XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO E SAÚDE II

EDITH MARIA BARBOSA RAMOS

JANAÍNA MACHADO STURZA

LITON LANES PILAU SOBRINHO

D597

Direito e saúde II[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Edith Maria Barbosa Ramos, Janaína Machado Sturza, Liton Lanes Pilau Sobrinho – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-331-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Saúde. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO E SAÚDE II

Apresentação

A realização do XXXII Congresso Nacional do CONPEDI aconteceu entre os dias 26, 27 e 28 de novembro de 2025, na cidade de São Paulo, tendo como instituição anfitriã a Universidade Presbiteriana Mackenzie.

O tema desta edição foi “Os caminhos da internacionalização e o futuro do Direito”, o qual, segundo o CONPEDI, reflete os desafios e as oportunidades de um mundo em profunda transformação. A temática é um convite à reflexão em um momento histórico marcado pela intensificação das interconexões globais — econômicas, políticas, culturais e tecnológicas, que desafiam as fronteiras tradicionais dos Estados e colocam o Direito diante de novas exigências e dilemas.

Em 27 do corrente mês, realizou-se o Grupo de Trabalho (GT) Direito e Saúde, ocasião em que foram apresentados estudos que exploraram diversas perspectivas e possibilidades de interação com a saúde enquanto direito social, fundamental e humano. Os trabalhos apresentados abarcaram temas como análises conceituais e relatos de experiências nos contextos brasileiro e internacional, com ênfase na efetivação da saúde e suas demandas, tendo como fundamento a Constituição Federal.

Dentre os temas abordados, destacam-se: a judicialização da saúde, notadamente no que concerne a medicamentos, internações hospitalares e tratamentos de alto custo; a saúde digital e suas interfaces com as tecnologias; questões de gênero relacionadas ao direito à saúde; medicamentos e experimentos em saúde; autonomia da vontade e perspectivas da saúde sob a ótica da bioética, entre outros.

Os trabalhos apresentados se revelaram enriquecedores, propiciando reflexões abrangentes e constituindo contribuições significativas para a pesquisa jurídica e social nas esferas acadêmicas brasileira e internacional, com destaque para o direito à saúde.

Janaína Machado Sturza – UNIJUI

Liton Lanes Pilau Sobrinho – Universidade do Vale do Itajaí

Edith Maria Barbosa Ramos - Universidade Federal do Maranhão

LEI GERAL DE PROTEÇÃO DE DADOS E A AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6387: TRATAMENTO DE DADOS PESSOAIS E SAÚDE PÚBLICA

GENERAL DATA PROTECTION LAW AND DIRECT ACTION OF UNCONSTITUTIONALITY 6387: PROCESSING OF PERSONAL DATA AND PUBLIC HEALTH

Catharina Orbage De Britto Taquary Berino
Eneida Orbage De Britto Taquary
Débora Soares Mendes

Resumo

Esta pesquisa visa a análise dos meios normativos e jurisprudenciais que dispõem sobre o tratamento de dados relacionados à saúde, em destaque a Lei Geral de Proteção de Dados – LGPD e a Ação Direta de Inconstitucionalidade 6387. Dessa maneira, busca-se explorar até onde a LGPD alcança a necessidade, a adequação e a proporcionalidade do manejo e do tratamento dos dados pessoais ante o tratamento de dados pessoais avaliados em caso de risco de saúde pública, à priori, e como a LGPD sustenta os direitos constitucionais de privacidade e liberdade em conferência com a coletividade. O problema da pesquisa é: qual a garantia de manipulação adequada de dados pessoais para a avaliação e o manejo de um risco para a saúde pública e, por extensão, à relação de preservação da privacidade e a saúde coletiva? As hipóteses são i) ocorreram implicações bioéticas da proteção de dados sensíveis no contexto pandêmico; ii) escolha entre privacidade e Direito à Saúde é uma falsa dicotomia, e que é possível e imperativo ter ambos. Os objetivos são: i) discutir a legislação, jurisprudência e doutrina brasileira sobre o tratamento de dados de saúde; ii) versar sobre os impactos para terceiros que captam e armazenam biodados; e: iii) correlacionar o Direito Fundamental à Proteção de Dados, à saúde e à privacidade em face do desenvolvimento científico. O método utilizado é a pesquisa bibliográfica com abordagem qualitativa e método jurídico – comparativo. Espera-se como resultado desconstituir a proteção da privacidade e da saúde como direitos antagônicos.

Palavras-chave: Lei geral de proteção de dados (lgpd), Ação direta de inconstitucionalidade 6387, Saúde pública, Direito à saúde, Bioética

Abstract/Resumen/Résumé

This research aims to analyze the regulatory and jurisprudential frameworks governing the processing of health-related data, particularly the General Data Protection Law (LGPD) and Direct Action of Unconstitutionality 6387. Thus, it seeks to explore the extent to which the LGPD addresses the necessity, adequacy, and proportionality of the handling and processing of personal data when considering the processing of personal data assessed a priori in the event of a public health risk, and how the LGPD supports the constitutional rights of privacy

and freedom in conjunction with the community. The research question is: what is the guarantee of appropriate handling of personal data for the assessment and management of a risk to public health and, by extension, the relationship between privacy preservation and public health? The hypotheses are: i) there were bioethical implications of the protection of sensitive data in the pandemic context; ii) the choice between privacy and the Right to Health is a false dichotomy, and that it is possible and imperative to have both. The objectives are: i) to discuss Brazilian legislation, case law, and doctrine on the processing of health data; ii) to address the impacts on third parties who collect and store biodata; and iii) to correlate the Fundamental Right to Data Protection, health, and privacy in light of scientific developments. The method used is bibliographic research with a qualitative approach and a comparative legal method. The expected outcome is to deconstruct the protection of privacy and health as conflicting rights.

