Estratégia de Saúde Digital (ESD), compreendendo-se que o pleno alcance das prioridades identificadas conduzirá à efetivação da Visão Estratégica de Saúde Digital para o Brasil.

Primeiramente, destaca-se a importância da Governança e Liderança para a ESD, visando desenvolvê-la sob a liderança do Ministério da Saúde, enquanto incorpora ativamente a contribuição dos atores externos por meio de plataformas de colaboração.

Outra prioridade é a Informatização dos Três Níveis de Atenção, que busca acelerar a implementação de políticas de informatização nos sistemas de saúde. Isso inclui a rápida adoção de prontuários eletrônicos e sistemas de gestão hospitalar, integrando essas tecnologias como parte essencial dos serviços e processos de saúde.

A terceira prioridade destaca o Suporte à Melhoria da Atenção à Saúde, alavancando a Rede Nacional de Dados em Saúde (RNDS) para oferecer suporte às melhores práticas clínicas, como serviços de telessaúde e aplicativos desenvolvidos

no Ministério da Saúde, além de outras aplicações provenientes da plataforma de colaboração.

O quarto ponto ressalta a importância de posicionar o Usuário como Protagonista, enfocando o engajamento ativo de pacientes e cidadãos. Este envolvimento visa promover a adoção de hábitos saudáveis, gerenciar a saúde pessoal, familiar e comunitária, ao mesmo tempo em que contribui para a construção participativa dos sistemas de informação que serão utilizados.

A quinta prioridade concentra-se na Formação e Capacitação de Recursos Humanos, buscando capacitar profissionais de saúde em Informática em Saúde, enquanto estabelece o reconhecimento dessa área como uma importante esfera de pesquisa e a Informática em Saúde como uma profissão relevante.

A sexta prioridade destaca a criação de um Ambiente de Interconectividade, permitindo que a Rede Nacional de Dados em Saúde facilite o trabalho colaborativo em todos os setores da saúde. Isso visa colocar em prática tecnologias, conceitos, padrões, modelos de serviços, políticas e regulamentações de forma eficiente.

Por fim, a sétima prioridade refere-se ao estabelecimento de um Ecossistema de Inovação. Esse ecossistema busca aproveitar plenamente o Ambiente de Interconectividade em Saúde, posicionando-se como um vasto laboratório de inovação aberta, sujeito às diretrizes, normas e políticas estabelecidas pela prioridade inicial. Essas prioridades coletivas delineiam uma abordagem abrangente para impulsionar a Saúde Digital no Brasil, promovendo a colaboração, a inovação e o empoderamento dos usuários no cenário da saúde digital.

Assim, a implementação da Estratégia de Saúde Digital para o Brasil 2020-2028 (Brasil, 2020) deve acelerar o uso de tecnologias digitais na saúde. No entanto, há exemplos concretos de como a tecnologia digital já está sendo usada para melhorar a saúde do Brasil, como a utilização da Telesaúde, prontuários eletrônicos e aplicativos de saúde.

3.2 DO USO DA TELESSAÚDE

Ao longo dos anos, os profissionais da medicina têm aproveitado a tecnologia das comunicações, como fax e telefones, em prol de seus pacientes. Continuamente, novas técnicas de informação e comunicação têm sido desenvolvidas, facilitando a troca de informações entre médicos e também entre médicos e pacientes.

Diante da nova realidade imposta pela pandemia do coronavírus (Covid-19), com o elevado risco de transmissão do vírus e com a cura ainda em fase de pesquisa, a demanda por mecanismos tecnológicos que facilitassem a comunicação entre o médico e o paciente emergiu a telessaúde como um recurso indispensável (Garcia; Maciel, 2020).

A telessaúde, conceituada como um conjunto abrangente de práticas de saúde realizadas remotamente, desempenha um papel fundamental na evolução do Sistema Único de Saúde (SUS) em direção à consecução dos princípios norteadores de acesso universal e integralidade na atenção à saúde (Lopes; Heimann, 2016).

No contexto atual, a telessaúde transcende barreiras geográficas, permitindo que profissionais de saúde alcancem pacientes em áreas remotas, contribuindo significativamente para a diminuição das disparidades no acesso aos serviços de saúde. Além disso, essa abordagem inovadora viabiliza a oferta de serviços especializados a pacientes que, de outra forma, enfrentariam dificuldades para receber atendimento médico qualificado.

A implementação da telessaúde também promove a integralidade na atenção à saúde ao facilitar a comunicação e colaboração entre diferentes profissionais e serviços de saúde. A troca eficiente de informações clínicas, a realização de teleconsultas e a promoção de discussões interdisciplinares contribuem para uma abordagem mais abrangente no cuidado ao paciente.

A acelerada evolução na velocidade de transmissão de dados nas redes, aliada ao desenvolvimento de dispositivos cada vez menores e mais sofisticados, geralmente integrados a smartphones, têm sido determinantes para a consolidação da telemedicina. O avanço tecnológico tem contribuído significativamente para a redução dos custos operacionais, a diminuição dos tempos de internação e a melhoria na qualidade dos cuidados prestados, especialmente para pacientes em regiões remotas e de difícil acesso (Ciancio; Rossi, 2022).

Ainda, a telessaúde surge como um instrumento estratégico para aprimorar a prevenção e o acompanhamento de condições crônicas, proporcionando monitoramento contínuo e intervenções oportunas, o que se alinha perfeitamente com a busca pela integralidade no SUS.

A lei 14.510/2022 (Brasil, 2022), de 27 de dezembro de 2022, foi responsável por conceituar, autorizar e disciplinar a prática da telessaúde no território nacional,

estabelecendo diretrizes que buscam equilibrar a inovação tecnológica com a segurança e qualidade na prestação de serviços de saúde.

> Art. 26-B. Para fins desta Lei, considera-se telessaúde a modalidade de prestação de serviços de saúde a distância, por meio da utilização das tecnologias da informação e da comunicação, que envolve, entre outros, a transmissão segura de dados e informações de saúde, por meio de textos, de sons, de imagens ou outras formas adequadas (Brasil, 2022).

Os princípios trazidos nos incisos do artigo 26-A (Brasil, 2022) são fundamentais para a integridade e eficácia da telessaúde, destacando-se a autonomia do profissional de saúde e o respeito à decisão do paciente, garantindo a confidencialidade dos dados e a promoção da universalização do acesso.

O artigo 26-C (Brasil, 2022) reforça a liberdade do profissional de saúde em decidir sobre a utilização da telessaúde, sublinhando a independência nas escolhas relacionadas ao atendimento remoto ou presencial, enquanto o artigo 26-D traz a importância dos conselhos federais de fiscalização do exercício profissional na definição de normas éticas relacionadas à telessaúde.

O artigo 26-F (Brasil, 2022) destaca a necessidade de justificação para restrições à telessaúde, abrindo espaço para uma discussão sobre os desafios regulatórios e a busca por equilíbrio entre a inovação e a segurança do paciente.

A Resolução n° 2.314/2022 (CFM, 2022), aprovada pelo Conselho Federal no Brasil, regulariza a prática profissional da telemedicina, abrangendo aspectos essenciais como o consentimento informado entre médico e paciente, a segurança das informações, a responsabilidade profissional e a validade jurídica dos atos médicos a distância (Moraes; Oliveira; Cruz, 2023).

Ressalta-se que além da teleconsulta, a Resolução prevê as seguintes modalidades: I) Teleinterconsulta; II) Telediagnóstico; III) Telecirurgia; IV) Telemonitoramento ou televigilância; V) Teletriagem; VI) Teleconsultoria.

Assim, a telemedicina consolidou-se como uma alternativa viável no atendimento médico no Brasil, sendo que em 2023, mais de 30 milhões de atendimentos médicos foram realizados à distância no país, conforme dados da Federação Nacional de Saúde Suplementar (Fenasaúde). Esse número representa um aumento de 172% em relação às 11 milhões de consultas remotas registradas entre 2020 e o final de 2022 (Lima, 2024).

No entanto, à medida que a telessaúde ganha destaque, a proteção da privacidade do paciente, a segurança dos dados de saúde transmitidos remotamente e a garantia de equidade no acesso a essas inovações são aspectos críticos que demandam atenção.

3.3 CONECTE SUS

A plataforma Conecte SUS, instituída pela Portaria Nº 1.434, de 28 de maio de 2020, surge como uma solução inovadora e necessária para a modernização e digitalização dos serviços de saúde no Brasil. Disponível tanto em formato de website quanto de aplicativo para smartphones, o Conecte SUS visa integrar e facilitar o acesso a informações de saúde para diversos públicos, incluindo cidadãos, estabelecimentos de saúde, profissionais e gestores.

O Conecte SUS Cidadão representa uma importante extensão do Sistema Único de Saúde (SUS), introduzindo um componente fundamental de interação direta com os usuários. Essa plataforma visa aproximar os cidadãos dos serviços de saúde, proporcionando maior autonomia e facilitando o acesso às informações relacionadas à sua saúde e aos serviços disponíveis.

Por meio do Conecte SUS Cidadão, os usuários podem realizar agendamentos, acessar resultados de exames, acompanhar seu histórico de atendimentos de forma digital, além de obter informações sobre vacinação.

A plataforma desempenha um papel fundamental na disponibilização do Certificado Nacional de Vacinação, especialmente da Covid-19. A capacidade dos cidadãos de gerar o Certificado Nacional de Vacinação por meio dessa plataforma além de simplificar o processo, estabelece um novo paradigma no qual a tecnologia desempenha um papel fundamental na documentação e verificação da imunização. Tal Certificado, agora amplamente conhecido como "passaporte da vacina", tornou-se requisito obrigatório para a participação em eventos em diversos estados e municípios brasileiros, sendo indispensável também para a entrada em alguns países.

Além disso, essa ferramenta contribui para o empoderamento do cidadão, permitindo que ele participe ativamente na gestão da sua própria saúde. O acesso fácil a informações relevantes promove uma maior conscientização sobre cuidados preventivos, facilitando a adoção de práticas saudáveis e contribuindo para a promoção do autocuidado.

Dessa forma, o Conecte SUS Cidadão representa uma significativa evolução na digitalização dos serviços de saúde, destacando-se como um relevante instrumento para promover transparência, participação ativa dos cidadãos e aprimoramento da qualidade dos serviços no SUS. Essa iniciativa reflete o compromisso em fortalecer a relação entre usuários e o sistema de saúde, alinhando-se aos princípios fundamentais de inclusão, acessibilidade e eficiência no atendimento público.

3.4 E-SUS

O e-SUS (Sistema Eletrônico de Informações do Sistema Único de Saúde) representa uma inovação significativa na gestão da saúde pública no Brasil. Criado em 2013 pelo Ministério da Saúde, o sistema tem como propósito modernizar e informatizar os processos que envolvem o atendimento à saúde, a coleta de dados epidemiológicos, a gestão de programas e a tomada de decisões pelos gestores públicos. Este sistema é parte integrante dos Sistemas Nacionais de Informação em Saúde (SNIS), um conjunto de ferramentas e bases de dados que suportam a gestão e a formulação de políticas públicas de saúde no Brasil.

A plataforma e-SUS é composta por diversos módulos que abrangem várias áreas da saúde, incluindo atenção básica, vigilância em saúde, saúde da criança, saúde da mulher, entre outros. Cada um desses módulos é projetado para facilitar o registro e o acompanhamento das atividades relacionadas a esses temas, proporcionando uma gestão mais eficaz e orientada por dados. A integração desses módulos permite uma visão vasta e detalhada das diversas frentes de atuação do sistema de saúde, possibilitando um acompanhamento preciso e contínuo das políticas e ações implementadas.

A tecnologia também vem sendo experimentada na saúde pública em programas como o e-SUS (Sistema Eletrônico de Informações do Sistema Único de Saúde), o qual faz parte dos Sistemas Nacionais de Informação em Saúde (SNIS) e tem o objetivo de modernizar o registro e a análise de informações relacionadas aos serviços de saúde.

Durante a pandemia de coronavírus, o e-SUS desempenhou um papel indispensável para salvar vidas: a rapidez na identificação de surtos, o acompanhamento da evolução da doença e a capacidade de tomar decisões

embasadas em informações atualizadas foram aspectos essenciais para enfrentar a crise sanitária. A plataforma permitiu a centralização e a análise de dados epidemiológicos em tempo real, facilitando a coordenação de ações entre diferentes níveis de governo e unidades de saúde. A capacidade de gerar relatórios e mapas de calor de casos de COVID-19, por exemplo, foi fundamental para a alocação de recursos e a implementação de medidas de contenção mais eficazes.

Além de sua importância em situações de crise, o e-SUS se destaca no gerenciamento rotineiro da saúde pública. Ao informatizar o processo de registro e análise de dados, a plataforma melhora a eficiência e a precisão das operações diárias. Isso inclui desde o agendamento de consultas até o acompanhamento de tratamentos e a vigilância epidemiológica. A digitalização dessas informações reduz a burocracia e os erros humanos, além de permitir que os profissionais de saúde acessem rapidamente o histórico dos pacientes, melhorando a qualidade do atendimento.

Nessa lógica, o Ministério da Saúde disponibilizou para uso gratuito dos municípios o Prontuário Eletrônico do Cidadão (PEC), que busca facilitar o processo de informatização das unidades básicas de saúde (UBS) em todo o território brasileiro. Durante os 10 anos de implementação do prontuário, também foram desenvolvidos o Centralizador Nacional de dados e diversos aplicativos mobile de apoio aos profissionais, como o e-SUS Atenção Domiciliar, o e-SUS Atividade Coletiva, o e-SUS Território, o e-SUS Vacinação e o Gestão e-SUS APS (Celuppi, 2024).

Outro benefício do e-SUS é a possibilidade de análises epidemiológicas mais detalhadas, essencial para a formulação de políticas públicas baseadas em evidências. Com dados precisos e atualizados, os gestores podem identificar tendências, monitorar o impacto de intervenções específicas e ajustar as estratégias de saúde conforme necessário.

Destaca-se que durante o período de 2013 a 2018 foram identificados 54 Sistemas Nacionais de Informação em Saúde (SNIS) em operação no Brasil. Esses sistemas, mantidos pelo Ministério da Saúde, abrangem diversas áreas, como cadastro, notificação de doenças, controle e logística de insumos e medicamentos, prontuários eletrônicos, gestão laboratorial, controle contábil da produção de procedimentos, entre outros (Coelho Neto; Andreazza; Chioro, 2021).

3.5 ASSISTENTE VIRTUAL COM INFORMAÇÕES SOBRE VACINAS

A disseminação de notícias falsas, ou *fake news*, sobre vacinas é um problema crescente no Brasil, com graves implicações para a saúde pública. A proliferação de informações incorretas e enganosas pode diminuir a confiança da população nas vacinas, resultando em menores taxas de imunização e um aumento na incidência de doenças que poderiam ser evitadas. A disseminação rápida dessas notícias falsas é facilitada pelas plataformas de mídia social e aplicativos de mensagens, que permitem que desinformações se espalhem para um público vasto de maneira praticamente instantânea.

Reconhecendo a gravidade dessa situação, o Ministério da Saúde lançou, em 04 de dezembro de 2023, uma iniciativa inovadora: um assistente virtual operando através do *WhatsApp*. Esse *chatbot* faz parte do programa “Saúde com Ciência” e tem como objetivo primordial fornecer informações oficiais e precisas sobre vacinação, combatendo assim as notícias falsas de forma eficaz.

A ferramenta é projetada para ser acessível e fácil de usar, garantindo que todos os cidadãos possam obter informações confiáveis diretamente do Ministério da Saúde. Isso não apenas facilita o acesso a dados corretos sobre vacinas, mas também fortalece a confiança do público nas campanhas de vacinação.

O *chatbot* oferece uma variedade de funcionalidades essenciais. Ele responde a perguntas comuns sobre vacinas, esclarece mitos e fornece dados atualizados sobre as iniciativas de vacinação em andamento. Além disso, os usuários podem enviar dúvidas e sugerir temas, permitindo que o Ministério da Saúde identifique áreas onde há maior necessidade de esclarecimento e desmentido de desinformações.

Um dos aspectos mais significativos desse assistente virtual é sua capacidade de emitir alertas e análises sobre *fake news*. As informações falsas identificadas serão analisadas e desmentidas, e essas correções serão amplamente divulgadas através do portal do programa, nas redes sociais do governo federal e atualizadas diretamente no *chatbot*. Esse fluxo contínuo de informações corretas e atualizadas é crucial para manter o público bem-informado e para combater a desinformação de maneira proativa (Ministério da Saúde, 2023).

3.6 SIMI-SP

O Sistema de Informações e Monitoramento Inteligente de São Paulo (SIMI-SP) exemplifica a integração de soluções tecnológicas avançadas na administração pública para a vigilância e gestão de crises de saúde pública.

Durante a pandemia de COVID-19, a necessidade de medidas eficazes para conter a disseminação do vírus levou o Estado de São Paulo a adotar estratégias inovadoras baseadas em inteligência artificial e análise de dados.

Instituído pelo Decreto n. 64.963 (São Paulo, 2020), o SIMI-SP foi desenvolvido em colaboração com quatro das principais operadoras de telefonia móvel do Brasil: VIVO, TIM, CLARO e OI. Este sistema aproveitava dados geográficos referenciais fornecidos pelas operadoras para monitorar a movimentação e a concentração de pessoas em diferentes áreas do estado, com o objetivo principal de identificar locais com alta densidade populacional, que poderiam representar potenciais focos de transmissão do vírus.

Um dos principais produtos do SIMI-SP foi a criação do Índice de Isolamento Social. Este índice permitia ao governo monitorar, em tempo real, o nível de adesão da população às medidas de distanciamento social impostas pelas autoridades sanitárias. Através da análise dos dados de mobilidade, era possível avaliar a eficácia das políticas de isolamento e identificar áreas onde as medidas necessitavam ser reforçadas.

A implementação do SIMI-SP exemplifica o conceito de "lógica dataficada e plataformizada" mencionado por Nóbrega e Girardi Júnior (2023). Esta abordagem refere-se à utilização de dados massivos (*big data*) e plataformas tecnológicas para a tomada de decisões em políticas públicas. No contexto da pandemia, a capacidade de coletar, processar e analisar grandes volumes de dados em tempo real permitiu ao governo de São Paulo reagir de maneira mais ágil e precisa às dinâmicas de propagação do vírus.

Contudo, a implementação de tais sistemas deve ser acompanhada de um rigoroso escrutínio ético e jurídico para assegurar que os direitos dos cidadãos sejam respeitados, sendo que a experiência de São Paulo com o SIMI-SP pôde servir como um modelo para outras jurisdições, não apenas em situações de emergência sanitária, mas também em outras áreas onde o uso da inteligência artificial para a gestão de

grandes volumes de dados pode contribuir para a eficiência e eficácia das políticas públicas de saúde.