Keywords/Palabras-claves/Mots-clés: General data protection law (lgpd), Direct action of unconstitutionality 6387, Public health, Right to health, Bioethics

1 INTRODUÇÃO

A presente pesquisa tem como objetivo analisar os instrumentos normativos e jurisprudenciais que regulam o tratamento de dados pessoais relacionados à saúde, com enfoque na Lei Geral de Proteção de Dados Pessoais (LGPD) e na Ação Direta de Inconstitucionalidade (ADI) 6387.

Em um cenário marcado pela crescente digitalização dos serviços de saúde e pela intensificação da coleta de informações sensíveis, torna-se imprescindível compreender em que medida a LGPD atende aos critérios de necessidade, adequação e proporcionalidade no manejo de dados pessoais em contextos de risco à saúde pública.

A investigação parte da premissa de que o tratamento de dados pessoais em situações emergenciais deve ser compatível com os direitos fundamentais à privacidade, à liberdade e à dignidade da pessoa humana, sem desconsiderar os interesses da coletividade e a efetividade das políticas públicas de saúde.

A ADI 6387, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil, questiona dispositivos da Medida Provisória nº 954/2020, que determinava o compartilhamento de dados de usuários de serviços de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) durante a pandemia de COVID-19.

O julgamento desta ação pelo Supremo Tribunal Federal (STF) revelou tensões constitucionais entre o direito à proteção de dados e a necessidade de atuação estatal em situações excepcionais. Nesse contexto, a LGPD emerge como um marco regulatório fundamental para a consolidação do direito à proteção de dados como direito autônomo, com implicações diretas sobre o setor da saúde, especialmente no que tange à coleta, armazenamento, compartilhamento e uso de informações biomédicas e genéticas.

O problema central da pesquisa consiste em indagar: qual a garantia de manipulação adequada dos dados pessoais para fins de avaliação e gestão de riscos à saúde pública, e como essa manipulação se articula com a preservação da privacidade individual e da saúde coletiva?

Para tanto, os objetivos específicos são: (i) discutir a legislação, jurisprudência e doutrina brasileiras sobre o tratamento de dados de saúde; (ii) examinar os impactos da coleta e armazenamento de biodados por terceiros, incluindo instituições públicas e privadas; e (iii) correlacionar os direitos fundamentais à proteção de dados, à saúde e à privacidade diante dos avanços científicos e tecnológicos, especialmente em contextos de emergência sanitária.

O método adotado é a pesquisa bibliográfica, com análise crítica dos dispositivos legais e decisões judiciais pertinentes, especialmente a LGPD e a ADI 6387, articulados com debates bioéticos e reflexões sobre a proteção de dados sensíveis. A abordagem interdisciplinar permite compreender os limites e possibilidades da atuação estatal e privada no tratamento de dados de saúde, considerando os princípios constitucionais e os parâmetros internacionais de direitos humanos (Piccoli *et al.*, 2021, pp. 66 – 68).

Os resultados obtidos indicam que, embora haja conformidade normativa quanto à necessidade, adequação e proporcionalidade no tratamento de dados pessoais em casos concretos, persiste a demanda por estruturas regulatórias mais específicas no âmbito público, bem como por maior atenção às peculiaridades da saúde suplementar privada Além disso, evidencia-se a importância de fortalecer mecanismos de controle e fiscalização, garantindo a efetividade dos direitos fundamentais em um ambiente cada vez mais digitalizado e vulnerável a abusos informacionais (Piccoli *et al.*, 2021, pp. 66 – 68).

2 DIREITO FUNDAMENTAL EM EVOLUÇÃO

A sociedade contemporânea, profundamente moldada pela revolução tecnológica, testemunha um volume sem precedentes de dados pessoais sendo gerados, coletados e processados. A informação advinda dos dados pessoais é uma fonte de poder, colocando a proteção dos dados pessoais no centro do debate jurídico e social (Haikal, 2021, p. 296).

A pandemia de COVID-19, em particular, evidenciou a urgência de regulamentações robustas, ao mesmo tempo em que desafiou os limites dos direitos fundamentais em nome da saúde pública (Prux; Piai, 2020, pp. 143 – 165).

Historicamente, o conceito de privacidade evoluiu do mero *right to be left alone* para uma compreensão mais abrangente, impulsionada pelo avanço tecnológico. A era da informação e o surgimento do *Big Data* transformaram a privacidade de um direito estático e individualista para um conceito mais amplo e dinâmico: a autodeterminação informativa, um direito que assegura aos indivíduos o controle sobre a divulgação e o uso de seus dados pessoais, bem como o conhecimento sobre suas próprias informações. Isso implica o direito de decidir sobre a divulgação e uso dos dados pessoais, os limites de sua circulação, e o conhecimento sobre suas informações (Barroso, 2019, pp. 1270 – 1279).

Esse conceito, com origem no julgamento da Corte Constitucional Alemã de 1983, enfatiza que, no contexto do processamento automatizado de dados, não existem mais dados

insignificantes. O risco reside mais na finalidade e nas possibilidades do processamento do que na natureza ou sensibilidade dos dados em si (Barroso, 2019, pp. 1270 – 1279).

A informação se consolidou como a principal fonte de riqueza na "*sociedade capitalista digital*", com empresas de tecnologia detendo um poder crescente. A preocupação se deslocou para a indústria de dados, levantando questões sobre concorrência, tributação e, crucialmente, privacidade (Barroso, 2019, pp. 1270 – 1279).

Nesse cenário, a coleta e o tratamento de dados pessoais para a formação de perfis (*profiling*) se tornaram uma atividade constante tanto por parte de instituições governamentais quanto de empresas privadas, gerando o que alguns autores descrevem como uma "*vigilância permanente*" ou *Surveillance as a Service* – SVaaS (Castellano, 2022, pp. 1 – 22).

Este processo, ao monetizar atributos da personalidade, levanta sérias preocupações sobre a erosão de direitos em favor de entidades com posição monopolista transnacional (Font; Boff, 2023, pp. 1 – 18).

Assim, os dados pessoais são um dos ativos mais valiosos do século XXI, abrangem informações relacionadas a uma pessoa natural identificada ou identificável, como nome, endereço, telefone, e-mail, e até mesmo dados de localização. No entanto, a Lei Geral de Proteção de Dados (LGPD), no Brasil Lei nº 13.709/2018, e o Regulamento Geral de Proteção de Dados (GDPR), da União Europeia, fazem uma distinção crucial para os dados sensíveis.

Dados sensíveis são aqueles que, por sua natureza, podem resultar em práticas discriminatórias em caso de vazamentos ou acessos indevidos. A LGPD os define como dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (Brasil, 2018).

Devido a essa natureza íntima e ao alto potencial de dano, os dados sensíveis exigem uma proteção especial e regras mais rigorosas para seu tratamento. A informação de saúde, por exemplo, é privada e confidencial por natureza, revelando detalhes íntimos da vida de uma pessoa (Brasil, 2018).

No Brasil, a proteção de dados pessoais foi elevada à categoria de direito fundamental autônomo. O Supremo Tribunal Federal (STF), em maio de 2020, ao julgar as Ações Diretas de Inconstitucionalidade (ADIs) contra a Medida Provisória nº 954/2020, reconheceu expressamente a proteção de dados como um direito fundamental. Essa decisão foi posteriormente confirmada pela Emenda Constitucional nº 115/2022, que incluiu

expressamente a proteção de dados pessoais, inclusive nos meios digitais, no rol dos direitos e garantias fundamentais da Constituição da República Federativa do Brasil de 1988 (CF/88) (Brasil, 2022).

A crise da COVID-19 impulsionou governos e empresas a avançar em três categorias principais de coleta e uso de dados: i) coleta e uso de dados de saúde, ii) rastreamento e localização geográfica, e iii) parcerias público-privadas. Tecnologias como o rastreamento com precisão de sensores de localização integrados a smartphones tornaram-se ferramentas de monitoramento e contenção da propagação da doença. (Da Silva et al., 2022, pp. 1 - 23)

O contact tracing (rastreamento de contatos), por exemplo, tornou-se crucial para identificar pessoas contaminadas e expostas ao vírus, bem como sua rede de contatos, para isolamento e testagem. Essa rápida implementação de tecnologias de vigilância digital, no entanto, gerou uma preocupação global com os riscos à privacidade e aos direitos humanos, afinal a crise sanitária não pode ser um cheque em branco para o sacrifício indiscriminado de direitos fundamentais.

Organizações como a *Human Rights Watch* e a Comissão Interamericana de Direitos Humanos (CIDH) alertaram para o risco de discriminação e a possibilidade de que esses sistemas de vigilância se tornassem permanentes e abusivos, extrapolando o período emergencial.

O caso da Medida Provisória nº 954/2020, que previa o compartilhamento compulsório de dados de milhões de usuários de telefonia com o IBGE para produção estatística, ilustra as tensões envolvidas, sendo uma política federal que em razão do excesso e não pela carência de ação do governo no combate à pandemia exigiu controle de constitucionalidade (Wang et al., 2023).

Por sua vez, o Supremo Tribunal Federal (STF) suspendeu sua eficácia, argumentando que a medida provisória não delimitava a finalidade, a amplitude ou a necessidade da estatística a ser produzida, nem oferecia mecanismos suficientes para proteger os dados pessoais de acessos não autorizados, vazamentos ou uso indevido. Ministros como Rosa Weber, Ricardo Lewandowski, Edson Fachin e Luiz Fux ressaltaram que a emergência, por mais penosa que seja, não pode gerar um regime de incompatibilidade com a proteção de direitos fundamentais (Brasil, 2020).