3.7 ROBÔ LAURA

O robô Laura foi desenvolvido por Jacson Fressatto, um analista de sistemas brasileiro, após a perda de sua filha Laura, falecida devido a uma infecção generalizada aos 18 dias de vida.

A sepse, responsável por cerca de 56% das mortes hospitalares no Brasil, conforme estudo da Universidade Federal de São Paulo (Unifesp) e do Instituto Latino Americano da Sepse (Ilas), levou Fressatto a buscar soluções. Atuando como voluntário em um hospital de Curitiba, ele percebeu que, apesar da tecnologia e do empenho dos profissionais de saúde, havia necessidade de melhorias nos processos.

Dessa forma, ele fundou a *startup* Laura Networks e criou o robô Laura, com o objetivo de reduzir em 5% as mortes por sepse, salvando até 12 mil vidas por ano.

O robô Laura utiliza computação cognitiva e machine learning para aprimorar a identificação e o tratamento da sepse nos hospitais. Ele aprende a identificar sintomas de doenças com base em protocolos internacionais e históricos de pacientes, analisando dados operacionais e fornecendo suporte aos profissionais de saúde na gestão de processos, reduzindo erros operacionais e economizando recursos. Conectado aos sistemas hospitalares, o robô processa informações dos pacientes e emite alertas em caso de risco, permitindo intervenções rápidas e eficazes.

As principais funções do robô Laura incluem o monitoramento de dados vitais para identificar precocemente a sepse, garantindo a conformidade com boas práticas operacionais, auxiliando na identificação de surtos epidemiológicos, gerenciando bancos de sangue e monitorando a resistência bacteriana e prescrições médicas. Além disso, oferece uma visão estratégica de custos ao monitorar o uso de recursos das instituições.

Os benefícios do robô Laura para os hospitais são significativos, já que otimiza os processos ao analisar o fluxo de informações dos pacientes, identificando falhas nas rotinas hospitalares e permitindo melhorias na gestão e treinamento de equipes. Reduz custos ao monitorar o uso de recursos e identificar erros, contribuindo para a sustentabilidade financeira. Melhora o atendimento ao paciente com monitoramento

constante, alertando as equipes de saúde sobre sinais de alerta, como mudanças nos parâmetros vitais, possibilitando intervenções rápidas e eficazes.

Durante a pandemia de COVID-19, a empresa desenvolveu uma tecnologia chamada PA Digital, voltada para pacientes infectados pelo coronavírus. Esse serviço digital permite que os pacientes informem seu estado de saúde à robô, que então aconselha se é necessário procurar atendimento médico, ajudando a evitar aglomerações e idas desnecessárias ao hospital.

Desde seu lançamento, a Laura tem apresentado resultados impressionantes. Entre outubro de 2016 e maio de 2020, o robô atendeu 8,6 milhões de pessoas e salvou 24 mil vidas – uma média de 18 vidas salvas por dia. Em termos de números, a taxa de mortalidade nos hospitais que utilizam a Laura é 25% menor, e o tempo de internação de um paciente diminuiu de 103 para 96 horas (Dias, 2021).

3.8 ROBÔ HUMANOIDE GRACE

Grace é o nome da robô-enfermeira criada para auxiliar nos cuidados médicos de pacientes. Trata-se de um humanoide, com aparência e movimentos projetados para se assemelhar aos de um ser humano, tornando as interações mais naturais e empáticas.

Embora não possua nacionalidade, parte de sua inteligência artificial foi desenvolvida no Brasil. Grace utiliza funcionalidades de inteligência artificial (IA), o que facilita algumas de suas programações. No entanto, a base de sua operação é a inteligência artificial geral (AGI), capaz de aprender e executar ações de maneira semelhante aos seres humanos, permitindo que Grace se torne progressivamente mais inteligente.

Grace possui a habilidade de ler sinais vitais e medir a temperatura das pessoas. Além disso, a robô foi concebida para auxiliar no cuidado cognitivo e oferecer companhia aos pacientes, especialmente aqueles em cuidados intensivos ou idosos que vivem sozinhos.

Além de suas capacidades de monitoramento, Grace pode desempenhar tarefas cotidianas e burocráticas, como registrar pedidos de refeições e coletar dados diários para acompanhamento do estado de saúde dos pacientes. Essas funções ajudam a aliviar a carga de trabalho dos profissionais de saúde, permitindo que dediquem mais tempo ao contato humano direto com os pacientes.

Atualmente, Grace está sendo testada em hospitais no Canadá e na Coreia do Sul.

3.9 USO DA I.A. NO DESENVOLVIMENTO DE MEDICAMENTOS

O processo de descoberta e desenvolvimento de medicamentos tem sido tradicionalmente um empreendimento demorado e caro, exigindo entre 10 e 15 anos desde a pesquisa inicial até a comercialização. Este período prolongado é resultado de várias fases de pesquisa, desenvolvimento, testes clínicos e aprovação regulamentar, cada uma das quais apresenta desafios significativos e custos elevados. No entanto, a inteligência artificial (IA) está emergindo como uma solução inovadora que pode transformar este cenário, prometendo inaugurar um novo capítulo no setor farmacêutico (Weise, 2024).

Empresas farmacêuticas de renome, como Janssen, Sanofi, AstraZeneca e Bayer, têm estabelecido parcerias com empresas de biotecnologia especializadas em IA e estão também desenvolvendo soluções internas para incorporar essa tecnologia em seus processos. O uso da IA pode potencialmente reduzir pela metade os prazos de descoberta de medicamentos, oferecendo uma vantagem competitiva significativa e trazendo benefícios tangíveis tanto para a indústria quanto para os pacientes (Gil, 2024).

Entre as aplicações da IA com forte potencial de impacto no curto prazo estão a automatização da extração e sumarização de informações, a identificação e priorização de compostos químicos, a pesquisa com dados de moléculas complexas, a determinação das condições ideais para a eficácia dos medicamentos e a seleção de participantes para testes clínicos. A IA pode ser utilizada para automatizar a extração e sumarização de informações de documentos como patentes, publicações científicas e dados de ensaios clínicos, reduzindo significativamente a carga de trabalho dos cientistas e permitindo que eles se concentrem em tarefas mais complexas e criativas.

Utilizando modelos treinados em conhecimento bioquímico, a IA pode acelerar a identificação e priorização de compostos químicos com maior probabilidade de tratar doenças específicas, um processo que tradicionalmente pode levar anos e pode ser reduzido a meses ou até semanas. Além disso, a IA é capaz de lidar com dados de moléculas complexas, como proteínas e enzimas, auxiliando na pesquisa e permitindo

avanços mais rápidos para os testes in vitro, aspecto crucial para o desenvolvimento de medicamentos que interajam com alvos biológicos específicos. A IA também pode analisar rapidamente dados de inúmeras fontes para determinar as condições ideais em que um medicamento terá o efeito desejado, otimizando a eficácia dos tratamentos.

Na seleção de participantes para testes clínicos, a IA pode usar indicadores biológicos para selecionar os melhores candidatos, facilitando a condução dos estudos e aumentando a probabilidade de sucesso dos ensaios.

Em conclusão, a integração da IA no processo de descoberta e desenvolvimento de medicamentos representa uma mudança de paradigma no setor. As empresas que adotarem essa tecnologia estarão melhor posicionadas para enfrentar os desafios da indústria, proporcionando tratamentos mais rápidos e eficazes aos pacientes e contribuindo para a saúde global de maneira significativa.

4 DA ASSISTENTE VIRTUAL SARA

4.1 IMPLANTAÇÃO

A implantação do assistente virtual SARA no município de Guarapuava é resultado de uma parceria entre a Secretaria Municipal de Saúde e o Instituto Laura Fressatto de Apoio à Saúde, organização sem fins lucrativos reconhecida por sua capacidade técnica e administrativa, baseada na experiência da entidade em implantar soluções semelhantes em outros municípios, como São Bernardo do Campo, Catanduvas e Curitiba.

A assistente virtual SARA foi uma resposta estratégica da Prefeitura de Guarapuava-PR, por intermédio da Secretaria de Saúde, para enfrentar a alta demanda por atendimentos médicos causados pela pandemia de COVID-19.

Iniciado em 2021, o projeto de saúde digital demandou um investimento de R$ 4 milhões, provenientes de programas federais e recursos municipais. Implementada em 19 de janeiro de 2022, a SARA foi integrada à infraestrutura da Rede Municipal de Saúde, com o objetivo de otimizar os serviços de saúde e melhorar o atendimento aos pacientes, especialmente os afetados pelo coronavírus.

A proposição inicial da plataforma foi plenamente executada durante o período crítico da pandemia. Utilizando um sistema de triagem robusto, a intervenção especializada de profissionais de saúde e a agilidade proporcionada pela teleconsulta, o robô SARA foi capaz de identificar, monitorar e prestar atendimento remoto, encaminhando os casos conforme a gravidade para atendimento presencial quando necessário.

Assim, este sistema desempenhou uma função determinante na significativa redução das filas de espera, notadamente para pacientes suspeitos de infecção pelo Coronavírus, assegurando a recuperação dos indivíduos e desempenhando um papel essencial na preservação de vidas.

4.2 AMPLICAÇÃO DA ATUAÇÃO DA SARA

4.2.1 Canal Específico Voltado para Crianças com Síndromes Gripais

Em maio de 2022, apenas quatro meses após a bem-sucedida implementação inicial da plataforma, a Secretaria Municipal de Saúde de Guarapuava decidiu expandir o serviço para atender a um grupo específico da população: crianças com síndromes gripais leves e moderadas. Esta decisão foi motivada pelo sucesso da SARA no atendimento a adultos durante a pandemia de COVID-19 e pela necessidade de oferecer um cuidado especializado e seguro às crianças, especialmente considerando a vulnerabilidade desse grupo em períodos de alta incidência de doenças respiratórias.

Este novo canal foi desenhado para atender as necessidades específicas das famílias, oferecendo um atendimento conveniente e seguro, reduzindo a necessidade de deslocamento até as unidades de saúde e, consequentemente, diminuindo o risco de exposição a outras doenças.

Para garantir a qualidade e a eficácia do atendimento, a Secretaria Municipal de Saúde contou com a colaboração de médicos do Instituto Laura Fressatto, proprietário da plataforma que faz a gestão dos médicos que compõem a rede de atendimento e a Secretaria de Saúde. Esses profissionais especializados realizaram consultas online, avaliando os sintomas das crianças e orientando os pais sobre os cuidados necessários. Esta abordagem permitiu que muitas questões de saúde fossem resolvidas remotamente, sem a necessidade de atendimento presencial.

4.2.2 Oferecimento de assistência e monitoramento a pacientes diagnosticados com diabetes e hipertensão

Em outubro de 2022, a plataforma SARA passou por mais uma expansão, estendendo suas capacidades para incluir assistência e monitoramento de pacientes diagnosticados com diabetes e hipertensão. Esta ampliação do escopo do robô SARA foi uma resposta às necessidades crescentes de cuidado contínuo e especializado para pacientes com doenças crônicas, que requerem acompanhamento regular e intervenções adequadas para manter a saúde e prevenir complicações.

Para implementar essa nova fase, a Secretaria de Saúde de Guarapuava adotou uma abordagem proativa ao contatar os pacientes previamente cadastrados nas Unidades Básicas de Saúde (UBS). Utilizando o *WhatsApp*, a Secretaria enviou mensagens informativas e orientações aos pacientes, explicando os novos serviços oferecidos pela plataforma SARA e como poderiam se beneficiar do monitoramento contínuo.

A integração dos serviços de monitoramento de diabetes e hipertensão ao robô SARA trouxe inúmeros benefícios significativos para a gestão da saúde dos pacientes crônicos. Entre as funcionalidades inovadoras, destaca-se a triagem inicial e a avaliação contínua, onde os dados clínicos e históricos médicos dos pacientes são coletados e monitorados periodicamente. A SARA envia lembretes regulares sobre a importância da adesão ao tratamento, incluindo a ingestão de medicamentos e a realização de atividades físicas. Em casos de parâmetros anormais ou alarmantes, são enviados alertas aos profissionais de saúde para intervenções rápidas.

4.2.3 Expansão de capacidade de atendimento para qualquer condição de saúde que permita a assistência virtual.

Em 2023, a assistente virtual SARA passou por uma evolução significativa, expandindo sua capacidade de atendimento para abranger qualquer condição de saúde que permita a assistência virtual. Esta ampliação marcou uma nova fase na utilização da tecnologia de saúde em Guarapuava, potencializando ainda mais a eficiência e a abrangência dos serviços de saúde oferecidos à população.

> Nessa nova versão da plataforma digital, os usuários terão disponíveis novas funções, como:
> - Agendamentos;
> - Consultas online;
> - Atestado de vacinação;
> - Call center;
> - Atendimentos de enfermagem e psicologia (critérios específicos);
> - Agendamento de preventivos procedimentos;
> - Atestado de vacinação direto no app;
> - Escala M-CHAT para rastreamento de autismo;
> - Projeto mães em rede (grupos de atendimento remoto a gestantes).
>
> (GUARAPUAVA, 2023)

A plataforma passou a permitir que os pacientes agendem consultas e procedimentos médicos diretamente, facilitando o planejamento dos cuidados de

saúde e garantindo que não percam seus compromissos. As consultas online possibilitam que médicos e outros profissionais de saúde atendam remotamente, reduzindo a necessidade de deslocamentos e oferecendo conforto aos pacientes. Além disso, os usuários podem acessar e obter seus atestados de vacinação diretamente na plataforma, mantendo seus registros atualizados de maneira conveniente.

Outra funcionalidade importante é a integração de um call center, que oferece suporte adicional aos usuários, respondendo a perguntas e fornecendo orientações rápidas e eficientes. A SARA também passou a incluir atendimentos de enfermagem e psicologia, sujeitos a critérios específicos, garantindo um cuidado holístico que abrange aspectos físicos e emocionais da saúde dos pacientes. O agendamento de procedimentos preventivos, como exames de rotina, é outro recurso disponível, incentivando a prática de cuidados preventivos e a detecção precoce de problemas de saúde.

A plataforma incorpora ainda a Escala M-CHAT (Modified Checklist for Autism in Toddlers), utilizada para o rastreamento precoce de sinais de autismo em crianças, permitindo intervenções mais rápidas e eficazes. O Projeto Mães em Rede, que oferece grupos de atendimento remoto a gestantes, proporciona suporte contínuo e informações valiosas para futuras mães, promovendo uma gestação mais saudável e tranquila.

Conforme a gravidade de cada usuário, o próprio sistema direciona a pessoa para o atendimento presencial. Além disso, a ferramenta funciona 24 horas por dia, todos os dias da semana.

Essas novas funcionalidades trazem inúmeros benefícios, como a ampliação da acessibilidade aos serviços de saúde, proporcionando uma experiência mais conveniente e economizando tempo e recursos. O cuidado integrado e o suporte especializado garantem que os pacientes recebam atendimento completo e adequado às suas necessidades. A presença de um *call center* e a coordenação eficiente de serviços através da plataforma contribuem para um atendimento mais rápido, preciso e satisfatório.

4.3 A UTILIZAÇÃO DA SARA PARA DESAFOGAR OS ATENDIMENTOS NAS UNIDADES DE SAÚDE DE GUARAPUAVA

A implementação da assistente virtual SARA em Guarapuava, município com aproximadamente 180.000 habitantes, representa uma estratégia inovadora para aliviar a sobrecarga nas Unidades Básicas de Saúde (UBS) e nos serviços de urgência e emergência. A plataforma SARA, que permite a conexão de pacientes com médicos por meio de consultas online, tem sido essencial para atender pessoas com problemas de saúde considerados leves e moderados, sem a necessidade de deslocamento até as unidades de saúde.

As Unidades de Pronto Atendimento (UPA) do Batel e as Unidades de Urgência e Emergência do Trianon e Primavera têm enfrentado uma situação crítica de superlotação. Em abril de 2023, essas unidades registraram 24.803 atendimentos, dos quais 74% não eram classificados como urgentes. A UPA do Batel, em particular, atendeu mais de 10 mil pacientes apenas naquele mês. Nos primeiros dias de maio do referido ano, mais de 6.800 pessoas receberam atendimento nas unidades de saúde, sendo que 4.990 desses casos não eram graves. De acordo com a Secretária de Saúde, Chayane Andrade Ceroni, esse aumento nos atendimentos é esperado nesta época do ano devido ao crescimento dos casos de síndrome gripal e, atipicamente, pelos casos de dengue. Embora os casos de urgência e emergência sejam priorizados, os casos leves acabam aguardando mais tempo para serem atendidos (Nascimento, 2024).

Neste contexto, a plataforma SARA atua como um canal de triagem digital, permitindo que pacientes com sintomas leves façam uma avaliação inicial de forma rápida e segura, sem sair de casa. Através do aplicativo Fala Saúde, os pacientes podem acessar a opção "Fale com a Sara" e realizar a triagem digital. Alternativamente, podem acessar o chat da SARA pelo site da Prefeitura de Guarapuava.

Após a triagem inicial, baseada nos sintomas relatados, a SARA classifica o risco do paciente. Em seguida, uma equipe de enfermeiros entra em contato via WhatsApp para conduzir a consulta até um médico, se necessário, ou para fornecer demais orientações. Este processo permite que os casos leves sejam gerenciados eficientemente sem sobrecarregar as UBS e os serviços de emergência. O

atendimento pode ser realizado por teleconsulta ou presencialmente, dependendo da gravidade da situação.

Convém destacar também que em meio ao aumento de casos de dengue em todo o Brasil no ano de 2024, a utilização da assistente virtual SARA se tornou uma ferramenta essencial na abordagem precoce e eficaz dos casos, facilitando o acesso e a triagem de casos suspeitos de dengue.

Assim, a utilização da SARA tem demonstrado ser uma solução eficaz para desafogar os atendimentos nas unidades de saúde de Guarapuava. Ao permitir que muitos pacientes com condições menos graves recebam cuidados adequados remotamente, a SARA libera recursos e tempo para que as UBS possam se concentrar em casos mais críticos.

4.4 RESULTADOS ALCANÇADOS

Da implantação do assistente virtual SARA em janeiro de 2022 até o mês de agosto de 2024, foram realizadas 16.550 consultas médicas, evidenciando o impacto significativo desta ferramenta na prestação de serviços de saúde.

O número de atendimentos variou consideravelmente ao longo dos meses, com um início marcado por flutuações, como os 561 atendimentos em janeiro de 2022 e uma redução acentuada para 136 em março do mesmo ano. A partir da metade de 2023, observou-se uma estabilização em torno de uma média mensal de atendimentos, que ganhou força ao longo de 2024.

De acordo com Relatório Técnico de Monitoramento e Avaliação elaborado pela Secretaria Municipal de Saúde de Guarapuava, durante o período de monitoramento de junho de 2023 a janeiro de 2024, a Assistente Virtual Sara demonstrou resultados significativos que evidenciam sua relevância e impacto positivo na prestação de serviços de saúde pública.

Durante o período indicado, foram estabelecidas metas específicas para a Sara, com o objetivo de garantir a eficácia e a qualidade dos serviços de saúde prestados à população. As principais metas incluíam: a oferta de atendimento de saúde virtual para toda a população, o treinamento e a capacitação das equipes de atenção primária e de urgência, e o suporte continuado à operação da plataforma.

Para alcançar essas metas, uma série de atividades estratégicas foi realizada. Entre elas, destaca-se a fiscalização contínua e a avaliação do trabalho prestado pela

equipe responsável pela operação do Assistente Virtual Sara. Esse processo envolveu a conferência regular dos relatórios de atendimentos médicos por meio de auditorias mensais, cujo propósito era identificar inconsistências e áreas que demandassem melhorias. As inconsistências identificadas foram comunicadas ao Instituto Laura Fressatto, que promoveu as correções necessárias e enviou relatórios ajustados, bem como os recibos correspondentes para pagamento.

Além disso, o Instituto foi responsável por receber, apurar e resolver eventuais queixas e reclamações apresentadas pela população ou pelos profissionais de saúde envolvidos. Esse processo de gestão de feedback foi fundamental para ajustar continuamente o serviço e aprimorar a experiência do usuário, garantindo a satisfação dos pacientes e a confiança da comunidade na utilização do Assistente Virtual Sara.

Outra atividade essencial realizada durante o período de monitoramento foi o treinamento e a capacitação das equipes de saúde envolvidas. Essas ações visaram assegurar que os profissionais da atenção primária e de urgência estivessem aptos a utilizar a plataforma com eficiência, contribuindo para a disseminação do uso da tecnologia e o fortalecimento da sua integração com o sistema de saúde local.

O número de atendimentos realizados pelo Assistente Virtual Sara durante o período Junho de 2023 a janeiro de 2024 evidenciou a crescente demanda e adesão da população aos serviços de saúde virtual.

Neste último ano, o número de consultas apresentou um crescimento substancial, atingindo um pico de 2.000 atendimentos em maio de 2024. Após este ponto, houve uma queda para cerca de 1.084 atendimentos em junho e julho, e uma diminuição mais acentuada em agosto de 2024.

Gráfico 1 – Atendimentos mensais realizado pelo assistente virtual Sara

Fonte: Secretaria Municipal de Saúde de Guarapuava (2024)

Esses números refletem não apenas a capacidade do Assistente Virtual Sara de atender a uma grande quantidade de pacientes de maneira eficaz, mas também a confiança depositada pela população na tecnologia como uma alternativa viável e segura para o atendimento de saúde.

Além disso, o volume de atendimentos revela a eficácia do Assistente Sara em fornecer suporte à saúde pública, atendendo desde condições leves a moderadas, e funcionando como um complemento ao sistema de saúde local. Ao facilitar o acesso a consultas, orientações médicas e telemonitoramento, a plataforma contribuiu significativamente para reduzir a sobrecarga das unidades de saúde presenciais e otimizar os recursos disponíveis, garantindo que o atendimento presencial pudesse ser direcionado para casos mais graves e complexos.

5 A PRIVACIDADE E OS DESAFIOS DA SAÚDE DIGITAL

É certo o potencial da IA na área de saúde para o fim de revolucionar o setor, transformando a forma como os serviços de saúde operam, buscando melhorar a qualidade dos cuidados oferecidos e alcançando resultados mais eficazes a custos mais acessíveis. No entanto, cabe destacar que este cenário suscita questões éticas, sociais e econômicas significativas (Sousa, 2020).

A OMS também ressalta que a integração da IA na prática médica enfrenta diversos desafios éticos, legais e sociais, entre eles o acesso equitativo, a privacidade dos dados, o uso adequado das tecnologias e a responsabilização em relação a esses aspectos (Lucas; Santos, 2021).

Um dos principais desafios da IA na saúde é o custo de desenvolvimento e implantação, já que os sistemas são complexos e requerem grandes quantidades de dados e recursos computacionais, o que pode tornar seu desenvolvimento e implantação relativamente caros.

A infraestrutura necessária para suportar sistemas de IA em saúde é robusta, incluindo hardware especializado e servidores de alta capacidade. Além disso, a infraestrutura precisa de atualizações constantes para acompanhar os avanços da tecnologia e as crescentes necessidades de processamento.

O desenvolvimento de IA envolve algoritmos sofisticados e técnicas avançadas de aprendizado de máquina e deep learning, que são intrinsecamente complexos e caros. Esses sistemas requerem grandes quantidades de dados para serem treinados, geralmente envolvendo informações de saúde que precisam ser devidamente protegidas.

Ainda, o treinamento e qualificação dos profissionais para uso seguro e eficaz do sistema também representam um custo elevado, já que a IA exige que profissionais da saúde estejam preparados para utilizá-la de maneira adequada.

A qualificação dos profissionais de saúde para operar sistemas de IA é onerosa, uma vez que exige cursos específicos, certificações e até treinamento internacional. Além disso, as instituições de saúde devem alocar tempo e recursos para essas atividades, o que pode prejudicar outras áreas em que os recursos são igualmente escassos.

Relatório da Organização Mundial da Saúde (OMS), datado de 2021, destaca a necessidade de cautela ao avaliar os benefícios e riscos associados à

implementação de tecnologias avançadas na área da saúde. O documento salienta três questões preponderantes que demandam especial atenção: a reprodução e amplificação de discriminações por meio dessas tecnologias, os potenciais perigos à segurança dos pacientes e do meio ambiente, e o recolhimento e uso não ético de dados sensíveis e relacionados à saúde (Bruno; Pereira; Faltay, 2023).

O viés racial no atendimento IA é uma questão complexa, onde um sistema que deveria atender de forma parcial e inclusiva acaba por reproduzir e até amplificar preconceitos e estereótipos raciais presentes nos dados ou algoritmos.

> Casos que materializam esses riscos se avolumam à medida que a IA se dissemina na área de saúde. Um grave viés racial foi relatado por Obermeyer et al. (2019), ao analisarem o algoritmo usado para orientar decisões de gestão e administrativas no sistema de saúde dos Estados Unidos. Orientado a otimizar custos, o sistema automatizado presumia incorretamente que pacientes brancos precisavam de maior cuidado que pacientes negros com o mesmo nível de necessidade de atendimento, alocando assim menos da metade dos recursos para pacientes negros do que para brancos, segundo estimativa dos pesquisadores. Outro estudo concluiu que ferramentas de IA treinadas para a detecção de câncer de pele têm dificuldade de diagnosticar pessoas não brancas (Lashbrook, 2018 *apud* Bruno, Pereira; Faltay, 2023).

A questão da ética também se destaca, uma vez que a implementação de sistemas de IA pode levar a decisões automatizadas que afetam diretamente a vida e a saúde dos pacientes. Esses sistemas devem ser programados para agir de acordo com princípios éticos rigorosos, garantindo que os direitos dos pacientes sejam respeitados e que as decisões sejam transparentes e justificáveis (Doneda, 2018).

Apesar dos desafios, o uso da inteligência artificial (IA) no Brasil está crescendo rapidamente para melhorar a eficiência e a eficácia dos serviços em geral e também de saúde, principalmente na automatização de tarefas de gestão e atendimentos.

5.1. IMPACTO DA TECNOLOGIA NA PRIVACIDADE DOS DADOS DE SAÚDE

O uso de tecnologias na saúde utiliza a coleta de dados para permitir gerenciamento e planejamento nos casos de emergência sanitária, como também produzir um alargamento nas expectativas de combater as doenças, uso de aplicativos que colaboram para tratamentos e realização de atendimentos e procedimentos médicos e até cirúrgicos por meio da telemedicina (Rodrigues, 2023).

Embora benéfico, o uso das tecnologias apresenta riscos significativos à privacidade dos dados dos pacientes. Os principais desafios incluem a segurança da informação, onde a proteção contra acessos não autorizados, vazamentos de dados e ataques cibernéticos é fundamental, pois a vulnerabilidade dos sistemas pode resultar em exposições de dados sensíveis, causando danos aos pacientes e violando sua privacidade; compliance com leis e regulamentações, onde a conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações específicas de saúde é um desafio contínuo, sendo necessário garantir que todos os processos e sistemas estejam alinhados com os requisitos legais para a proteção de dados pessoais; e capacitação de profissionais, pois a falta de treinamento adequado dos profissionais de saúde e de TI pode comprometer a segurança dos dados, sendo essencial que todos os envolvidos estejam cientes das melhores práticas de segurança da informação e da importância da privacidade dos dados.

A integração de tecnologias no SUS oferece oportunidades significativas para a melhoria dos serviços de saúde, mas também impõe desafios consideráveis para a privacidade dos dados dos pacientes. Abordar esses desafios de forma proativa, através do fortalecimento da segurança da informação, conformidade com leis e regulamentações, e capacitação de profissionais, é essencial para garantir que os benefícios das inovações tecnológicas sejam plenamente alcançados sem comprometer a privacidade e a segurança dos dados pessoais.

5.2 DO DIREITO À PRIVACIDADE

5.2.1 Contexto histórico

A preservação dos direitos à intimidade e à vida privada sempre foi uma questão fundamental no desenvolvimento das sociedades humanas. Esses direitos emergiram como uma necessidade intrínseca ao progresso humano, diretamente ligados à busca pela dignidade e pela autonomia individual. Historicamente, a proteção da privacidade agiu na resistência contra opressões e arbitrariedades, configurando-se como um elo na promoção de uma sociedade justa e equitativa.

Na Antiguidade, a concepção de privacidade era bastante diferente da que temos hoje. Nas sociedades gregas e romanas, a vida pública e privada era menos separadas do que são atualmente, com a vida doméstica frequentemente exposta aos

olhos da comunidade. No entanto, havia uma certa proteção dos assuntos pessoais dentro das estruturas familiares e domésticas.

Na transição em direção à Idade Média, observa-se um lento e gradual reconhecimento da necessidade de isolamento, ainda que o conceito de individualidade estivesse longe do que conhecemos hoje. Durante esse período, a privacidade começou a ser cada vez mais valorizada, especialmente entre os mais abastados, como a nobreza e o clero (Doneda, 2006).

O Renascentismo, período que se estendeu aproximadamente do século XIV ao XVII, trouxe uma valorização do indivíduo e, com isso, um crescente reconhecimento da importância da privacidade. Filósofos e pensadores começaram a enfatizar a dignidade humana e a necessidade de proteger a vida pessoal contra interferências externas. No Iluminismo, que seguiu o renascentismo, essa ideia foi ainda mais desenvolvida, com teóricos como John Locke e Jean-Jacques Rousseau argumentando a favor dos direitos naturais e da autonomia individual. A proteção à privacidade começou a ser vista como essencial para a liberdade e a dignidade humanas.

No século XIX, com o advento da Revolução Industrial, a urbanização e as mudanças sociais trouxeram novos desafios para a privacidade. As cidades em crescimento e a vida em sociedade aumentaram a necessidade de proteger os direitos individuais contra a vigilância e a intrusão. Nesse contexto, o artigo de Samuel Warren e Louis Brandeis, "The Right to Privacy" (1890), foi um marco, defendendo o direito de ser deixado em paz como um direito fundamental.

No século XX a dinâmica desse cenário começou a transformar-se de maneira mais marcante ao longo da década de 1960, impulsionada, sobretudo, pelo aumento exponencial na circulação de informações, decorrente do avanço significativo das tecnologias de coleta e sensoriamento (Cancelier, 2017).

Inicialmente centrado na discussão sobre violações do direito de personalidades públicas, notadamente quando fotografadas em situações íntimas ou embaraçosas, o debate evoluiu consideravelmente. Atualmente, a atenção sobre o direito à privacidade concentra-se nos riscos para a personalidade de inúmeros cidadãos, cujos dados pessoais são coletados, processados e transferidos por entidades governamentais e privadas, utilizando modernas tecnologias da informação (Joelsons, 2021).

O avanço tecnológico e a crescente coleta, processamento e compartilhamento de dados pode levar à criação de perfis detalhados das pessoas, os quais podem ser usados para fins diversos como marketing, publicidade, vigilância e até controle social.

Nesse contexto, observou-se tanto na doutrina quanto na prática jurídica uma nítida evolução no entendimento do direito à privacidade. Esse direito transcende a concepção puramente negativa de ser deixado em paz, transformando-se em uma prerrogativa que engloba o controle ativo dos dados pessoais pelo próprio indivíduo.

5.2.2 Direito À Privacidade E Proteção Dos Dados Pessoais Como Direitos Fundamentais

Consagrado no artigo 5º da Constituição Federal de 1988 (Brasil, 1988), o direito à privacidade representa um dos pilares fundamentais dos direitos individuais no ordenamento jurídico brasileiro. Essa prerrogativa assegura ao cidadão a proteção de sua esfera mais íntima, resguardando-o contra ingerências indevidas por parte do Estado ou de terceiros.

No contexto constitucional, o direito à privacidade se manifesta como uma salvaguarda essencial para a preservação da dignidade humana, permeando diversas dimensões da vida cotidiana, desde as relações familiares até as interações digitais na era da informação, já que a interpretação e aplicação desse direito têm evoluído para acompanhar os desafios impostos pelas transformações sociais e tecnológicas.

> Esse direito vem assumindo paulatinamente maior relevo, com a contínua expansão das técnicas de virtualização do comercio, de comunicação, como defesa natural do homem contra as investidas tecnológicas e a ampliação, com a necessidade de locomoção, do círculo relacional do homem, obrigando-o a exposição permanente perante públicos os mais distintos, em seus diferentes trajetos sociais, negociais ou de lazer. É fato que as esferas da intimidade tem-se reduzido com a internet e os novos meios eletrônicos (Bittar, 2015).

Ganha destaque a recente Emenda Constitucional 115, de 10 de fevereiro de 2022 (Brasil, 2022), a qual acrescentou 3 dispositivos na Constituição Federal relacionados à proteção de dados pessoais, principalmente nos meios digitais:

> Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:

> "Art. 5º, LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."
> Art. 2º O caput do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:
> "Art. 21, XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei." (NR)
> Art. 3º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:
> "Art. 22, XXX - proteção e tratamento de dados pessoais." (Brasil, 2022).

Ao constar expressamente no rol do art. 5º (Brasil, 2022), passa o direito à proteção de dados pessoais a dotar de prerrogativas inerentes às garantias constitucionais, com status de cláusula pétrea, sendo mais um instrumento de suma importância e necessário para a proteção ao direito da privacidade.

Ainda, no art. 21, inc. XXVI (Brasil, 2022), o legislador conferiu à União a competência para organizar e fiscalizar a proteção e tratamento dos dados pessoais. Essa escolha é motivada pelo fato de que os dados, especialmente quando armazenados em meios digitais, não estão restritos a limites geográficos específicos, sendo necessário implementar medidas de proteção e fiscalização em nível nacional para assegurar um tratamento uniforme do assunto (Souza; Acha, 2022).

Por fim, o inciso XXX do artigo 22 (Brasil, 2022) reforça a competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais, garantindo que as regras sobre proteção de dados sejam uniformes e aplicáveis aos demais entes federativos, facilitando a implementação de políticas nacionais de proteção de dados e assegurando que todos os cidadãos brasileiros estejam sujeitos às mesmas proteções e obrigações

5.2.3 Código Civil e a Salvaguarda da Esfera Privada

No âmbito infraconstitucional, o direito à vida privada é reconhecido também no art. 21 do Código Civil de 2002 (Brasil, 2002): “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (Brasil, 2015).

Ao referir-se à "vida privada", o Código Civil imediatamente reflete a disposição constitucional de proteção à vida privada, conforme estipulado no artigo 5º, inc. X, da CF. Esta disposição não apenas resguarda a vida privada, mas também a intimidade, a honra e a imagem (Doneda, 2008).

Assim, o CC, ao reiterar essa proteção, estabelece um mecanismo claro para que o indivíduo possa buscar reparação judicial em casos de violação. Isso inclui a possibilidade de responsabilização civil daqueles que, de alguma forma, violem a esfera privada do indivíduo, causando-lhe dano moral ou material.

No contexto do ordenamento jurídico brasileiro, os elementos constitutivos da responsabilidade civil estão dispostos no artigo 186 do Código Civil (Brasil, 2002). Adicionalmente, a Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes específicas para a responsabilidade civil dos agentes de tratamento de dados pessoais em sua Seção III - Da Responsabilidade e do Ressarcimento de Danos, abrangendo os artigos 42 a 45 (Brasil, 2018).

Não obstante a proteção à vida privada ser um direito fundamental que encontra respaldo tanto na Constituição Federal quanto no Código Civil, para que essa proteção seja efetiva, é necessário um esforço conjunto que inclua a aplicação rigorosa da legislação, a educação da população, o uso de tecnologias de proteção e a criação de mecanismos de fiscalização, para ser possível garantir uma tutela abrangente e eficaz da privacidade dos indivíduos, preservando sua dignidade e autonomia.

5.2.4 Política Nacional de Cibersegurança (Decreto 11.856/23)

O Decreto nº 11.856 (Brasil, 2023), de 26 de dezembro de 2023, institui a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber), reforçando a proteção à privacidade dos dados pessoais, sendo indispensável nos dias atuais para garantir a segurança cibernética no Brasil, protegendo informações sensíveis contra ameaças digitais.

> A cibersegurança, ou segurança cibernética, refere-se à prática de proteger sistemas, redes e programas de ataques digitais. Esses ataques geralmente visam acessar, alterar ou destruir informações sensíveis, extorquir dinheiro de usuários ou interromper processos empresariais.
>
> Implementar medidas eficazes de cibersegurança é particularmente desafiador, pois atualmente há mais dispositivos do que pessoas no país e os hackers se tornam cada vez mais inovadores. A PNCiber e o CNCiber surgem como respostas essenciais a esses desafios, buscando elevar o nível de proteção e segurança de dados no Brasil. (SERPRO, 2023)

Conforme exposto na Nota Técnica SSIC/GSI N.º 01/2023 (Brasil, 2023), que justifica o projeto de lei para o estabelecimento da PNCiber, esta é uma iniciativa destinada a unificar a fragmentada regulação existente no país, minimizar o crescente número de incidentes que afetam o Brasil, gerando consideráveis prejuízos para a sociedade brasileira, reduzir o déficit tecnológico nacional no setor e aumentar a participação do Brasil na cooperação internacional sobre o tema.