Os riscos são ainda mais evidenciados quando se observa comparativamente o uso de provas de georreferenciamento no âmbito processual penal, onde a norma e jurisprudência brasileira também enfrenta o conflito de princípios basilares. Embora possa ser eficiente para

a persecução penal, não há solidez no ordenamento em relação à cadeia de custódia de provas de georreferenciamento quanto a busca reversa por dados de localização (obtendo IPs de todos os usuários em um local e hora específicos) para identificar suspeitos de crimes levanta a questão da violação da privacidade e autodeterminação informativa de inúmeras pessoas sem relação com a investigação (Smanio, 2021, pp. 49–76).

A legislação brasileira é esparsa e omissa nesse ponto, forçando o Superior Tribunal de Justiça (STJ) a ponderar a eficiência probatória com a limitação ao direito fundamental à privacidade do investigado. Para ser constitucional, tal medida exige reserva de jurisdição prévia e deve respeitar os requisitos de cautelaridade e subsidiariedade, além de uma delimitação temporal bem fundamentada para mitigar a violação de privacidade de terceiros inocentes (Smanio, 2021, pp. 49–76).

Mesmo em situações excepcionais, a observância de todos os direitos e garantias constitucionais contra o arbítrio estatal ganha ainda mais importância. O uso de tecnologias de rastreamento de contatos (*contact tracing*) durante a pandemia, por exemplo, deve seguir o protocolo da descentralização, usar abordagens baseadas em proximidade (como Bluetooth), empregar técnicas seguras de transmissão e encriptação de dados, e prever mecanismos de destruição dos dados coletados após o fim da crise. Além disso, a adesão a tais aplicativos deve ser facultativa para o cidadão (Pinheiro *et al.*, 2019).

Em que pese não tenha sido formatada especificamente para situações de pandemia, a Lei Geral de Proteção de Dados, Lei nº 13.709/2018, é um instrumento crucial para a proteção de dados pessoais no Brasil, seus princípios de finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização são plenamente aplicáveis. A LGPD também prevê a Autoridade Nacional de Proteção de Dados (ANPD), essencial para a fiscalização e garantia do cumprimento das normas (Brasil, 2018).

A proteção de dados é um direito multifacetado que exige constante atenção e adaptação às novas realidades tecnológicas. O desafio reside em equilibrar a inovação e o interesse público com a inalienável dignidade da pessoa humana, garantindo que o avanço tecnológico sirva à sociedade sem comprometer as liberdades e a privacidade individuais (Gemignani, 2023, pp. 1 – 332).

A experiência da pandemia revelou a necessidade de um reforço axiológico ao microssistema de proteção de dados pessoais, consolidando a autodeterminação informativa como um direito fundamental autônomo. Isso implica a adoção de princípios como *privacy by design*, minimização de dados, anonimização, segurança robusta no tratamento e

armazenamento, e descarte adequado das informações após o período da crise (Piccoli *et al.*, 2021, pp. 66 – 68).

Neste sentido, proteger os direitos digitais das pessoas também promove a saúde pública em seu sentido amplo, sem que se precise de vigilância abusiva e ilícita. A crise da COVID-19 não foi apenas uma nova pandemia, mas também um catalisador que expôs falhas institucionais e a necessidade de redesenhar os mundos sociotécnicos com base em valores humanos essenciais, garantindo que a tecnologia sirva ao interesse social.

3 TRATAMENTO DE DADOS E EXPERIÊNCIAS

As aplicações de rastreamento de contatos coletam e tratam dados pessoais, bem como incluem informações de saúde, geolocalização e proximidade. É fundamental compreender que o tratamento de dados pessoais, especialmente os relacionados à saúde, possui natureza privada e confidencial, justificando uma proteção abrangente na legislação.

Os principais modelos de processamento de dados são centralizado e descentralizado. No modelo centralizado, "os dados de todos os usuários são registrados em um servidor central, geralmente controlado por uma instituição pública ou privada". Quando um indivíduo testa positivo, "os identificadores de seus contatos anteriores são enviados ao sistema central, que os associa a aparelhos e notifica os usuários" (Da Silva et al., 2022, pp. 1 – 23).

Enquanto no modelo descentralizado, "uma entidade central não tem acesso às informações pessoais dos usuários". Os dispositivos geram "identificadores temporários que são compartilhados via Bluetooth com dispositivos próximos e armazenados criptograficamente em cada aparelho" (Da Silva et al., 2022, pp. 1 – 23).

Neste sentido, se um usuário é diagnosticado, ele pode compartilhar sua lista de identificadores passados com um servidor central, e outros dispositivos verificam se esses identificadores estão em suas próprias listas de contatos (Da Silva et al., 2022, pp. 1 – 23).

Este modelo "é considerado o que melhor protege a privacidade", visto que a maior parte das informações permanece fragmentada nos celulares (Da Silva *et al.,* 2022, pp. 1 – 23). A maioria dos trabalhos científicos aponta para a proteção do direito à privacidade por esse modelo, embora "*alguns estudos também mostrem ameaças, tornando os indivíduos mais suscetíveis a ataques virtuais*". As aplicações "*devem seguir o protocolo da descentralização*" (Da Silva et al., 2022, pp. 1 – 23).

As tecnologias de geolocalização empregadas incluem Global Positioning System (GPS), Bluetooth e Triangulação ou *Cell-Site Location Information* (CSLI). Em apertada síntese, o GPS compartilha "*coordenadas geográficas com alta precisão (raio de até 5 metros)*", é considerado mais invasivo, permitindo o mapeamento exato da localização de uma pessoa e a formação de perfis (Pinheiro *et al.*, 2019, p. 256).