Implementar medidas eficazes de cibersegurança é particularmente desafiador, pois atualmente há mais dispositivos do que pessoas no país e os hackers se tornam cada vez mais inovadores. A PNCiber e o CNCiber surgem como respostas essenciais a esses desafios, buscando elevar o nível de proteção e segurança de dados no Brasil.

Entre os princípios da PNCiber, destacam-se a garantia dos direitos fundamentais, incluindo a proteção dos dados pessoais e da privacidade. Estes princípios são essenciais para a segurança dos dados de pacientes, que contêm informações extremamente sensíveis e privadas.

A criação do Comitê Nacional de Cibersegurança (CNCiber) é um passo significativo para a coordenação das ações de cibersegurança no país. O comitê tem a responsabilidade de propor atualizações e medidas para incrementar a segurança cibernética, formular propostas para a prevenção e resposta a incidentes cibernéticos, e promover a educação em segurança cibernética.

Além disso, a PNCiber incentiva o desenvolvimento de tecnologias de segurança cibernética e a adoção de medidas de gestão de riscos, que são essenciais para proteger a integridade, a confidencialidade e a disponibilidade dos dados pessoais.

A educação e a capacitação técnico-profissional em segurança cibernética, previstas pela PNCiber, também são igualmente importantes.

Assim, a implementação da PNCiber assegura que, no setor de saúde, as instituições adotem medidas de segurança adequadas para proteger dados sensíveis contra acessos não autorizados, vazamentos e ataques cibernéticos.

5.3 CASOS DE VAZAMENTOS E PROBLEMAS ENVOLVENDO A PRIVACIDADE DOS DADOS DE PACIENTES

Os casos de vazamento de dados pessoais, quando se tornam públicos, geram uma sensação de desconfiança significativa entre os cidadãos e consumidores em

relação às instituições que permitiram a difusão dessas informações. A exposição de dados sensíveis pode incluir detalhes sobre condições de saúde, histórico médico, e outros dados pessoais que os indivíduos esperam manter confidenciais.

Ainda, a difusão indevida de dados pode causar danos concretos aos indivíduos, incluindo discriminação, especialmente no caso de dados sensíveis. Por exemplo, a exposição de informações sobre doenças transmissíveis, condições de saúde mental ou status sorológico pode levar a discriminação no local de trabalho, perda de emprego, ou estigma social.

Outro risco significativo envolve a transferência de dados pessoais sem o consentimento dos titulares ou a utilização desses dados para fins distintos daqueles que legitimaram sua coleta. Esse tipo de transferência levanta sérias preocupações sobre a privacidade e a segurança das informações pessoais, além de ilustrar os potenciais abusos no uso de dados sensíveis.

A esfera da saúde constitui uma das áreas mais férteis em geração de dados, abrangendo desde as informações dos pacientes e seus registros médicos até os dados provenientes de ensaios clínicos, pesquisas e estudos.

Muitos sistemas de saúde estão interconectados para facilitar o compartilhamento de informações entre hospitais, clínicas, laboratórios e outras instituições. Ainda, a infraestrutura de tecnologia da informação em organizações de saúde por vezes inclui sistemas mais antigos que não acompanham a evolução tecnológica, criando lacunas em termos de segurança cibernética.

Diversos vazamentos de dados relevantes no contexto da saúde já foram noticiados. Merecem destaque alguns destes incidentes de segurança, incluindo a divulgação não autorizada de informações da Anvisa relacionadas a pacientes autorizados a utilizar canabidiol e episódios de violações de segurança no Ministério da Saúde entre os anos de 2020 e 2021 (Silva; Cunha, 2023).

Em 2020, a Agência Nacional de Vigilância Sanitária (Anvisa) enfrentou uma situação delicada relacionada à exposição inadvertida de informações pessoais de 1.900 pacientes que utilizam medicamentos à base de canabidiol (CBD) para fins terapêuticos. Este incidente ocorreu durante o envio de uma mensagem aos pacientes e empresas do setor, onde, em vez de utilizar a funcionalidade de cópia oculta (BCC), a agência usou a cópia aberta (CC), expondo assim os endereços de e-mail dos destinatários.

Em 2020, o Hospital Israelita Albert Einstein confirmou um grave incidente de segurança envolvendo o vazamento de dados de aproximadamente 16 milhões de pessoas que tiveram suspeita ou diagnóstico confirmado de Covid-19. Este vazamento ocorreu devido à exposição de senhas de sistemas do Ministério da Saúde, resultando na disponibilização de dados pessoais e médicos na internet por quase um mês.

Também no ano de 2020 uma nova falha do Ministério da Saúde expôs dados de cerca de 243 milhões de brasileiros na internet. De acordo com "O Estado de S. Paulo" (São Paulo, 2020), o vazamento foi causado pela exposição indevida de login e senha de acesso ao sistema do Ministério da Saúde, mesma falha que expôs 16 milhões de pacientes que tiveram Covid-19.

No ano de 2021 registrou-se um incidente em que o Sistema Único de Saúde (SUS) no Brasil foi alvo de um ataque cibernético. A equipe de segurança do Ministério da Saúde detectou prontamente a intrusão e reportou-a imediatamente às autoridades competentes. Segundo informações do próprio Ministério da Saúde, o ocorrido configurou-se como um ataque de ransomware, uma técnica empregada por hackers para criptografar os arquivos do sistema, demandando o pagamento de um resgate em contrapartida à chave de descriptografia. Como desdobramento dessa ação, alguns sistemas foram impactados, resultando na interrupção drástica de alguns serviços de saúde em pleno contexto de pandemia (Silva, Cunha. 2023):

> Um grupo hacker assumiu a autoria do ataque. Os invasores publicaram no site do Ministério da Saúde e no ConecteSUS que 50 terabites de dados foram copiados e excluídos, e cobraram um contato do governo para devolver as informações. Pouco antes das 7h, a mensagem foi retirada.
>
> O ataque gerou uma série de problemas. Em vários locais de vacinação acabou provocando aumento nas filas e demora no atendimento. Em Goiânia, por exemplo, o registro da aplicação das doses estava sendo feita manualmente. Em Teresina, a prefeitura registrou a aplicação das doses em um site alternativo. Em Salvador, alguns passageiros foram impedidos de embarcar em ônibus intermunicipais porque, com aplicativo fora do ar, não conseguiram mostrar o comprovante de vacinação (G1, 2021).

O crescimento exponencial na velocidade, diversidade e volume de dados (BIG DATA) também suscita sérias preocupações relacionadas à privacidade. As grandes empresas de tecnologia (BIGTECHS) assumem a liderança nesse cenário de big data e estão cada vez mais coletando e processando dados pessoais (Zuboff, 2021).

O conceito de "big data" oferece vastas oportunidades para o progresso do conhecimento em no âmbito da saúde pública na medida em que, a minuciosa coleta de dados por meio de prontuários médicos eletrônicos resulta em um extenso conjunto de informações. Esses dados, quando devidamente analisados, apresentam o potencial de antecipar necessidades e guiar a implementação de ações planejadas com estratégias mais precisas e eficazes. No entanto, são levantadas preocupações sobre o potencial uso de tais informações (Alves Filho, 2023).

> Uma das principais ferramentas de discussão de casos clínicos entre profissionais de saúde tem sido o WhatsApp, aplicativo pertencente à empresa Meta (ex-Facebook). O app também está sendo utilizado em larga escala para comunicação entre médicos e seus pacientes. Apesar de a empresa afirmar que os dados são criptografados ponta a ponta, informações recentes levantam suspeitas de que equipes internas e ferramentas autônomas (tipo inteligência artificial) têm, sim, tido acesso ao conteúdo das mensagens (PROPUBLICA, 2012). Além disso, a empresa Meta também vem sofrendo denúncias de ex-funcionários por questões éticas relacionadas à análise de conteúdo de sua principal rede social, o Facebook (BBC BRASIL, 2021). Tal problema pode inclusive ser mais grave em outras plataformas de redes sociais, como o Telegram, que deliberadamente possui regras elásticas de proteção dos dados e moderação de conteúdo (Caetano, 2021 *apud* Silva; Cunha. 2023)

Vale destacar também que as grandes empresas de tecnologia mantêm centros de dados em diferentes partes do mundo para otimizar a eficiência e a disponibilidade de seus serviços, onde do ponto de vista da segurança, o armazenamento internacional de dados implica em desafios adicionais, uma vez que diferentes jurisdições podem ter diferentes padrões de segurança cibernética.

Neste contexto ganha força o conceito de soberania digital, o qual refere-se à capacidade de um país em gerenciar seus próprios dados e informações dentro de sua jurisdição, sem interferências externas de outros países ou corporações (Silva; Cunha, 2023).

Assim, entende-se que a disponibilidade generalizada de informações de saúde para as grandes empresas de tecnologia pode resultar em sérias violações éticas e abalar a confiança dos pacientes no sistema de saúde digital. Ainda, a falta de transparência nas práticas das Big Techs em relação à coleta, armazenamento e uso de dados agrava a preocupação, sendo fundamental estabelecer soluções tecnológicas internas, juntamente com regulamentações claras que garantam a

proteção da privacidade dos pacientes, a segurança dos dados e a transparência nas práticas das *Big Techs*.

5.4 DIRETRIZES QUE BUSCAM O SIGILO DOS DADOS DE PACIENTES

O direito à privacidade dos dados médicos garante ao indivíduo a manutenção das informações a seu respeito e seus problemas de saúde inacessíveis a outros indivíduos. Toda informação decorrente de interações médicas é considerada confidencial, e o acesso a ela deve ser protegido (Carvalhal *et al*., 2017).

A privacidade e sigilo de informações são abordadas em diversas normas setoriais e éticas. O Código de Ética Médica (CEM) (CFM, 2019), ferramenta normativa essencial que orienta o exercício ético da profissão, em seu capítulo IX trata do sigilo profissional e do dever de confidencialidade de informações médicas relacionadas ao paciente.

A Portaria 1.820, de 13 de agosto de 2009 (Brasil, 2009), publicada pelo Ministério da Saúde e que dispõe sobre os direitos e deveres dos usuários da saúde, já trazia em seu texto a garantia das pessoas nas consultas e em diversos tipos de procedimentos a confidencialidade de toda e qualquer informação pessoal.

A Política Nacional de Informação e Informática em Saúde (PNIIS) de 2016 representa um importante marco regulatório no contexto da saúde no Brasil, e estabelece diretrizes e princípios para a gestão de informações nesse setor. Em consonância com as preocupações contemporâneas sobre privacidade e proteção de dados, a PNIIS também aborda questões relacionadas ao direito à privacidade dos indivíduos.

No âmbito da PNIIS, o direito à privacidade é reconhecido como um elemento essencial na gestão da informação em saúde. A política estabelece medidas específicas para garantir a confidencialidade e a segurança das informações pessoais dos pacientes, reconhecendo a sensibilidade dos dados relacionados à saúde e a necessidade de proteção especial.

O Plano Nacional de Saúde 2016-2019, aprovado pelo Conselho Nacional de Saúde, apoiou em seu “objetivo 11” a promoção de ações para assegurar a preservação dos aspectos éticos, de privacidade e de confidencialidade em todas as etapas do processamento das informações.

> O fortalecimento dos canais de interação com os usuários do SUS ocorrerá mediante apoio à criação de estruturas descentralizadas de ouvidoria em saúde; da implementação de políticas de estímulo à participação de usuários e entidades da sociedade no processo de avaliação dos serviços prestados pelo SUS; da promoção de ações para assegurar a preservação dos aspectos éticos, de privacidade e confidencialidade em todas as etapas do processamento das informações decorrentes; da disseminação de informações aos cidadãos sobre o direito à saúde e às relativas ao exercício desse direito; da realização de estudos e pesquisas visando à produção do conhecimento, no campo da ouvidoria em saúde, para subsidiar a formulação de políticas de gestão do SUS (PNS. 2016)

Especialmente após a crise desencadeada pela pandemia de Covid-19, iniciada em março de 2020, foram registradas inúmeras instâncias de vazamento de informações relacionadas à certificação da população e aos casos positivos da doença. Diante disso, percebe-se que o setor da saúde emergiu como um dos campos com maior susceptibilidade a violações de dados e sua subsequente divulgação (Zaganelli; Binda Filho, 2022).

Apesar das garantias à privacidade estabelecidas por várias normas na área da saúde, a coleta e o tratamento de dados no âmbito da saúde pública permaneceram desprovidos de legislação ou regulamentação específica por um período significativo.

5.5 LGPD

As conversas em torno da preservação da privacidade dos dados pessoais ganharam maior destaque com o aumento do uso de tecnologias nas atividades cotidianas e a expansão da internet para a transmissão de informações, notícias e outros meios de comunicação (Lima; Gonçalves; Costa, 2021).

Estima-se que mais de uma centena de nações tenha promulgado legislação voltada para a proteção de dados pessoais (Consumers International, 2018). Dentre essas regulamentações destaca-se a General Data Protection Regulation (GDPR), uma norma que estabelece e orienta as principais diretrizes para a preservação da privacidade de informações pessoais no âmbito da União Europeia. Inicialmente publicada em 2016, a GDPR entrou em vigor em 2018, impondo a necessidade de conformidade às suas exigências legais para países que mantêm relações comerciais com a Europa (Ferreira, 2023).

A promulgação do Marco Civil da Internet em 2014 (Lei n. 12.965/14) marcou um avanço significativo na legislação brasileira, proporcionando uma base legal sólida para a regulação do uso da internet e a salvaguarda da privacidade, estabelecendo um arcabouço legal ao definir princípios destinados a proteger a privacidade e os dados pessoais dos usuários, tais como a garantia da inviolabilidade e sigilo das comunicações privadas.

Seguindo essa diretriz e inspirado no Regulamento Geral de Proteção de Dados da União Europeia, em agosto de 2018, foi sancionada a Lei n° 13.709/18 (Brasil, 2018), chamada de Lei Geral de Proteção de Dados Pessoais (LGPD).

> É possível afirmar que a concreta e talvez mais importante consequência da EC 115/2022 seja a de emprestar força normativa e efetividade a Lei Geral de Proteção de Dados em seus termos. Isso porque, além da aplicabilidade imediata respaldar a incidência deste dispositivo a todos os casos concretos, uma vez que é a norma disponível e voltada a regulação do tratamento de dados no Brasil, o texto do novo inciso LXXIX, ao dispor que “é assegurado, nos termos da lei, o direito fundamental a proteção de dados pessoais...”, prevê e também confirma que trata-se a LGPD do instrumento normativo que assegura o exercício do direito a proteção de dados. (Franco, 2022).

Dentre os 65 artigos presentes na LGPD (Brasil, 2018), identifica-se 5 pilares fundamentais em torno dos quais se estrutura a proteção do indivíduo detentor de dados: i) universalidade e abrangência da aplicação da LGPD; ii) legitimidade do tratamento de dados mediante a aplicação de condições legais específicas; iii) princípios e direitos garantidos aos titulares; iv) deveres impostos aos agentes responsáveis pelo tratamento; e v) responsabilização dos agentes envolvidos no tratamento de dados pessoais (Mendes, 2018).

Não obstante a abrangência da LGPD se estender sobre todos os setores, sua relevância é ainda mais pronunciada no contexto da saúde pública. Isto porque três em cada quatro brasileiros dependem exclusivamente do Sistema Único de Saúde (SUS), e no contexto da relação médica, é pertinente considerar que os dados inerentes a essa interação são classificados como "dados sensíveis", onde sua violação pode acarretar sérios danos.

Dados pessoais, de acordo com a LGPD, são informações que permitem identificar direta ou indiretamente uma pessoa. Isso inclui uma variedade de informações, como CPF, RG, data e local de nascimento, localização em GPS, prontuário de saúde, entre outros.

Já dados pessoais sensíveis, conforme estabelecido pelo art. 5º, inc, II, da LGPD, são aquele que abrangem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual, além de dados genéticos ou biométricos quando vinculados a uma pessoa natural.

A legislação estabelece regras específicas para o tratamento de dados pessoais sensíveis, exigindo maior cuidado e consentimento explícito por parte do titular. Tal abordagem visa garantir que informações delicadas sejam manuseadas com responsabilidade e respeito à privacidade, reduzindo o risco de uso inadequado ou discriminação.

É importante destacar que as informações sensíveis de saúde não estão restritas ao contexto da telessaúde, uma vez que existe a possibilidade de armazenamento desses dados por instituições de saúde, como hospitais ou clínicas, em outras modalidades, incluindo a presencial. A proteção aos dados pessoais sensíveis de saúde busca não apenas a preservação da intimidade do paciente, mas também objetivam o auxílio às instituições públicas na gestão dos dados.

Ainda, ressalta-se que as disposições abrangentes da Lei Geral de Proteção de Dados (LGPD) são de interesse nacional, requerendo aderência por parte dos Órgãos Gestores em Saúde em nível federal, estadual, distrital e municipal (Aragão; Schiocchet, 2020).

5.5.1 Autoridade Nacional de Proteção de Dados (ANPD)

Com a LGPD, surgiu também a sua agência reguladora, a Autoridade Nacional de Proteção de Dados (ANPD).

A ANPD é um órgão brasileiro criado em 2019 pela Lei 13.853 (Brasil, 2019), tendo um papel que vai além da mera fiscalização e imposição de sanções em casos de violações à LGPD. Além do caráter fiscalizatório e sancionatório, a ANPD desempenha um papel normativo e deliberativo significativo.

A missão da ANPD é zelar pela proteção dos dados pessoais no Brasil, visando proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade das pessoas naturais, conforme estabelecido no decreto que regula a autoridade.

A ANPD é também responsável pela interpretação da LGPD, podendo estabelecer normas e diretrizes para a implementação eficaz da legislação. Essa atuação é determinante para assegurar a proteção dos titulares de dados pessoais, ao mesmo tempo em que proporciona segurança jurídica aos agentes de tratamento em suas atividades cotidianas.

A ANPD possui uma estrutura organizacional bem delineada, composta por diversos órgãos que desempenham papéis específicos na implementação e fiscalização da Lei Geral de Proteção de Dados (LGPD). O Conselho Diretor, composto por cinco diretores, figura como o órgão central de tomada de decisões estratégicas.

O órgão consultivo, denominado Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, é composto por 23 representantes, incluindo membros da sociedade civil, proporcionando uma perspectiva plural na orientação das políticas relacionadas à proteção de dados.

Os órgãos de assistência direta e imediata ao Conselho Diretor incluem a Secretaria-Geral, a Coordenação-Geral de Administração e a Coordenação-Geral de Relações Institucionais e Internacionais, desempenhando papéis cruciais no suporte operacional e na gestão de relações institucionais.

Órgãos seccionais, como a Corregedoria, a Ouvidoria e a Procuradoria-Federal especializada, têm responsabilidades específicas, como a apuração de infrações internas, o recebimento de feedback da sociedade e o suporte jurídico, respectivamente.

Os órgãos específicos singulares, tais como a Coordenação-Geral de Normatização, a Coordenação-Geral de Fiscalização e a Coordenação-Geral de Tecnologia e Pesquisa, desempenham funções especializadas relacionadas à elaboração de normas, à fiscalização das atividades de tratamento de dados e à promoção de tecnologias e pesquisas no contexto da proteção de dados.

Essa estrutura organizacional abrangente reflete o compromisso da ANPD em abordar de maneira abrangente os desafios e oportunidades associados à proteção de dados pessoais, garantindo a eficácia na implementação da LGPD e promovendo uma cultura de respeito à privacidade no cenário nacional.

Caso a ANPD identifique práticas em desacordo com a LGPD, cabe a ela a aplicação de sanções administrativas previstas na Lei (Brasil, 2018), com o intuito de garantir a conformidade e promover a proteção dos direitos dos titulares dos dados.

Entre as sanções estão a advertência, multa, suspensão do tratamento de dados e a eliminação dos dados.

Conforme estabelecido no art. 55-J da lei 13.709/18 (Brasil, 2018), a atuação da Autoridade Nacional de Proteção de Dados vai muito além da simples imposição de penalidades, abrangendo aspectos normativos, interpretativos e educativos.

Quanto aos dados de saúde, a ANPD se torna fundamental na proteção da privacidade dos pacientes, tendo também o poder de fiscalizar as organizações que lidam com tais, incluindo instituições de saúde pública, laboratórios, e outras entidades do setor.

Por fim, destaca-se que ao estabelecer um ambiente regulatório claro e equilibrado, a ANPD promove a inovação responsável no setor da saúde, contribuindo para a manutenção da confiança da população no sistema de saúde pública.

5.5.2 Desafios e Oportunidades da LGPD nos Dados do SUS

O sistema de saúde brasileiro apresenta desafios, especialmente por adotar um modelo de acesso universal, equitativo e descentralizado. A complexidade é evidenciada pela participação de diversos atores e organizações, públicas ou privadas, no processo de saúde-doença dos cidadãos brasileiros. Isso demanda estratégias de organização e articulação na rede de atenção à saúde, tanto para encaminhamento assistencial quanto para a transmissão de dados de saúde. (Fantonelli *et al.*, 2021)

Na proteção de dados pessoais conforme estabelecido pela LGPD, as principais partes envolvidas são as seguintes: a) Titular de Dados: pessoa física que fornece seus dados pessoais ao consumir um produto ou serviço; b) Controlador: pessoa física ou jurídica que recebe os dados pessoais de um titular para realizar algum tratamento desses dados; c) Operador: pessoa física ou jurídica contratada pelo controlador para operar os dados dos titulares, executando atividades específicas de tratamento; d) Encarregado: indivíduo contratado pelo controlador, responsável por intermediar a comunicação entre as demais partes envolvidas, assegurando a conformidade com a LGPD; e) Autoridade Nacional de Proteção de Dados (ANPD): órgão governamental encarregado de fiscalizar e garantir a conformidade com as disposições da LGPD, promovendo a proteção efetiva dos dados pessoais.

Neste cenário, a implementação da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) é composta por diversos artigos que estabelecem princípios, direitos e obrigações relacionadas à coleta, armazenamento, processamento e compartilhamento de dados pessoais.

O artigo 6º da LGPD (Brasil, 2018) define princípios que devem nortear o tratamento de dados pessoais. Entre eles estão a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

Os arts. 7º e 11º da LGPD (Brasil, 2018) delineiam as circunstâncias em que os dados pessoais e dados pessoais sensíveis podem ser utilizados no contexto da saúde:

> Art. 7° O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses [...] VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. (Brasil, 2018)
>
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses [...] f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

Destaca- se, no entanto, que a legislação não estabelece uma definição clara para "tutela da saúde", nem fornece delineamentos precisos sobre quem são considerados profissionais de saúde, a natureza dos serviços de saúde e a autoridade sanitária, criando uma margem para potenciais usos inadequados.

Ainda quanto ao art. 11, o seu parágrafo 4º (Brasil, 2018) traz a proibição do uso de dados com o intuito de obter vantagem econômica, exceto quando se destinar à prestação de serviços de saúde ou assistência farmacêutica.

Já o parágrafo 5º do art. 11 (Brasil, 2018) veda às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. Essa restrição visa mitigar os riscos associados a tais práticas, que poderiam potencialmente ampliar situações de discriminação e desigualdade social, particularmente prejudicando grupos socialmente marginalizados.

O capítulo III da lei em seus artigos 17 e 18 confere aos titulares dos dados diversos direitos, como acesso às informações, correção de dados incompletos ou imprecisos, a exclusão de dados desnecessários ou tratados em desconformidade com a lei, além de informações sobre o compartilhamento.

No âmbito do SUS, o titular dos dados de saúde tem o direito de obter, a qualquer momento, informações claras e transparentes sobre quais dados estão sendo coletados, para quais finalidades e como estão sendo tratados.

O capítulo IV da LGPD (Brasil, 2018) trata especificamente sobre o tratamento dos dados pessoais pelo Poder Público, onde o art. 23 destaca que as pessoas jurídicas de direito público têm permissão para realizar o tratamento de dados, desde que esteja alinhado com sua finalidade pública, dentro das atribuições e competências legais. Para cumprir essa prerrogativa, é necessário informar ao cidadão sobre a finalidade, procedimentos e práticas adotadas no tratamento desses dados. Adicionalmente, o artigo institui a obrigação de designar um Encarregado, responsável por esclarecer dúvidas dos titulares e orientar os profissionais quanto ao manejo adequado dos dados.

O art. 25 da Lei (Brasil, 2018) trata da necessidade de manter os dados em formato interoperável e estruturado para uso compartilhado, o que possibilita a execução de políticas públicas, prestação de serviços públicos e a disseminação e acesso das informações pelo público em geral.

De acordo com o artigo 7º (Brasil, 2018), a administração pública está autorizada a processar dados quando isso visa a execução de políticas públicas previstas em leis, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Nesse contexto, o consentimento do titular dos dados torna-se dispensável. Entretanto, para a comunicação e o compartilhamento de dados é exigida a obtenção do consentimento do titular, a menos que haja previsão legal para tal exceção, como no caso de dados públicos ou na execução descentralizada respaldada contratualmente e com um fim específico, conforme estabelecido no artigo 27 (Brasil, 2018).

No contexto da saúde pública, pode haver situações em que o processamento de dados pessoais sensíveis é necessário para fins de interesse público, como o monitoramento e controle de epidemias, a implementação de políticas de vacinação ou a condução de pesquisas científicas relacionadas à saúde. Em tais casos, o artigo

27 pode oferecer bases legais específicas para o tratamento desses dados, mesmo sem o consentimento explícito do titular.

Ao observar os princípios e agir em conformidade com a LGPD (Brasil, 2018) há uma oportunidade para promover a confiança dos titulares de dados e manter a reputação e a integridade das instituições, demonstrando o compromisso com a proteção dos direitos dos indivíduos.

No entanto, para atuar em conformidade com a LGPD, a rede de saúde pública deve adotar uma abordagem que vá desde a coleta até o armazenamento e o compartilhamento de dados. Isso leva a implementação de políticas claras relacionadas à privacidade e segurança da informação, juntamente com investimentos substanciais em tecnologia e no aprimoramento da capacitação dos profissionais envolvidos (Lima; Gonçalves; Costa, 2021).

5.5.3 Da previsão de Anonimização e Pseudonimização dos dados

A Lei Geral de Proteção de Dados (LGPD) incorpora a segurança como um dos seus dez princípios gerais (Brasil, 2018), estabelecendo que os agentes de tratamento devem implementar medidas técnicas, administrativas e de segurança capazes de resguardar os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, tais como destruição, perda, alteração, comunicação, difusão ou qualquer outra forma de tratamento inadequado ou ilícito (Brasil, 2018).

Uma das estratégias para salvaguardar a privacidade de indivíduos em bases de dados reside na utilização de técnicas de anonimização e pseudonimização, as quais podem ser compreendidas como a alteração ou eliminação de informações nas bases de dados, tornando impossível a identificação dos indivíduos.

Estes métodos são comumente executados por meio de três abordagens distintas: 1) supressão, que implica na remoção de categorias específicas de dados sensíveis da base de dados; 2) substituição, que engloba a troca de dados sensíveis por informações não sensíveis ou fictícias; e 3) generalização, que se concretiza pela substituição de dados particulares por categorias mais abrangentes. A título de exemplo, a idade dos indivíduos pode ser representada por intervalos, como "entre 20 e 30 anos" (Souza; Coutinho; Albuquerque, 2020).

A anonimização de dados, de acordo com o art. 5º, inc. XI da LGPD (Brasil, 2018), envolve o uso de meios técnicos razoáveis e disponíveis no momento do

tratamento com o objetivo de garantir que os dados percam a possibilidade de associação direta ou indireta a um indivíduo. Ainda, de acordo com o art. 12 da Lei (Brasil, 2018), salvo exceções, os dados que passaram pelo processo de anonimização não são mais considerados pessoais para os fins da Lei.

Assim, um dado só é considerado anonimizado quando perde definitivamente a possibilidade de identificar uma pessoa natural, sendo tal processo irreversível.

No contexto de dados de saúde, a prática da anonimização é especialmente significativa na medida em que permite que informações sensíveis sejam utilizadas para pesquisa, estatísticas e políticas de saúde, ao mesmo tempo em que preserva a identidade dos titulares.

Destaca-se que a ausência de procedimentos de anonimização dos dados que trafegam entre instituições de saúde em todas as instâncias federativas, sobretudo em municípios ou comunidades com populações reduzidas, configura uma situação potencialmente problemática. Em contextos nos quais o número de titulares é limitado, os riscos de identificação dos indivíduos tornam-se consideravelmente mais significativos (Aragão; Schiochchet, 2020).

O Artigo 13 da LGPD (Brasil, 2018) também é de extrema importância na medida que incorpora a pseudonimização como uma ferramenta alternativa para a condução de estudos em saúde pública. A pseudonimização de dados refere-se à prática de tornar impossível a associação direta ou indireta de um dado a um indivíduo, utilizando informações adicionais ou suplementares mantidas pelo controlador em um ambiente seguro e controlado, conforme estipulado pelo parágrafo 4º.

Assim, a pseudonimização requer a exclusão dos identificadores pessoais dos dados, sendo substituídos por identificadores artificiais, elementos que codificam e dissociam as informações do titular. Essa técnica não se limita à pseudonimização de nomes, podendo ser aplicada a qualquer tipo de dado. Tal procedimento não apenas preserva a confidencialidade dos dados, mas também facilita a gestão eficaz da privacidade, abrangendo um espectro mais amplo de informações sensíveis além dos nomes.

Por ser a pseudonimização uma forma de simulação de apagamento pode haver um processo de reversão. Caso aconteça a reversão, o titular é exposto e o tratamento adequado deve ser colocado em prática.

Embora a anonimização e a pseudonimização sejam técnicas de mascaramento de dados, existem contextos em que a escolha entre uma e outra é

determinante para a adequação do processo. A opção pela anonimização revela-se mais apropriada quando o controlador não necessita mais conduzir o tratamento de dados pessoais, mas busca realizar análises sobre as atividades dos titulares de maneira genérica, sem envolver qualquer dado que possa identificar individualmente o titular. Por outro lado, a pseudonimização demonstra utilidade ao aumentar a segurança dos dados durante o seu tratamento pelo controlador, ocultando informações de identificação para operadores que não necessitam desses detalhes. (Xavier, 2021).

Tendo em vista que o mascaramento de dados usando anonimização ou pseudonimização pode ser um grande aliado na proteção de dados pessoais, a Autoridade Nacional de Proteção de Dados (ANPD) manifestou a intenção de aprofundar-se nesses temas e os incluiu como uma das principais áreas de foco na Agenda Regulatória para o biênio 2023-2024.

6 PONDERAÇÃO ENTRE O DIREITO À SAÚDE E O DIREITO À PRIVACIDADE DOS DADOS

A harmonização do direito à saúde com o direito à privacidade dos dados pessoais é um desafio contemporâneo que exige uma abordagem equilibrada e cuidadosa. As inovações tecnológicas na área da saúde trazem inúmeros benefícios, como a melhoria na precisão dos diagnósticos e a eficiência nos tratamentos, mas também envolvem a coleta e o tratamento de dados pessoais sensíveis, o que demanda uma proteção rigorosa para evitar abusos e violações da privacidade.

A Lei Federal nº 8.080/1990, a qual regulamenta o direito à saúde, inclui o direito à informação do cidadão e o dever do Estado de fundamentar suas políticas e ações em informações sanitárias e evidências científicas, legitimando assim a coleta e uso de informações pessoais (Ventura; Coeli, 2018).

O direito à privacidade é um direito fundamental de natureza individual, que se revela no conjunto de informações que a pessoa opta por manter em seu controle ou comunicar apenas a quem lhe aprouver, sem sujeição legal, abrangendo, inclusive, as relações familiares e afetivas, hábitos, imagem e pensamentos (Silva, 2014, p. 208).

Por sua vez, o direito fundamental à saúde é caracterizado como um direito coletivo, sendo um dever do Estado assegurá-lo à população. Essa garantia se efetiva por meio da implementação de políticas públicas, promoção de acesso indiscriminado a todos e prestação de serviços voltados para a redução de doenças.

Os dados pessoais na área da saúde desempenham uma função que transcende a mera proteção da privacidade, visando à proteção de um bem comum. A noção de bem comum na saúde está intrinsecamente ligada ao interesse coletivo, delineando os valores e parâmetros que devem guiar o uso e a divulgação dos dados pessoais como um bem jurídico protegido. Isso visa assegurar, predominantemente, a satisfação das necessidades coletivas, estabelecendo um equilíbrio entre a proteção da privacidade individual e a promoção do bem-estar da comunidade como um todo.

Assim, direitos fundamentais que coexistem de maneira harmônica podem, no contexto democrático e pluralista, gerar antinomias, tal como na colisão entre o direito à privacidade e o direito à saúde. Ambos os direitos são de igual importância e se dirigem ao mesmo fim: a promoção do bem-estar e da dignidade humana.

Ignorar a importância da privacidade em nome da saúde significa deixar de enfrentar o verdadeiro problema. Pacientes que desconfiam da proteção de seus dados podem omitir informações determinantes para o diagnóstico e tratamento. Normalmente, a falta de uma política robusta de proteção de dados e a omissão ou conivência do Poder Público agravam a situação, já que a alternativa – desenvolver sistemas seguros e transparentes – é mais complexa e onerosa.

Percebe-se que a colisão entre esses direitos fundamentais tem como principal raiz a ineficiência do Estado em promover políticas públicas adequadas tanto para a proteção da saúde quanto para a privacidade dos dados. Isso leva o Judiciário a intervir para solucionar o problema no caso concreto, considerando a ponderação de valores e interesses.

Esta ideia é trazida pelo constitucionalista Fernandes (2019, p. 158), que assim expõe:

> Destarte, em face de uma colisão entre princípios, o valor decisório será dado a um princípio que tenha, naquele caso concreto, maior peso relativo, sem que isso signifique invalidação daquele compreendido como de peso menor. Para Alexy, nesses termos, teríamos que observar a lei da ponderação: “Quanto maior é o grau de não satisfação ou de afetação de um princípio, tanto maior deve ser importância da satisfação do outro”. Em face de outro caso, portanto, o peso dos princípios poderá se redistribuído de maneira diversa, pois nenhum princípio goza antecipadamente de primazia (precedência incondicionada) sobre os demais.

A abordagem teórica de Robert Alexy (2008), renomado jurista alemão, surge como uma referência sólida. Fundamentada na jurisprudência da Alemanha, sua proposta enfatiza o uso da técnica da ponderação e do princípio da proporcionalidade como meios eficazes para enfrentar o desafio da colisão entre direitos fundamentais, especialmente quando estes são estruturados como princípios.

Alexy (2008) sustenta que todos os princípios, em sua abstração, possuem igual relevância. Em situações de conflito entre esses princípios, preconiza-se a análise minuciosa das circunstâncias fáticas e jurídicas do caso em questão, a fim de determinar qual princípio deve ser privilegiado ao final do processo de ponderação.

> Se dois princípios colidem - o que ocorre, por exemplo, quando algo é proibido de acordo com um princípio e, de acordo com o outro, permitido -, um dos princípios terá que ceder. Isso não significa, contudo, nem que o princípio cedente deva ser declarado inválido, nem que nele deverá ser introduzida uma cláusula de exceção. Na verdade, o que ocorre é que um dos princípios

> tem precedência em face do outro sob determinadas conduções. Sob outras condições a questão da precedência pode ser resolvida de forma oposta. Isso é o que se quer dizer quando se afirma que, nos casos concretos, os princípios têm pesos diferentes e que os princípios com maior peso têm precedência. (Alexy, 2008, p. 95)

A resolução de conflitos entre princípios não exige a exclusão de nenhum princípio, mas sim uma ponderação proporcional de seus valores ou pesos, conforme definido por Alexy (2015) na "lei de colisão". Segundo Alexy (2015), conflitos de interesse baseados em princípios são resolvidos através de um sopesamento entre os princípios conflitantes, sem que haja uma prioridade intrínseca entre eles. No caso concreto, essa colisão de princípios é resolvida pela ponderação, onde se busca otimizar os princípios para alcançar um bem maior para a sociedade. O Princípio da Proporcionalidade é frequentemente utilizado como critério de ponderação para determinar qual princípio é mais justo na situação específica (Martins, 2017).

A técnica de balanceamento, sopesamento ou ponderação foi pioneiramente aplicada pelo Tribunal Constitucional Alemão, tendo sua estreia registrado no caso Lüth em 1958. Assim decidindo, o Tribunal Constitucional Alemão estabeleceu dois postulados que têm sido seguidos até hoje: 1|) os direitos fundamentais garantidos pela Constituição exercem influência em toda a legislação ordinária, implicando que toda interpretação da ordem jurídica deve ser conduzida à luz da Constituição, mesmo em casos envolvendo relações entre particulares (eficácia horizontal dos direitos fundamentais constitucionais); 2) a ponderação é um método de resolução aplicado a casos complexos nos quais normas constitucionais, estruturadas como princípios, entram em conflito (Cardoso, 2016).

Essa abordagem de ponderação e proporcionalidade entre princípios têm encontrado eco no Brasil, sendo amplamente adotada não apenas pela doutrina jurídica, mas também pelo Poder Judiciário, como instrumento essencial na busca por soluções que conciliam interesses divergentes, preservando a coerência do ordenamento jurídico e garantindo a efetiva proteção dos direitos fundamentais dos cidadãos.