Contudo, não é considerado confiável para "*determinar a proximidade exata para transmissão de doenças contagiosas*". Seu uso é "*mais crítico e, inclusive, desaconselhado por alguns estudiosos no combate à COVID-19, por apresentar riscos mais sérios à privacidade*" (Pinheiro *et al.*, 2019, p. 262).

O Bluetooth utiliza "*ondas curtas e baixa energia para comunicação entre dispositivos próximos*". Permite detectar quando duas pessoas estão a uma distância epidemiologicamente relevante (ex.: 1,5 a 2 metros por 15 minutos). A troca de identificadores via Bluetooth é anônima, e "o sistema de alerta não informa o local ou a identidade da pessoa infectada". Esta é a "tecnologia mais recomendada para proteção de dados pessoais" em aplicações de rastreamento de contato (Pinheiro *et al.*, 2019, p. 256).

Na Triangulação ou CSLI, a geolocalização é feita pelas empresas de telecomunicações, baseada na infraestrutura fixa da rede (torres, antenas, Estações Rádio Base – ERB) que determina a posição do aparelho celular pelo sinal recebido. A CSLI, a partir de uma torre, tem precisão de alguns quarteirões, enquanto a triangulação, usando múltiplas torres, tem precisão de poucos metros. Este método é utilizado para identificar a quantidade total de equipamentos conectados a uma antena, permitindo criar mapas de calor de aglomerações, "*geralmente sem identificar o titular*" (Smanio, 2021, pp. 49 – 76).

É crucial que essas aplicações utilizem dados anonimizados. A anonimização é uma técnica fundamental para proteger a privacidade, tornando um dado relativo a um titular não identificável por meio de "meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Da Silva *et al.*, 2022, pp. 1 – 23).

No entanto, o desafio reside na "reidentificação" de dados supostamente anonimizados. Estudos demonstram que, mesmo com a anonimização, é possível reidentificar indivíduos a partir de poucos pontos de dados. Por isso, não se pode falar em dados insignificantes, pois qualquer informação pessoal, ao ser cruzada com outras, pode levar à identificação (Prux; Piai, 2020, pp. 143 – 165).

Para garantir a efetividade da anonimização, é necessário que o processo seja irreversível ou que os esforços para reversão sejam desproibitivamente altos em termos de

custo e tempo, considerando as tecnologias disponíveis. Técnicas como a aleatorização ou generalização são recomendadas para que o dado perca a capacidade de associação, direta ou indireta, a um indivíduo (Pinheiro *et al.*, 2019, p. 260). A pseudonimização, que substitui identificadores por um código chave único mantido separadamente, é outra técnica crucial para dificultar a identificação do titular (Da Silva *et al.*, 2022, pp. 1 – 23).

O caso do Sistema de Monitoramento Inteligente (SIMI-SP) do Governo de São Paulo levantou questionamentos acerca do tratamento de dados pessoais. Embora alegasse usar apenas dados anonimizados de ERBs para medir níveis de isolamento e aglomeração, críticos apontaram a ausência de consentimento esclarecido dos usuários, a falta de transparência sobre a efetiva anonimização e as técnicas de segurança, e a possibilidade de discriminação algorítmica (Martins *et al.*, 2021, pp. 232 – 255).

A despeito de uma decisão judicial ter validado o uso por considerar os dados anonimizados, as preocupações com a segurança e a privacidade persistiram. Diversos exemplos ao redor do mundo ilustram os desafios e as armadilhas do uso de dados de geolocalização no combate à pandemia (Martins *et al.*, 2021, pp. 232 – 255).

A experiência asiática exemplifica o uso intensivo de dados para controle da pandemia, muitas vezes com menos salvaguardas de privacidade. A Coreia do Sul, por exemplo, rastreou e publicou dados detalhados online sobre a localização de pessoas infectadas, incluindo imagens de CFTV e histórico de uso de cartões de crédito (Prux; Piai, 2020, pp. 143 – 165).

O aplicativo chamado "Tracetogether", utilizado em Singapura, permitia às pessoas compartilharem voluntariamente suas informações e rastrear outras com quem entram em contato via Bluetooth. Se um usuário do aplicativo contrair COVID-19, todos os que entraram em contato com essa pessoa são notificados, juntamente com o governo, mas não há transparência sobre quem pode ter acesso a essas informações (Prux; Piai, 2020, pp. 143 – 165).

A China utilizou o aplicativo "*Alipay Health Code*", que gerenciava a quarentena por um sistema de cores, funcionando como um "passaporte" para acesso a serviços e transporte público. A atribuição de códigos de cores aos cidadãos tinha por base estado de saúde e histórico de viagens demonstram a capacidade de controle e vigilância em massa, levantando sérias questões sobre a liberdade individual (Prux; Piai, 2020, pp. 143 – 165),

Em Taiwan, foi implementado um "cercado eletrônico" para quarentenas, emitindo alertas e fazendo ligações se as pessoas se afastassem de seu local de isolamento. Embora

fosse uma medida de política pública, a implicação de vigilância constante e a invasão da liberdade de locomoção são evidentes (Prux; Piai, 2020, pp. 143 – 165).

Na Índia, os governos estaduais carregaram arquivos PDF online com nomes, endereços residenciais e histórico de viagens de pessoas em quarentena, tornando-os acessíveis a todos (Font; Boff, 2023, pp. 1 – 18).

Na Argentina e no Peru, jornais publicaram informações pessoais de pessoas infectadas, como idade, locais de viagem e hospitais. Similarmente, uma plataforma do Ministério da Saúde do Peru permitiu que relatórios de saúde de pacientes fossem acessados publicamente por alguns dias, apenas com o número de identidade, antes que um segundo autenticador fosse adicionado (Font; Boff, 2023, pp. 1 – 18).

4 LGPD, UM NORTEADOR

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, embora inspirada no RGPD, encontrava-se em período de vacatio legis durante boa parte da pandemia, o que gerou incerteza jurídica e, em muitos casos, a necessidade de consentimento expresso do titular para o tratamento de dados. No entanto, a legislação brasileira já possuía normas setoriais anteriores, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação e o Marco Civil da Internet, que garantiam alguma proteção de dados (Da Silva *et al.*, 2022, pp. 1 – 23).

O ordenamento jurídico brasileiro, influenciado por regulamentações internacionais como o Regulamento Geral de Proteção de Dados (RGPD) europeu, promulgou a Lei nº 13.709/2018 (LGPD). Esta lei define dado pessoal como informação relacionada a pessoa natural identificada ou identificável e, crucialmente, dado pessoal sensível, que abrange informações sobre saúde ou à vida sexual, dado genético ou biométrico. O tratamento de dados sensíveis exige "*camadas de proteção mais robustas e hipóteses legais específicas*" (Oliveira, 2022, p. 6).

O Regulamento Geral de Proteção de Dados (RGPD) da União Europeia (Regulamento UE 2016/679) é um marco regulatório global que serviu de forte inspiração para a Lei Geral de Proteção de Dados (LGPD) brasileira (Barroso, 2019, pp. 1270-1279). O enfoque da norma é a proteção dos direitos e garantias fundamentais dos cidadãos, buscando mitigar riscos na coleta, uso, compartilhamento e armazenamento de dados, e assegura a

soberania de cada indivíduo sobre seus dados, com direitos de acesso e retificação, além da exigência de consentimento prévio para o uso (Barroso, 2019, pp. 1270 – 1279).

No contexto da pandemia, o Comitê Europeu para a Proteção de Dados (CEPD) publicou diretrizes em 2020 que exigiam a realização de Avaliações de Impacto à Proteção de Dados (AIPDs) antes da implementação de ferramentas de rastreamento de contatos, priorizando dados de localização agregados e anonimizados. A União Europeia, por meio da Diretiva 2006/24, impôs a retenção de dados de tráfego para fins de investigação criminal, afetando "*quase toda a população europeia*" (Oliveira, 2022, p. 6).

Contudo, o Tribunal de Justiça da União Europeia declarou essa diretiva inválida, por exceder os limites da proporcionalidade, infringindo os direitos à privacidade e à proteção de dados, enfatizando a necessidade de regras claras e precisas para regulamentar o alcance e a aplicação de tais medidas (União Europeia, 2014).

A LGPD estabelece uma série de princípios que devem guiar o tratamento de dados pessoais. Dentre eles, destacam-se a finalidade (propósitos legítimos, específicos e informados), adequação (compatibilidade com as finalidades), e necessidade (limitação ao mínimo indispensável, pertinente e não excessivo). Outros princípios incluem transparência, segurança, prevenção, não discriminação, livre acesso, qualidade dos dados e responsabilização e prestação de contas (Da Silva *et al*, 2022, pp. 1 – 23). A regra para o tratamento é o consentimento do titular, que deve ser "*livre, informado e inequívoco*" (Oliveira, 2022, p. 6).

Contudo, a referida Lei permite que a administração pública trate dados pessoais sem consentimento para a "*execução de políticas públicas previstas em leis e regulamentos*", desde que observados os princípios gerais (Brasil, 2018). Essa era a base da Medida Provisória nº 954/2020 para determinar que operadoras de telecomunicações compartilhassem dados cadastrais (nome, telefone e endereço) de seus usuários com o Instituto Brasileiro de Geografia e Estatística (IBGE) para "*produção estatística oficial*" durante a pandemia de COVID-19. O Supremo Tribunal Federal (STF), em maio de 2020, suspendeu a eficácia (Brasil, 2020).

A decisão do Supremo Tribunal Federal foi emblemática ao reconhecer a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informativa. Os Ministros argumentaram que a Medida Provisória nº 954/2020 apresentava inconstitucionalidade formal por falta de urgência e relevância, e material por violar direitos

fundamentais como a dignidade da pessoa humana, a intimidade, a vida privada e o sigilo de dados (Brasil, 2020).

A Ministra Relatora Rosa Weber destacou que a MP não delimitava "*o objeto, a finalidade e a amplitude da estatística a ser produzida, bem como não esclarecia se havia necessidade de disponibilizar os dados e como estes seriam efetivamente utilizados*" (Fachin, 2022, pp. 298 – 313).

Em seu voto, o Ministro Gilmar Mendes ressaltou que "*a autonomia do direito fundamental em jogo nessa ADI exorbita, em essência, de sua mera equiparação com o conteúdo normativo da cláusula de proteção de sigilo*" (Fachin, 2022, pp. 298 – 313).