Na prática judicial, a aplicação da técnica de ponderação exige uma análise detalhada e contextualizada do caso concreto. O julgador deve considerar todas as circunstâncias relevantes, os valores em jogo e as consequências das diferentes soluções possíveis. A decisão deve ser bem fundamentada, demonstrando

claramente como os princípios da proporcionalidade e da concordância prática foram aplicados para alcançar uma solução justa e equilibrada.

Entretanto, o Supremo Tribunal Federal, ao analisar os casos que lhe são apresentados, não vem mantendo a coerência na adoção da tese alexyana, frequentemente empregando-a sem critério metodológico adequado e de maneira equivocada. Esse uso inadequado resulta em uma interpretação das premissas teóricas do autor como uma possibilidade inadequada de ato de escolha do julgador, caracterizando um verdadeiro solipsismo judicial. Dessa forma, o balanceamento é utilizado como um "artifício mágico", uma espécie de "método coringa" de motivação judicial (Pedron; Rodrigues, 2022).

A técnica de ponderação, quando aplicada à proteção de dados pessoais e ao direito de acesso à informação pública, envolve um teste de dano e interesse público. Trata-se de sopesar o interesse público na transparência contra o interesse na proteção da privacidade e da autodeterminação informativa dos titulares dos dados. A legislação espanhola reconhece a importância de diferentes níveis de proteção de dados pessoais, de acordo com a sensibilidade das informações e o grau potencial de dano à esfera privada decorrente de seu acesso público. Esse modelo pode servir de referência para o Brasil, ao definir critérios de ponderação que promovam um equilíbrio justo entre transparência e privacidade, assegurando que nenhum direito seja sacrificado além do necessário para proteger o outro (Bento, 2020).

Assim, a harmonização do direito à saúde com o direito à privacidade dos dados pessoais é essencial para assegurar que as inovações tecnológicas em saúde beneficiem a sociedade sem comprometer a dignidade e a autonomia dos indivíduos. A adoção de políticas e práticas robustas de proteção de dados, juntamente com uma abordagem ética e transparente, pode promover um ambiente onde ambos os direitos fundamentais coexistam de maneira equilibrada e eficaz.

6.1 A PROTEÇÃO DE DADOS DOS PACIENTES NO CONTEXTO DA SARA

Conforme o Plano de Trabalho da implantação do assistente virtual SARA em Guarapuava, a proteção dos dados dos pacientes é considerada uma prioridade, seguindo estritamente os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normativas vigentes.

O plano estabelece que a ferramenta SARA deve atender a todos os princípios da LGPD, garantindo a privacidade e o anonimato dos pacientes atendidos. Os dados coletados serão anonimizados para evitar qualquer associação direta com os indivíduos, a menos que seja necessário para fins específicos de atendimento médico, assegurando que sejam utilizados exclusivamente para finalidades relacionadas ao atendimento de saúde e nunca para outros fins não autorizados.

O acesso aos dados dos pacientes é restrito às equipes imediatas de operação vinculadas à Secretaria de Saúde, controlado e limitado exclusivamente à finalidade de prestação de assistência à saúde, evitando qualquer uso indevido ou não autorizado.

Além disso, o uso da ferramenta exigirá que os pacientes aceitem os termos de uso, incluindo o consentimento informado para o tratamento de seus dados conforme a LGPD, assegurando que eles estejam cientes de como suas informações serão utilizadas, protegidas e mantidas. O plano também reforça que os dados coletados serão usados exclusivamente para prestar assistência médica e melhorar a gestão da saúde pública no município.

O plano de trabalho prevê ainda a utilização de um painel de gestão em tempo real para monitoramento dos atendimentos, priorizando casos de maior risco aparente, sempre dentro dos limites de privacidade estabelecidos pela LGPD.

Conforme informações da Secretaria de Saúde de Guarapuava, todos os dados transmitidos entre o assistente SARA e os sistemas de saúde são protegidos por criptografia TLS (Transport Layer Security), o que impede a interceptação ou alteração das informações durante a transferência. Além disso, os dados armazenados nos servidores são protegidos por criptografia AES-256, garantindo que, mesmo que alguém consiga acessar os servidores sem autorização, esses dados permaneçam inacessíveis sem as chaves de criptografia corretas.

A autenticação multifator (MFA) e o gerenciamento de acessos baseado em funções (RBAC) são medidas implementadas para assegurar que apenas indivíduos autorizados tenham acesso aos dados dos pacientes. No SARA, médicos e demais profissionais de saúde que necessitam acessar informações sensíveis devem passar por um processo de autenticação que exige mais de uma forma de verificação de identidade, como uma combinação de senhas, tokens físicos ou biometria. O SARA também utiliza um sistema de gerenciamento de acessos baseado em funções (RBAC), onde cada usuário possui permissões específicas de acordo com suas

responsabilidades. Isso assegura que os profissionais só tenham acesso às informações necessárias para realizar suas tarefas, minimizando o risco de acesso indevido.

O compromisso do SARA com a privacidade dos dados dos pacientes é refletido em suas políticas de privacidade rigorosas, orientadas pelo princípio da minimização de dados, que prevê a coleta e o processamento apenas dos dados estritamente necessários para os fins pretendidos. A política de privacidade também garante que os pacientes sejam informados de maneira transparente sobre o uso de seus dados. Antes de qualquer dado ser coletado ou processado, é necessário que o paciente forneça consentimento explícito, alinhando-se aos requisitos das legislações de proteção de dados, como a LGPD e a GDPR.

Ainda, o sistema SARA é submetido a auditorias regulares de segurança e a um monitoramento contínuo destinado a identificar atividades suspeitas, assegurando a conformidade com as normas de proteção de dados.

Percebe-se então que tais medidas visam proteger os direitos dos pacientes e criar um ambiente seguro e confiável para o uso de tecnologias de saúde digital, promovendo um atendimento eficiente e seguro, centrado no cidadão.

6.2 PROPOSTAS PARA O APRIMORAMENTO DA PRIVACIDADE DOS DADOS SEM COMPROMETER O DIREITO À SAÚDE

A proteção à privacidade dos dados pessoais no setor de saúde é um desafio crescente em um cenário onde a tecnologia se torna cada vez mais essencial para o atendimento de qualidade e a gestão eficiente.

O uso intensivo de sistemas digitais, inteligência artificial, e o armazenamento massivo de informações médicas proporcionam uma série de benefícios, como a personalização do atendimento, a melhoria dos processos de diagnóstico, e a otimização de recursos.

O setor de saúde lida com dados sensíveis, como históricos médicos, resultados de exames e informações genéticas, cujo uso ou divulgação inadequada pode levar a discriminações, estigmatização ou até mesmo consequências financeiras para os indivíduos.

O aprimoramento da privacidade dos dados pessoais no setor de saúde é essenciais para garantir a confiança dos pacientes e a eficiência dos serviços de

saúde. Para alcançar esse equilíbrio, é necessário implementar políticas de governança de dados que estabeleçam diretrizes claras para a coleta, armazenamento, uso e compartilhamento de informações de saúde.

Essas políticas devem ser éticas e estar em conformidade com a legislação vigente, como a Lei Geral de Proteção de Dados (LGPD), garantindo que todas as operações com dados pessoais sejam conduzidas de maneira responsável.

6.2.1 Conscientização dos cidadãos sobre a privacidade individual

A coleta e o processamento em massa de dados pessoais expõem os cidadãos a diversos riscos, incluindo o uso indevido das informações e ataques cibernéticos.

É necessário que todos compreendam seus direitos à privacidade e saibam como exercê-los. A conscientização é o primeiro passo para a proteção individual e coletiva, promovendo um ambiente digital mais seguro e responsável.

Para efetivar a conscientização, é necessário um esforço conjunto que inclua campanhas de educação pública, utilizando diversos meios de comunicação para disseminar informações sobre a LGPD e os direitos de privacidade. Também é essencial investir em programas de capacitação em segurança digital para diferentes públicos, como estudantes, profissionais e idosos, abordando práticas seguras de navegação e proteção de dados. Além disso, deve-se incentivar as organizações a serem claras e transparentes sobre suas práticas de coleta e uso de dados, facilitando o entendimento e a confiança dos consumidores. Por fim, a colaboração entre governo, setor privado e ONGs é fundamental para desenvolver e distribuir materiais educativos acessíveis e de fácil compreensão.

Assim, um processo educativo, contínuo e abrangente, deve ser visto como um investimento na proteção dos dados pessoais e na construção de uma cultura de privacidade no Brasil.

6.2.2 Do Consentimento Informado

O Guia de Boas Práticas Clínicas adotado pela OMS em 1995 apresentou soluções importantes para a proteção da privacidade dos pacientes e dos participantes de ensaios clínicos. Tal documento foi criado com o objetivo de harmonizar os padrões de ensaios clínicos em diversos países das Américas, e aborda várias diretrizes e responsabilidades relacionadas à condução de ensaios clínicos, enfatizando a importância de garantir a integridade científica e ética dos estudos.

Segundo o guia, o consentimento informado é o processo pelo qual o sujeito confirma voluntariamente sua participação após ser informado sobre os aspectos relevantes do estudo, consistindo em um documento escrito que deve ser claro e compreensível para o participante.

O processo de consentimento inclui fornecer informações claras, precisas e compreensíveis, garantindo que o sujeito entenda o propósito do estudo, os procedimentos, riscos, benefícios, alternativas e seus direitos. O consentimento deve ser obtido antes da participação e deve cumprir as exigências regulatórias aplicáveis e os princípios éticos da Declaração de Helsinki[2]. Novas informações relevantes devem ser comunicadas ao sujeito de forma oportuna. O consentimento deve ser voluntário, sem coerção, e deve garantir a privacidade dos dados do sujeito. Em situações de emergência, o consentimento do representante legal pode ser solicitado, e, em caso de alterações significativas no estudo, o consentimento deve ser atualizado e novamente obtido.

Os principais propósitos deste processo são assegurar que o sujeito controla a decisão de participar ou não da pesquisa clínica e garantir que este participe apenas quando a pesquisa for consistente com seus interesses, valores e preferências.

Nesse contexto, o titular dos dados deve ter acesso amplo e claro às ah tá informações sobre o tratamento dos seus dados, de modo a visualizar, de forma transparente, a legalidade, a legitimidade e a segurança deste tratamento, conforme seu propósito, adequação e necessidade. Esse acesso capacita o titular a refletir

[2] A Declaração de Helsinque foi criada pela Associação Médica Mundial e dispõe sobre ética em procedimentos de pesquisas clínicas com seres humanos. Cita a proteção da saúde do paciente como primeiro dever do médico em pesquisas deste tipo e a importância da consciência ética por parte dos pesquisadores.

sobre o tratamento dos seus dados e a tomar decisões informadas, alinhadas com seus direitos. A transparência no tratamento de dados pessoais deve ser diretamente proporcional à sua magnitude (tanto qualitativa quanto quantitativamente) e à capacidade de compreensão dos titulares em relação aos novos e dinâmicos produtos e serviços oferecidos para seu uso. (Maldonado; Blum, 2019).

Assim, a transparência promovida pelo consentimento informado fortalece a confiança dos pacientes, enquanto a conformidade com regulamentações como a LGPD assegura a legalidade do processamento de dados. A segurança dos dados é aprimorada, pois o consentimento define claramente as responsabilidades das partes envolvidas, estabelecendo medidas de proteção, garantindo que os dados sejam utilizados de forma ética e apropriada.

6.2.3 Das Técnicas de Anonimização e Pseudonimização

As técnicas de anonimização e pseudonimização são essenciais para a proteção de dados de pacientes no setor de saúde, oferecendo soluções práticas e eficazes para preservar a privacidade e a segurança das informações pessoais. Tais métodos previstos na Lei Geral de Proteção de Dados (LGPD) reduzem os riscos associados a vazamentos de dados e ciberataques, contribuindo para um ambiente mais seguro e confiável no setor de saúde.

A anonimização transforma os dados pessoais de forma que a identificação do indivíduo se torne impossível, garantindo que a privacidade dos pacientes seja mantida. Por não serem mais considerados dados pessoais sob a LGPD, os dados anonimizados estão isentos de diversas exigências legais, o que simplifica a conformidade regulatória e permite seu uso em pesquisas sem comprometer a privacidade dos pacientes.

A pseudonimização, por sua vez, trata os dados pessoais de maneira que eles não possam ser associados diretamente a um indivíduo específico sem informações adicionais que são mantidas separadas. Essa técnica aumenta a segurança dos dados ao dificultar a identificação direta dos pacientes, ao mesmo tempo em que permite que os dados sejam utilizados de forma controlada e revertidos para sua forma original quando necessário. Isso é particularmente útil em ambientes de saúde onde a identificação do paciente pode ser imprescindível em determinados contextos.

Em suma, a aplicação dessas técnicas no setor de saúde não apenas atende às exigências da LGPD, mas também promove um uso ético e seguro dos dados dos pacientes, protegendo suas informações contra acessos não autorizados e ciberataques. Dessa forma, a anonimização e a pseudonimização são ferramentas vitais para criar um ambiente de confiança e segurança, essencial para o avanço das pesquisas e a prestação de serviços de saúde de qualidade.

6.2.4 Realização de auditorias

A Realização de auditorias regulares também se faz necessária para garantir que as práticas de gestão de dados estejam em conformidade com as políticas de privacidade e segurança.

Independentemente de suas diversas modalidades, a auditoria consiste em um processo sistemático, crítico e contínuo, que analisa as ações e decisões de pessoas e instituições que prestam serviços na área de saúde, visando à otimização da gestão administrativa por meio da verificação e controle dos processos e resultados. Seu objetivo é garantir o maior benefício, o menor risco e a máxima eficiência possíveis, buscando assegurar que os benefícios estejam em conformidade com as disposições planejadas, normas e legislações vigentes. (Melo; Vaistman, 2008).

Durante as auditorias, são avaliados os sistemas e processos utilizados para a gestão de dados, com o objetivo de identificar quaisquer vulnerabilidades ou falhas de segurança. Isso pode incluir a detecção de configurações incorretas, software desatualizado, ou práticas inadequadas de gerenciamento de acesso.

Assim, as auditorias regulares ajudam a assegurar que todas as práticas de gestão de dados estejam alinhadas com as políticas estabelecidas de privacidade e segurança. Isso inclui verificar se os procedimentos de coleta, armazenamento, processamento e compartilhamento de dados estão sendo realizados de acordo com as regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD).

6.2.5 Mecanismos de fiscalização e aplicação de sanções

A elaboração de mecanismos de fiscalização contínua permite uma resposta rápida e eficiente a potenciais incidentes de segurança, minimizando o risco de vazamentos de dados e outras violações de privacidade, podendo incluir sistemas automatizados de monitoramento que detectam atividades suspeitas ou anômalas em tempo real, como tentativas de acesso não autorizado ou movimentações incomuns de dados.

A Lei Geral de Proteção de Dados (LGPD) estabeleceu um sistema de monitoramento e punição, visando assegurar a conformidade com os padrões de proteção de dados definidos e responsabilizar aqueles que violam as regras, sendo a ANPD a agência encarregada de supervisionar a conformidade no Brasil, possuindo autoridade para conduzir investigações, monitorar práticas corporativas, receber reclamações, aplicar sanções e desenvolver diretrizes de proteção de dados pessoais.

Além das sanções administrativas que vão de advertência até multas significativas (Brasil, 2018) a LGPD também possibilita ações judiciais individuais ou coletivas em casos de violação de dados pessoais. Os usuários têm o direito de buscar indenização por danos materiais, morais ou coletivos decorrentes da violação de seus dados pessoais. Essa oportunidade de ação judicial reforça a importância da proteção de dados e oferece aos usuários meios para buscar reparação em caso de violação de sua privacidade.

No entanto, se torna imprescindível a existência de uma infraestrutura robusta e eficiente para a implementação prática do regulamento e sua efetiva utilidade, já que a mera existência da legislação não é suficiente, sendo necessário um sistema eficaz de aplicação e fiscalização.

6.2.6 Infraestruturas De Segurança Cibernética

A vulnerabilidade da estrutura cibernética é agravada pelo uso de senhas fracas, falhas em softwares, serviços de rede instáveis, interfaces inseguras, falta de atualização, componentes desatualizados e proteção de privacidade insuficiente. A transferência inadequada de dados, controle deficiente de dispositivos, configurações padrão vulneráveis e segurança física insuficiente expõem os sistemas a acessos não

autorizados, comprometendo a privacidade, autenticidade e acessibilidade das informações sensíveis (Tenaglia, 2024).

Entre os mecanismos de fiscalização, a criptografia é uma técnica fundamental para proteger dados sensíveis durante a transmissão e o armazenamento. Ela assegura que somente indivíduos autorizados possam acessar e interpretar esses dados.

Quando os dados são criptografados, eles são transformados em um formato ilegível para qualquer pessoa que não possua a chave de decriptação apropriada. Por exemplo, se um registro médico foi interceptado durante a transmissão entre um hospital e um laboratório, ele não poderá ser decifrado sem a chave correta.

Apesar dos benefícios, a criptografia também apresenta desafios, onde a perda das chaves decriptação forem perdidas poderão tornar os acessos aos dados inacessíveis permanentemente.

Investir em medidas de segurança cibernética, como firewalls, sistemas de detecção de intrusão e práticas rigorosas de controle de acesso também é importante para proteger os sistemas de TI das instituições de saúde contra-ataques cibernéticos. Firewalls atuam como barreiras de segurança que controlam o tráfego de rede entre diferentes zonas de segurança, monitorando e filtrando o tráfego com base em regras predefinidas.

Existem diversos tipos de firewalls, incluindo os de rede, que protegem redes inteiras, e os de aplicação, que monitoram o tráfego de dados de aplicações específicas. A implementação de firewalls previne acessos não autorizados e contra-ataques cibernéticos, como tentativas de invasão e disseminação de malware.

Os sistemas de detecção de intrusão (IDS) monitoram a rede ou sistemas em busca de atividades suspeitas ou violações de políticas de segurança, alertando os administradores quando detectam comportamentos anômalos ou potencialmente maliciosos. Existem IDS baseados em assinaturas, que detectam ataques conhecidos ao comparar padrões de tráfego com uma base de dados, e os baseados em anomalias, que identificam atividades anômalas ao comparar o comportamento atual da rede com um perfil esperado. IDS são fundamentais para a detecção precoce de ameaças e permitem respostas rápidas a incidentes de segurança, minimizando danos potenciais.