A Corte enfatizou que a situação de emergência "*não pode gerar um regime de incompatibilidade com a proteção de direitos fundamentais*", e que o compartilhamento de dados deve seguir "*mandamentos constitucionais e legais, observando uma estrita relação entre necessidade e adequação*" (Fachin, 2022, pp. 298 – 313).

A decisão da Ação Direta de Inconstitucionalidade (ADI) 6387 teve um impacto significativo sobre as empresas de telecomunicações, que detêm vastos volumes de dados pessoais, uma vez que a Medida Provisória nº 954/2020 impunha para essas empresas a transferência de dados cadastrais de milhões de usuários para o IBGE. O Supremo Tribunal Federal, ao suspender a Medida Provisória em questão, criticou a ausência de mecanismos técnicos e administrativos aptos a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida (Brasil, 2020).

A Agência Nacional de Telecomunicações (ANATEL) também recomendou "*extrema cautela no tratamento dos dados de usuários de serviços de telecomunicações*". Isso demonstra que a simples previsão de sigilo ou posterior eliminação dos dados não é suficiente sem garantias concretas de segurança e governança (Brasil, 2020).

5 LGPD E A PERSPECTIVA DE BIODADOS, BIOÉTICA E DIREITO À SAÚDE

No âmbito dos biodados e da saúde pública, a pandemia acelerou a adoção de tecnologias como a telemedicina e os aplicativos de rastreamento de contatos. Todavia, a implementação dessas ferramentas deu-se, em grande parte, sem regulamentação específica e consistente acerca da segurança das informações de saúde, as quais, por sua natureza sensível, demandam proteção mais rigorosa (Prux; Piai, 2020, pp. 143 – 165).

Os biodados podem ser definidos como informações obtidas a partir de características biológicas, fisiológicas, comportamentais ou de saúde de um indivíduo, capazes de identificá-lo ou de revelar aspectos relacionados à sua condição física, psicológica ou genética (Doneda, 2022).

Esse conceito engloba desde dados biométricos tradicionais — como impressões digitais, íris, voz e reconhecimento facial — até informações genéticas e de saúde, os chamados dados sensíveis pela legislação de proteção de dados, a exemplo da Lei Geral de Proteção de Dados (LGPD) no Brasil (Brasil, 2018) e do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia (União Europeia, 2016).

No campo jurídico e bioético, os biodados são considerados dados de natureza sensível porque envolvem elementos da identidade e da dignidade da pessoa humana. Por esse motivo, exigem proteção reforçada, em razão do risco de discriminação e de violação de direitos fundamentais (Doneda, 2022; Pinheiro *et al.*, 2024; Sarlet, 2021).

Assim, ao mesmo tempo em que os biodados são indispensáveis para avanços científicos, tecnológicos e de segurança, sua coleta, tratamento e armazenamento devem observar princípios como o da finalidade, da necessidade e da proporcionalidade, de forma a assegurar a privacidade e a autodeterminação informativa do titular (Doneda, 2022; Pinheiro *et al.*, 2022; Sarlet, 2021).

A doutrina e a jurisprudência internacionais, a exemplo do Regulamento Geral sobre a Proteção de Dados (RGPD), apontam para a necessidade de elaboração prévia de Relatórios de Impacto à Proteção de Dados (RIPD) antes da coleta e do tratamento em larga escala. No Brasil, entretanto, a Medida Provisória nº 954/2020 previa a elaboração desses relatórios somente após o compartilhamento, o que foi rechaçado pelo Supremo Tribunal Federal.

Emergem, daí, novas inquietações, notadamente quanto ao *profiling* (formação de perfis comportamentais) e à discriminação algorítmica. A ampla capacidade de armazenamento, cruzamento e manipulação de informações requer que a regulação estabeleça parâmetros objetivos e precisos, aptos a resguardar os dados pessoais contra abusos, acessos indevidos e usos ilícitos. Soma-se a isso a carência de transparência nos processos de tratamento e a incerteza quanto à efetividade da anonimização, fatores que intensificam a insegurança jurídica (Haikal, 2021, p. 296).

Entre as recomendações direcionadas a aplicativos de rastreamento, destacam-se a descentralização das bases, a utilização de tecnologias de proximidade (como o Bluetooth), protocolos seguros de transmissão e criptografia, bem como mecanismos que assegurem a

eliminação definitiva das informações ao término da pandemia (Da Silva *et al.,* 2022, pp. 1 – 23).

A consolidação do direito à saúde na Constituição da República Federativa do Brasil de 1988 representou um marco civilizatório para o Brasil. Ao declarar a saúde como "*direito de todos e dever do Estado*", a Carta Magna inaugurou um modelo universal e igualitário, fundado no princípio da dignidade da pessoa humana (Brasil, 1988).

Desde então, a saúde passou a ser analisada não apenas sob a ótica biomédica, mas também como um fenômeno jurídico e social, o qual exige políticas públicas de promoção, prevenção e reparação, além de mecanismos regulatórios que garantam sua efetividade.