Práticas rigorosas de controle de acesso garantem que apenas usuários autorizados possam acessar informações sensíveis. Métodos como a autenticação

multifatorial (MFA), que requer múltiplas formas de verificação, e o princípio do menor privilégio, que concede aos usuários apenas os privilégios necessários para suas funções, são essenciais. O gerenciamento de identidades e acessos (IAM) permite controlar de forma centralizada as identidades digitais e os direitos de acesso dos usuários. O controle de acesso adequado impede que indivíduos não autorizados obtenham acesso a dados sensíveis, protegendo a confidencialidade e a integridade das informações.

Assim, medidas de segurança cibernética que protegem a privacidade e a integridade dos dados dos pacientes asseguram a continuidade e a eficiência dos serviços de saúde e reforçam a confiança dos pacientes.

6.2.7 Treinamento Adequado Dos Profissionais

O comportamento humano é um dos fatores críticos quando se trata de segurança dos dados, onde erros humanos, práticas inadequadas e até mesmo a falta de conhecimento podem gerar possíveis violações, aumentando a vulnerabilidade dos sistemas e das informações.

Para diminuir esses riscos, a educação e o treinamento contínuos dos profissionais de saúde são fundamentais para garantir a proteção dos dados pessoais dos pacientes e a eficiência dos serviços de saúde. Capacitar esses profissionais sobre a importância da privacidade dos dados e as melhores práticas para protegê-los é essencial em um cenário onde a tecnologia e a digitalização dos sistemas de saúde estão em constante evolução.

Profissionais de saúde, incluindo médicos, enfermeiros, administradores e técnicos, lidam diariamente com uma quantidade significativa de informações sensíveis. Sem o devido treinamento, eles podem estar vulneráveis a erros que comprometam a privacidade dos pacientes. A conscientização sobre a legislação vigente, como a Lei Geral de Proteção de Dados (LGPD), e a compreensão dos princípios básicos de segurança da informação são passos essenciais para prevenir incidentes de segurança.

Ainda, a criação de normas, formais ou informais, é essencial para orientar os colaboradores de uma instituição de saúde quanto à privacidade das informações, tanto da instituição como um todo quanto das informações específicas dos pacientes contidas nos prontuários eletrônicos. Essas normas podem ser internas,

desenvolvidas pela própria instituição, ou podem incorporar normas externas reconhecidas. Exemplos de documentos normativos que abordam questões legais e éticas da profissão incluem os códigos de ética médica e de enfermagem, os quais fornecem diretrizes fundamentais para a conduta dos profissionais de saúde em relação à privacidade da informação (Magnano, 2015).

Assim, a implementação de uma cultura de privacidade e segurança dentro das instituições de saúde fortalece a confiança dos pacientes no sistema de saúde. Quando os pacientes sabem que suas informações estão sendo tratadas com cuidado e respeito, eles são mais propensos a compartilhar informações completas e precisas, o que é essencial para um diagnóstico e tratamento eficazes.

7. CONSIDERAÇÕES FINAIS

A presente dissertação analisou a relação entre o avanço tecnológico e a concretização do direito social à saúde, enfatizando a aplicação de tecnologias como a inteligência artificial (IA) na saúde pública brasileira. A pesquisa demonstrou que as inovações tecnológicas têm o potencial de transformar significativamente a gestão e a prestação de serviços de saúde, proporcionando melhorias substanciais na eficiência, precisão dos diagnósticos e personalização dos tratamentos.

Entre as inovações tecnológicas analisadas, destacou-se o papel da assistente virtual SARA, um sistema baseado em inteligência artificial que foi projetado para apoiar a gestão de saúde pública na cidade de Guarapuava-PR.

Ao analisar as propostas apresentadas neste trabalho para o aprimoramento da privacidade dos dados sem comprometer o direito à saúde, é possível observar que a plataforma SARA atende a diversos aspectos fundamentais, embora ainda existam pontos que demandam melhorias. A SARA implementa um sistema que informa os pacientes sobre os termos de uso e privacidade antes da utilização, aplica técnicas de proteção de dados, como a anonimização de informações pessoais em relatórios e a pseudonimização para acesso interno por profissionais de saúde, e promove a capacitação dos profissionais de saúde para o uso seguro da plataforma. A plataforma também conta com mecanismos de segurança digital, como sistemas de autenticação e criptografia, alinhados às boas práticas de proteção de dados sensíveis, e realiza auditorias regulares para garantir conformidade com legislações como a LGPD.

Contudo, ainda falta um programa abrangente de educação digital para conscientizar os cidadãos sobre a importância da privacidade e os riscos associados ao compartilhamento de dados pessoais. Além disso, não está plenamente documentado se a plataforma inclui mecanismos de fiscalização e aplicação de sanções em caso de violações ou não conformidade às normas, e ainda carece de integração com um ecossistema mais amplo de governança de dados para garantir que as diretrizes nacionais sejam implementadas de forma integral e eficiente.

Assim, embora a SARA seja um modelo de sucesso na aplicação de tecnologia para melhorar o acesso à saúde, respeitando em grande parte os princípios de proteção de dados e privacidade, avanços adicionais são necessários.

Por fim, recomenda-se a realização de estudos futuros que explorem mais detalhadamente os impactos sociais e econômicos da integração de tecnologias como a SARA na saúde pública, bem como o desenvolvimento de mecanismos mais eficazes para a proteção de dados e privacidade. A continuidade da pesquisa nessa área é essencial para garantir que as inovações tecnológicas contribuam de forma positiva e sustentável para a concretização do direito à saúde no Brasil.

Assim, conclui-se que a gestão tecnológica na saúde pública, exemplificada pelo uso da assistente virtual SARA, representa um caminho promissor para a concretização do direito social à saúde, desde que acompanhada de uma robusta estrutura de proteção de dados e um compromisso contínuo com os princípios éticos e legais.

REFERÊNCIAS

ABREU, T. S. N. Análise jurídica do artigo 196 da Constituição Federal de 1988, à luz da jurisprudência do Supremo Tribunal Federal. **Cadernos Ibero-Americanos de Direito Sanitário**, [s. l.], v. 3, n. 3, p. 50–61, 2014. DOI: 10.17566/ciads.v3i3.53

ALEXY, R. A **Teoria dos direitos fundamentais**. São Paulo: Editora Malheiros, 2008.

ALEXY, R. Colisão de direitos fundamentais e realização de direitos fundamentais no Estado de Direito Democrático. **Revista de Direito Administrativo**, Rio de Janeiro, v. 217, 2015.

ALVES FILHO, F. C. Pluralismo jurídico global: reflexões na era das big techs e a proteção de dados. **Revista Contemporânea**, [S. l.], v. 3, n. 12, p. 28760-28786, 2023.

ARAGÃO, S. M.; SCHIOCCHET, T. Lei geral de proteção de dados: desafio do sistema único de saúde. **Revista Eletrônica de Comunicação**: Informação e Inovação em Saúde, Rio de Janeiro, v. 14, n. 3, p. 692-708, jul./set. 2020.

BAPTISTA, T. W. F. História das políticas de saúde no Brasil: a trajetória do direito à saúde. *In*: BAPTISTA, T. W. F. **Políticas de saúde: organização e operacionalização do Sistema Único de Saúde**. [S. l: s. n.], 2007. p. 29-60.

BENTO, L. V. Critérios de ponderação entre o direito de acesso a informações públicas e o direito à proteção de dados pessoais: lições a partir do modelo espanhol. **Revista da CGU**, Brasília, v. 12, n. 22, 2020. Disponível em: https://ojs.cgu.gov.br/index.php/Revista_da_CGU/article/view/173. Acesso em: 5 ago. 2024.

BITTAR, C. A. **Os direitos da personalidade**. 8. ed. São Paulo: SARAIVA, 2015.

BONAVIDES, P. **Curso de direito constitucional**. 15. ed. São Paulo: Malheiros, 2004.

BRASIL. Autoridade Nacional de Proteção de Dados. **ANDP publica Agenda Regulatória 2023-2024**. Brasília: ANDP, 2023.Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024. Acesso em: 29 jan. 2024.

BRASIL. **Decreto 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília: Senado Federal, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 10 ago. 2024.

BRASIL. **Decreto n. 7.508, de 28 de junho de 2011**. Regulamenta a Lei nº 8.080, de 19 de setembro de 1990, para dispor sobre a organização do Sistema Único de Saúde - SUS, o planejamento da saúde, a assistência à saúde e a articulação interfederativa, e dá outras providências. Brasília: Senado Federal, 2011. Disponível

em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7508.htm. Acesso em: 28 nov. 2023.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direito e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Senado Federal, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 22 dez. 2023.

BRASIL**. e-SUS APS**. Brasília: e-SUS, [2024]. Disponível em: https://sisaps.saude.gov.br/esus/. Acesso em: 11 nov. 2023.

BRASIL. **Lei 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília: Senado Federal, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em 20 dez. 2023.

BRASIL. **Lei 8.142, de 28 de dezembro de 1990**. Dispõe sobre a participação da comunidade na gestão do Sistema Único de Saúde (SUS) e sobre as transferências intergovernamentais de recursos financeiros na área da saúde e dá outras providências. Brasília: Senado Federal, 1990.

BRASIL. **Lei complementar nº 141, de 13 de janeiro de 2012**. Regulamenta o § 3o do art. 198 da Constituição Federal para dispor sobre os valores mínimos a serem aplicados anualmente pela União, Estados, Distrito Federal e Municípios em ações e serviços públicos de saúde; estabelece os critérios de rateio dos recursos de transferências para a saúde e as normas de fiscalização, avaliação e controle das despesas com saúde nas 3 (três) esferas de governo; revoga dispositivos das Leis nos 8.080, de 19 de setembro de 1990, e 8.689, de 27 de julho de 1993; e dá outras providências. Brasília: Senado Federal, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp141.htm. Acesso em: 23 nov. 2023.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília: Senado Federal, 2002.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Brasília: Senado Federal, 2018.

BRASIL. **Lei n° 14.510/2022, de 27 de dezembro de 2022**. Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. Brasília: Senado Federal, 2022.

BRASIL. **Ministério da Saúde lança assistente virtual no WhatsApp com informações oficiais sobre a vacinação**. Brasília: Ministério da Saúde, 2023. Disponível em: https://www.gov.br/saude/pt-

br/assuntos/noticias/2023/dezembro/ministerio-da-saude-lanca-assistente-virtual-no-whatsapp-com-informacoes-oficiais-sobre-a-vacinacao. Acesso em: 4 dez. 2023.

BRASIL. Ministério da Saúde. Conselho Nacional de Secretários de Saúde. Sistema Único de Saúde. **Coleção progestores**: para entender a Gestão do SUS. Brasília: CONASS, 2007. v. 1.

BRASIL. Ministério da Saúde. **Plano nacional de saúde**. Brasília: Ministério da Saúde, 2016. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/plano_nacional_saude_2016_2019_30032015_final.pdf. Acesso em: 4 dez. 2023.

BRASIL. Ministério da Saúde. **Portaria n. 1.820, de 13 de agosto de 2009**. Dispõe sobre os direitos e deveres dos usuários da saúde. Brasília: Senado Federal, 2009. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2009/prt1820_13_08_2009.html. Acesso em: 5 dez. 2023.

BRASIL. Ministério da Saúde. **Saúde digital e telessaúde**. [S. l.]: Ministério da Saúde, [2023]. Disponível em: https://www.gov.br/saude/pt-br/composicao/seidigi/saude-digital/telessaude/telessaude. Acesso em: 25 nov. 2023.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Informática do SUS. Estratégia de Saúde Digital para o Brasil 2020-2028 [recurso eletrônico] / Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. – Brasília : Ministério da Saúde, 2020. 128 p. : il.

BRASIL. Ministério da Saúde. **SEIDIGI**. Brasília: Ministério da Saúde, [2023]. Disponível em: https://www.gov.br/saude/pt-br/composicao/seidigi. Acesso em: 23 nov. 2023.

BRASIL. **Nota técnica SSIC/GSI N.º 01/2023**. Proposta de Projeto de Lei de Criação da Política Nacional de Cibersegurança. Brasília: GSI, 2023. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf. Acesso em: 11 ago. 2024

BRASIL. Sendo Federal. **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988.

BRASIL. Serviços e informações do Brasil. **Conect SUS Cidadão**. Brasília: GOV, 2023. Disponível em:https://www.gov.br/pt-br/servicos/acessar-a-plataforma-movel-de-servicos-digitais-do-ministerio-da-saude. Acesso em: 23 nov. 2023.

BRASIL. Sistema Único de Saúde. [página inicial]. Disponível em: https://www.gov.br/saude/pt-br/assuntos/saude-de-a-a-z/s/sus. Acesso em: 27 nov. 2023.

BRASIL. Supremo Tribunal Federal. **STF define critérios para a concessão judicial de medicamentos não incorporados ao SUS**. Brasília: STF, 2024. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-define-criterios-para-a-

concessao-judicial-de-medicamentos-nao-incorporado-ao-sus/. Acesso em: 29 out. 2024.

BRUNO, F.; PEREIRA, P. C.; FALTAY, P. **Inteligência artificial e saúde**: ressituar o problema. [S. l.: s. n.], 2023.

BVS - BIBLIOTECA VIRTUAL DE SAÚDE. **Lei n. 8080**: 30 anos de criação do Sistema único de Saúde (SUS). Brasília: BVS, [2023]. Disponível em: https://bvsms.saude.gov.br/lei-n-8080-30-anos-de-criacao-do-sistema-unico-de-saude-sus/#:~:text=Em%2019%2F9%2F1990%20foi,Único%20de%20Saúde%20(SUS).. Acesso em: 27 nov. 2023.

CAMBRICOLI, F. **Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros**. São Paulo: Estadão, 2020. Disponível em: https://www.estadao.com.br/saude/nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes/. Acesso em: 24 jan. 2024.

CANCELIER, M. V. L. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, n. 76, p. 213-239, 2017. DOI: https://doi.org/10.5007/2177-7055.2017v38n76p213

CARDOSO, D. B. **Colisão de direitos fundamentais**: ponderação e proporcionalidade na visão de Robert Alexy. [S. l.: s. n.], 2016.

CARVALHAL, G. F. *et al*. Recomendações para a proteção da privacidade do paciente. **Revista bioética**, Brasília, v. 25, n. 1, 2017. Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/1133. Acesso em: 26 jan. 2025.

CELUPPI, I. C. *et al*. Dez anos do prontuário eletrônico do cidadão e-SUS APS: em busca de um Sistema Único de Saúde eletrônico. **Revista de Saúde Pública**, São Paulo, v. 58, 2024. Disponível em: https://rsp.fsp.usp.br/wp-content/plugins/xml-to-html/include/lens/index.php/?xml=1518-8787-rsp-58-23.xml. Acesso em: 9 ago. 2024.

CFM – CONSELHO FEDERAL DE MEDICINA. **Código de ética médica**. Brasília: CFM, 2019. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf Acesso em: 5 dez. 2023.

CFM - Conselho Federal de Medicina. **Resolução CFM nº 2.314/2022, que define e regulamenta a telemedicina no Brasil**. Brasília: CFM, 2022. Disponível em: cfm.org.br. Acesso em: 20 de nov. 2023.

CIANCIO, L.; ROSSI, A. Telemedicina e trattamento dati sanitari: ecco perché serve maggiore tutela della privacy. **Networkdigital360**, Roma, 23 nov. 2022.. Disponível em: https://www.cybersecurity360.it/legal/privacy-dati-personali/telemedicina-e-trattamento-dati-sanitari-ecco-perche-servemaggiore-tutela-della-privacy/. Acesso em: 3 ago. 2024.

COELHO NETO, G. C.; ANDREAZZA, R.; CHIORO, A. Integração entre os sistemas nacionais de informação em saúde: o caso do e-SUS Atenção Básica. **Revista de Saúde Pública**, São Paulo, v. 55, p. 93, 2021.

CONCEIÇÃO, J. V. S. **As informações individuais privadas na internet**: a lgpd aplicada na obtenção e no devido uso dos dados de natureza pessoal. **Revista Brasileira de Estudos de gestão e Desenvolvimento Regional**, Cáceres, v. 2, n. 1, p. 125-141, 2024. DOI: https://doi.org/10.30681/rbegdr.v2i1.12573

COSSETI, M. C. O que é inteligência artificial?. Disponível em: https://tecnoblog.net/responde/o-que-e-inteligencia-artificial/. Acesso em 20 Out 2023.

CRUZ, E. P. **Ministério da Saúde planeja inclusão de inteligência artificial no SUS**. Brasília: Agência Brasil, 2023 Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2023-05/ministerio-da-saude-planeja-inclusao-de-inteligencia-artificial-no-sus. Acesso em: 03 dez. 2023.

DALLARI, S. G. A construção do direito à saúde no Brasil. **Revista de Direito Sanitário**, São Paulo, v. 9, n. 3, p. 9-34, 2008. DOI: 10.11606/issn.2316-9044.v9i3p9-34

DIAS, M. C. **Robô Laura**: a startup curitibana que já salvou 24 mil vidas no Brasil. 18/02/2021. Disponível em: https://gazzconecta.com.br/gazz-conecta/robo-laura-tecnologia-e-saude/. Acesso em: 8 ago. 2024.

DONEDA, D. C. M.; MENDES, L. S.; SOUZA, C. A. P.; AN, M. M. N. B. G. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar-Revista de Ciências Jurídicas**, Fortaleza, v. 23, n. 4, p. 1-17, 2018.

DONEDA, D. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, D. **Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro**: da emergência de uma revisão conceitual e da tutela de dados pessoais. [S. l.]: Âmbito Jurídico, 2008. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/privacidade-vida-privada-e-intimidade-no-ordenamento-juridico-brasileiro-da-emergencia-de-uma-revisao-conceitual-e-da-tutela-de-dados-pessoais/. Acesso em: 14 dez. 2023.

EGUES, J. **SUS Digital**: uso inteligência artificial pode melhorar a saúde pública? [S. l.]: Tecmundo, 2023. Disponível em: https://www.tecmundo.com.br/ciencia/267730-sus-digital-uso-inteligencia-artificial-melhorar-saude-publica.htm. Acesso em: 4 dez. 2023.

FANTONELLI, M.; CELUPPI, I. C.; OLIVEIRA, F. M.; BURIGO, F.; DALMARCO, E. M.; WAZLAWICK, R. S. Lei geral de proteção de dados e a interoperabilidade na saúde pública. **Journal of Health Informatics**, Brasilia, v. 12, 2021. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/809. Acesso em: 13 dez. 2023.

FERNANDES, B. G. **Curso de direito constitucional**. 11. ed. Salvador: Ed. Juspodivm, 2019.

FERREIRA, R. S. S. **Direito à saúde no Brasil**: a judicialização das demandas em saúde. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Rondônia, Rondônia, 2023. Disponível em: https://ri.unir.br/jspui/bitstream/123456789/4883/1/MONOGRAFIA%20RAINE%20SAMILA.pdf. Acesso em: 15 jan. 2024.

FORATO, F. **Anvisa expõe dados de 1.900 pessoas que usam óleo de cannabis**. [S. l.]: Canal Tech, 2020. Disponível em https://canaltech.com.br/juridico/anvisa-expoe-dados-de-1900-pessoas-que-usam-oleo-de-cannabis-160068/. Acesso em: 24 jan. 2024

FRANCO, W. O. **A proteção de dados pessoais no Brasil**: Aspectos e reflexos da emenda constitucional 115/2022 no ordenamento jurídico brasileiro. 2022. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Ciências Jurídicas e Sociais, Brasília, 2022. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/16205. Acesso em: 12 ago. 2024.

FUTURO DA SAÚDE. **Conecte SUS: como o Governo Federal está investindo em dados no sistema de saúde**. [S. l.]: Futuro da Saúde, 2021. Disponível em: https://futurodasaude.com.br/conecte-sus/. Acesso em: 29 nov. 2023.

G1. **Ataque hacker tira do ar site do Ministério da Saúde e o ConecteSUS**. São Paulo: G1, 2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/12/10/ataque-hacker-ao-site-do-ministerio-da-saude-tira-do-ar-o-conectesus.ghtml. Acesso em 22 jan. 2024.

GARCIA, M. L.; MACIEL, N. F. A inteligência artificial no acesso à saúde: Reflexões sobre a utilização da telemedicina em tempos de pandemia. **Revista Eletrônica Direito e Política**, Itajaí, v. 15, n. 2, p. 623–643, 2020. DOI 10.14210/rdp.v15n2.p623-643

GET PRIVACY. **O que é a ANPD e quais são as suas funções**. [S. l.]: Get Privacy, [2023]. Disponível em: https://getprivacy.com.br/anpd-o-que-e/. Acesso em: 20 dez. 2023.

GIL, M. A. 5 aplicações da IA generativa na criação de novos medicamentos. [S. l.]: Negócios, 2024. Disponível em: https://epocanegocios.globo.com/inteligencia-artificial/noticia/2024/04/5-aplicacoes-da-ia-generativa-na-criacao-de-novos-medicamentos.ghtml. Acesso em: 9 ago. 2024.

GOMES, H. S.; TEIXEIRA, L. B. **Plano de IA de Lula mira supercomputador, mas sem superar EUA e China**. [S. l.]: UOL, 2024.Disponível em: https://www.uol.com.br/tilt/colunas/helton-simoes-gomes/2024/07/30/plano-de-ia-de-lula-mira-supercomputador-mas-nao-fara-brasil-superar-eua.htm?cmpid=copiaecola. Acesso em 30 jul. 2024.

GUARAPUAVA. **‘Sara’, assistente virtual para triagem e monitoramento de casos de covid-19 em Guarapuava, já está disponível para usuários do aplicativo fala saúde**. Guarapuava: Prefeitura de Guarapuava, 2022. Disponível em: https://guarapuava.pr.gov.br/noticias/sara-assistente-virtual-para-triagem-e-

monitoramento-de-casos-de-covid-19-em-guarapuava-ja-esta-disponivel-para-usuarios-do-aplicativo-fala-saude/. Acesso em: 3 dez. 2023.

GUARAPUAVA. **Lançamento do SARA 2.0 conta com participação do Poder Legislativo**. Guarapuava: Prefeitura de Guarapuava, 2023. Disponível em: https://www.guarapuava.pr.leg.br/imprensa/noticias/lancamento-do-sara-2-0-conta-com-participacao-do-poder-legislativo. Acesso em: 3 dez. 2023.

GUARIZI, D. D; OLIVEIRA, E. V. Estudo da inteligência artificial aplicada na área da saúde. *In*: COLLOQUIUM EXACTARUM, 6., 2014, Presidente Prudente. **Anais** [...]. Presidente Prudente, 2014. p. 26-37.

INFORCHANNEL. **Assistente virtual voltada para atendimento à saúde pública agora terá coordenação do cuidado**. [S. l.]: InforChannel, 2022. Disponível em: https://inforchannel.com.br/2022/05/23/assistente-virtual-voltada-para-atendimento-a-saude-publica-agora-tera-coordenacao-do-cuidado/. Acesso em: 3 dez. 2023.

JNOTICIAS. **Inovação na saúde pública**: Prefeito Celso Góes lança SARA 2.0. [S. l.]: Jnotícias, 2023. Disponível em: https://jnoticias.com.br/inovacao-na-saude-publica-prefeito-celso-goes-lanca-sara-2. Acesso em: 3 dez. 2023.

JOELSONS, M. O íter histórico dos direitos da personalidade, o direito à privacidade e seus desafios na sociedade da informação. Revista de Direito Privado, [s. l.], v. 107, p. 33-60, 2021. Disponível em:https://www.researchgate.net/profile/Marcela-Joelsons-2/publication/352132080_O_ITER_HISTORICO_DOS_DIREITOS_DA_PERSONALIDADE_O_DIREITO_A_PRIVACIDADE_E_SEUS_DESAFIOS_NA_SOCIEDADE_DA_INFORMACAO/links/60ba479192851cb13d7967ea/O-ITER-HISTORICO-DOS-DIREITOS-DA-PERSONALIDADE-O-DIREITO-A-PRIVACIDADE-E-SEUS-DESAFIOS-NA-SOCIEDADE-DA-INFORMACAO.pdf. Acesso em: 22 dez. 2023.

JORNAL EXTRA GUARAPUAVA. **SARA**: Assistente virtual auxilia no combate à dengue em Guarapuava. Guarapuava: Jornal Extra Guarapuava, 2024. Disponível em: https://www.extraguarapuava.com.br/saude/sara-assistente-virtual-auxilia-no-combate-a-dengue-em-guarapuava/. Acessado em: 7 ago. 2024.

LIMA, B. **Telemedicina: modelo cresce com integração no SUS, inteligência artificial e expansão na rede privada**. Brasília: Globo, 24. Disponível em: https://oglobo.globo.com/saude/noticia/2024/04/29/telemedicina-modelo-cresce-com-integracao-no-sus-inteligencia-artificial-e-expansao-na-rede-privada.ghtml. Acesso em: 7 ago. 2024.

LIMA, I. S.; GONÇALVES, J. R.; COSTA, D. A Lei Geral de Proteção de Dados Pessoais nos Serviços de Saúde Pública. **Revista Processus de Políticas Públicas e Desenvolvimento Socia**l, [s. l.], v. 5, n. 10, p. 58–78, 2023. DOI: 10.5281/zenodo.8367336

LIMA, N. T.; FONSECA, C.; HOCHMAN, G. A saúde na construção do Estado Nacional no Brasil: Reforma Sanitária em perspectiva. *In*: LIMA, N. T. (org.). **Saúde e democracia**: história e perspectivas do SUS. Rio de Janeiro: Editora Fiocruz, 2005.

LOBATO, M. M. **Slang e o Brasil e problema vital**. São Paulo: Brasiliense, 1957.

LOPES, J. E.; HEIMANN, C. Uso das tecnologias da informação e comunicação nas ações médicas a distância: um caminho promissor a ser investido na saúde pública. **Journal of Health Informatics**, Brasília, v. 8, n. 1, 2016. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/364. Acesso em: 24 nov. 2023.

LUCAS, L. B.; SANTOS, D. O. Considerações sobre os desafios jurídicos do uso da inteligência artificial na medicina. **Revista de Direito**, [s. l.], v. 13, n. 01, p. 01–25, 2021. DOI: 10.32361/2021130112292

LUCCA, M. **Ativismo Judicial**: o papel do STF perante o Covid-19. [S. l.]: Migalhas, 2021. Disponível em: https://www.migalhas.com.br/depeso/342273/ativismo-judicial-o-papel-do-stf- perante-o-covid-19. Acesso em: 10 jan 2024.

MAGNANO, O. A. **Mecanismos de proteção da privacidade das informações de prontuário eletrônico de pacientes de instituições de saúde**. 2015. Dissertação (Mestrado em Administração e Negócios) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015.

MALDONADO, V. N.; BLUM, R. O. **LGPD**: lei geral de proteção de dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MARTINS, A. R. L. **Direito ao meio ambiente equilibrado x direito a manifestação cultural**: solução do conflito aparente de normas fundamentais sob a ótica de Robert Alexy. [S. l.: s. n.], 2017. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/4991/TCC%20Arique%20Rieno%20-VERSAO%20FINAL%20-%20COM%20FICHA%20CATALOGR%c3%81FICA.pdf?sequence=1&isAllowed=y. Acesso em: 6 ago. 2024.

MEDICAL WAY. **Robô Laura**: conheça mais essa inovação na área da saúde. [S. l.]: Medical Way, c2022. Disponível em: https://medicalway.com.br/blog/marco-19-robo-laura-conheca-mais-essa-inovacao-na-area-da-saude/. Acesso em: 7 ago. 2024.

MELO, M.B.; VAITSMAN, J. Auditoria e avaliação no Sistema Único de Saúde. **São Paulo em Perspectiva**, São Paulo, v. 22, n. 1, p. 152-164, jan./jun. 2008. Disponível em: http://produtos.seade.gov.br/produtos/spp/v22n01/v22n01_11.pdf. Acesso em: 15 jun. 2024.

MORAES, K. E. F.; OLIVEIRA, N. L.; CRUZ, C. G. G. Teleconsulta e a garantia do direito à saúde. **Revista Foco**, Curitiba, v. 16, n. 11, p. e3524, 2023. DOI: 10.54751/revistafoco.v16n11-021

MV INFORMÁTICA. **Até 2028, o Brasil deve investir para consolidar a digitalização da tecnologia na saúde com sete prioridades de trabalho**. Recife: MV informática, 2023. Disponível em: https://mv.com.br/blog/tecnologia-melhora-saude-publica-no-brasil. Acesso em: 28 nov. 2023.

NASCIMENTO, V. **Sara atende pacientes com casos leves e moderados em Guarapuava**. Curitiba: Rede Sul de Notícias, 2024. Disponível em: https://redesuldenoticias.com.br/noticias/sara-atende-pacientes-com-casos-leves-e-moderados-em-guarapuava/. Acesso em: 7 ago. 2024.

NÓBREGA, A. P. N.; GIRARDI JÚNIOR, L. SIMI-SP: plataformização como estratégia de enfrentamento da pandemia de covid-19. **Revista Eletrônica De Comunicação, Informação & Inovação Em Saúde**, São Paulo, v. 17, n. 1, p. 33–46, 2023. DOI: https://doi.org/10.29397/reciis.v17i1.3452

OMS – ORGANIZAÇÃO MUNDIAL DA SAÚDE. **Informações do projeto e-SUS Atenção Básica**. [S. l.]: OMS, 2019. Disponível em: https://digitalhealthatlas.org/pt/-/projects/922/published. Acesso em 23 nov. 2023.

PAULINO, M. **Conecte SUS**: app traz histórico do cidadão no sistema de saúde e possibilita acesso a serviços e informações. [S. l.]: Observatório Social do Brasil, 2024. Disponível em: https://osblimeira.org.br/conecte-sus-app-traz-historico-do-cidadao-no-sistema-de-saude-e-possibilita-acesso-a-servicos-e-informacoes/. Acesso em 23 nov. 2023.

PEDRON, Flávio Quinaud; RODRIGUES, Fábio Lopes. A Teoria da Norma e o Supremo Tribunal Federal: Estudo de casos. **Revista da Faculdade de Direito do Sul de Minas**, Porto Alegre, v. 38, n. 1, pp. 51-67, jan./jun. 2022.

PEDUZZI, P. **Saúde lança assistente virtual com informações sobre vacinas**. Brasília: Agência Brasil, 2023. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2023-12/saude-lanca-assistente-virtual-com-informacoes-sobre-vacinas. Acesso em: 4 dez. 2023.

PORTAL HOSPITAIS BRASIL. **Robô-enfermeira é testada no Canadá e na Coreia do Sul**. [S. l.]: Portal Hospital Brasil, 2022. Disponível em: https://notaalta.espm.br/o-melhor-de-hoje/robo-enfermeira-e-testada-no-canada-e-na-coreia-do-sul/. Acesso em: 9 ago. 2024.

PRÊMIO GESTOR PÚBLICA PARANÁ. **Guarapuava otimiza atendimento médico com inteligência artificial**. Curitiba: PGP, 2023. Disponível em:https://pgp-pr.org.br/guarapuava-otimiza-atendimento-medico-com-inteligencia-artificial/. Acesso em: 7 ago.2024.

QUEDEVEZ, G. F. Direito à saúde e o uso de assistentes digitais. [S. l.]: Barreto Veiga Advogados, 2022. Disponível em: https://bvalaw.com.br/direito-saude/. Acesso em: 28 nov. 2023.

REDE SUL DE NOTÍCIAS. **Sara 2.0 começa a atender com mais tecnologia em Guarapuava**. [S. l.]: Rede Sul de Notícias, 2023. Disponível em: https://redesuldenoticias.com.br/noticias/sara-2-0-comeca-a-atender-com-mais-tecnologia-em-guarapuava/. Acesso em: 3 dez. 2023.

RODRIGUES, F. L. L. O uso da Inteligência Artificial no âmbito da saúde: os limites de sua utilização frente às questões da privacidade e a busca pela ampla garantia da inclusão dos benefícios. *In*: MAIA, A. P. *et al***. Neurodireito, Neurotecnologia e Direitos Humanos**. Porto Alegre: Revista Advogados, 2023, p. 131-142. Disponível em: https://www.researchgate.net/profile/Ana-Maria-Lopes/publication/368128401_Neurodireito_Neurotecnologia_e_Direitos_Humanos/links/63dc16fd64fc8606380b727a/Neurodireito-Neurotecnologia-e-Direitos-Humanos.pdf#page=133. Acesso em: 3 dez. 2023.

RPN. **Programa nacional telessaúde brasil redes**: uma década de inovação. [S. l.]: RPN, 2017. Disponível em: https://www.rnp.br/arquivos/documents/Livro%20-%20Telessa%C3%BAde.pdf. Acesso em: 28 nov. 2023.

RPN. **Programa telesaúde Brasil redes**. [S. l.]: RPN, [2023]. Disponível em: https://www.rnp.br/inovacao/solucoes/telessaude-brasil-redes. Acesso em: 24 nov. 2023.

SANTO DIGITAL. **Inteligência artificial na indústria farmacêutica**: entenda aplicações e tendências. [S. l.]: Santo Digital, 2024. Disponível em: https://santodigital.com.br/industria-farmaceutica/. Acesso em: 09 ago. 2024.

SÃO PAULO **Decreto n. 64.963, de 05 de maio de 2020**. Institui o Sistema de Informações e Monitoramento Inteligente - SIMI, destinado ao enfrentamento da pandemia da COVID-19, e dá providências correlatas. São Paulo: Palácio dos Bandeirantes, 2020. Disponível em: https://www.saopaulo.sp.gov.br/wp-content/uploads/2020/05/Decreto-64963-de-05-de-maio-de-2020-SIMI.pdf. Acesso em: 04 dez. 2023.

SERPRO. **Brasil lança sua primeira Política Nacional de Cibersegurança**. [S. l.]: SERPRO, 2023. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2023/brasil-lanca-pnciber. Acesso em: 10 ago. 2024.

SILVA, A. B.; CUNHA, F. J. A. P. **Lei Geral de Proteção de Dados e o controle social da saúde**. Porto Alegre: Editora Rede Unida, 2023.

SILVA, J. A. **Curso de direito constitucional positivo**. 30. ed. São Paulo: Malheiros, 2008.

SOUSA, M. E. A. Direitos humanos e princípios comuns entre inteligência artificial e direito à saúde. **Cadernos Ibero-Americanos de Direito Sanitário**, [s. l.], v. 9, n. 3, p. 26-48, 2020.

SOUSA, T. R.; COUTINHO, M.; COUTINHO, L.; ALBUQUERQUE, R.. LGPD: levantamento de técnicas criptográficas e de anonimização para proteção de bases de dados. *In*: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 20., 2020, Petrópolis. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 55-68. DOI: https://doi.org/10.5753/sbseg.2020.19227.

SOUZA, N. B.; ACHA, F. R. A proteção de dados como direito fundamental: uma análise a partir da emenda constitucional 115/2022. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [s. l.], v. 8, n. 9, p. 666–684, 2022. DOI 10.51891/rease.v8i9.6822

TENAGLIA, M. R. **Simulação de ataques cibernéticos nos dispositivos iot em ambientes de saúde**. 2024. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Pontificia Universidade de Goiás, Goiânia, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7816. Acesso em: 31 jul. 2024.

TINSIDE. H**ospital Albert Einstein confirma vazamento de dados de 16 milhões de pessoas**. [S. l.]: Tinside, 2020. Disponível em: https://tiinside.com.br/26/11/2020/hospital-albert-einstein-confirma-vazamento-de-dados-de-16-milhoes-de-pessoas/. Acesso em: 24 jan. 2024.

VENTURA, M.; COELI, C. M. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança **Cadernos de Saúde Pública**, São Paulo, v. 34, n. 7, p. e00106818, 2018. DOI 10.1590/0102-311x00106818.

VIACAVA, F. *et al*. SUS: oferta, acesso e utilização de serviços de saúde nos últimos 30 anos. **Ciência & saúde coletiva**, [s. l.], v. 23, p. 1751-1762, 2018.

VIEIRA, F. S. Judicialização e direito à saúde no Brasil: uma trajetória de encontros e desencontros. **Revista de Saúde Pública**, [s. l.], v. 57, p. 1, 2023.

WEISE, A. **IA na fabricação de medicamentos**: como a tecnologia pode acelerar a indústria farmacêutica. [S. l.]: Futuro da Saúde, 2024. Disponível em: https://futurodasaude.com.br/ia-desenvolvimento-de-medicamentos/. Acesso em: 9 ago. 2024.

XAVIER, F. C. **O uso dos processos de anonimização e pseudonimização no contexto da LGPD**. [S. l.]: Migalhas, 2021. Disponível em: https://www.migalhas.com.br/depeso/342896/o-uso-dos-processos-de-anonimizacao-e-pseudonimizacao-da-lgpd. Acesso em: 29 jan. 2024.

ZAGANELLI, M. V.; BINDA FILHO, D. L. O sigilo médico e os dados sensíveis na telemedicina à luz da Lei Geral de Proteção de Dados. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, [s. l.], v. 17, n. 3, 2023. DOI: 10.29397/reciis.v17i3.3689

ZUBOFF, S. **A era do capitalismo de vigilância**. São Paulo: Editora Intrínseca, 2021