Neste contexto, o advento da Lei Geral de Proteção de Dados (LGPD), em 2018, ampliou o debate sobre a tutela da saúde em meio ao avanço da digitalização. O setor de saúde, pela natureza sensível das informações que manipula, tornou-se campo privilegiado para observar os limites entre a autonomia individual, a proteção da privacidade e a necessidade de políticas públicas voltadas ao bem coletivo (Brasil, 2018).

O desafio, portanto, é articular o direito fundamental à proteção de dados com o direito fundamental à saúde, sem transformar um em obstáculo ao outro, mas reconhecendo a sua complementaridade (Brasil, 2018).

A saúde, enquanto direito social, foi incorporada ao ordenamento jurídico brasileiro em consonância com tratados internacionais de direitos humanos, como o Pacto Internacional sobre os Direitos Econômicos, Sociais e Culturais (PIDESC, 1992) e a Declaração Universal sobre Bioética e Direitos Humanos (Unesco, 2006). Ambos consagram a saúde como um bem coletivo, ligado à dignidade, igualdade e não discriminação.

Por outro lado, a proteção de dados pessoais emergiu inicialmente como uma dimensão do direito à privacidade, evoluiu para o conceito de autodeterminação informativa. No Brasil, esse movimento culminou no reconhecimento da proteção de dados como direito fundamental autônomo na Emenda Constitucional nº 115/2022.

Assim, ao lado do direito à saúde, surge uma nova fronteira jurídica: a garantia de que a coleta, o armazenamento e o tratamento de biodados – informações genéticas, biométricas e clínicas – respeitem valores éticos e constitucionais.

Com a globalização e o avanço tecnológico, os biodados tornaram-se um ativo econômico e estratégico. Sistemas de *Big Data* em saúde, inteligência artificial e telemedicina ampliaram a capacidade de análise epidemiológica e de personalização de tratamentos.

Contudo, também potencializaram riscos de *profiling*, discriminação algorítmica e mercantilização da vida humana.

A bioética, nesse ponto, exerce função essencial de mediação entre ciência, direito e sociedade. O princípio da não maleficência exige que o uso de dados não cause danos; o da justiça impõe critérios equitativos de acesso e tratamento; e o da autonomia assegura o consentimento informado como instrumento de autodeterminação.

Durante a pandemia da COVID-19, tais dilemas se intensificaram: tecnologias de rastreamento de contatos e sistemas de monitoramento de mobilidade coletiva foram utilizados em nome da saúde pública, mas sem a devida transparência sobre os riscos à privacidade. Como evidenciado na ADI 6387, o Supremo Tribunal Federal reforçou que medidas excepcionais não podem comprometer permanentemente garantias fundamentais.

A proteção de biodados não pode ser analisada isoladamente, mas no marco do direito à saúde. Enquanto a Constituição Federal de 1988 prevê a universalidade e integralidade do Sistema Único de Saúde (SUS), a LGPD assegura parâmetros de necessidade, adequação e proporcionalidade no tratamento de dados.

Nesse sentido, o direito à saúde não se limita à prestação de serviços clínicos, mas também inclui a salvaguarda da intimidade e da confidencialidade das informações pessoais. A tutela da saúde e da privacidade, portanto, devem caminhar juntas, reforçando a noção de que a escolha entre um ou outro é uma falsa dicotomia.

A bioética, ao estabelecer limites éticos para a inovação tecnológica, reforça esse entendimento, impedindo que a busca pela saúde coletiva se converta em justificativa para a erosão de direitos individuais.

A realidade contemporânea da saúde no Brasil exige uma interação constante entre Estado, sociedade civil e setor privado. Planos de saúde, hospitais privados e empresas de tecnologia passaram a manejar grandes volumes de dados sensíveis, muitas vezes sem controles transparentes.

Nesse cenário, cabe ao Estado não apenas regular, mas também fiscalizar e criar condições de governança de dados que garantam a confiança social. A Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel estratégico, mas ainda carece de estrutura robusta e autonomia política para impor sanções e exigir conformidade.

Por sua vez, a sociedade civil deve ser protagonista na construção de uma cultura de proteção de dados, exigindo transparência, consentimento informado e prestação de contas. O setor privado, por fim, precisa internalizar práticas de *privacy by design* e *privacy by default*,

para evitar que a exploração econômica dos dados comprometa os fundamentos éticos e jurídicos da saúde.

O aumento da judicialização da saúde no Brasil revela tanto a insuficiência das políticas públicas quanto a confiança da população no Poder Judiciário como garantidor de direitos. Nos últimos anos, a judicialização expandiu-se para além da cobertura de medicamentos e tratamentos, alcançando também a proteção de dados sensíveis, sobretudo diante de falhas de segurança em plataformas de saúde digital.

O desafio futuro será equilibrar o interesse público sanitário com a garantia da privacidade, fortalecendo tanto o SUS quanto a governança digital em saúde. É nesse ponto que o Direito, aliado à bioética, assume função instrumental: assegurar que a inovação tecnológica se converta em benefício humano, e não em nova forma de exclusão e vulnerabilidade.

6 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo desta pesquisa evidenciou que a proteção de dados pessoais, especialmente aqueles relacionados à saúde, tornou-se uma dimensão central do debate contemporâneo sobre o direito à saúde.

Desde a Constituição Federal de 1988, a saúde foi consagrada como direito de todos e dever do Estado, impondo a formulação de políticas públicas capazes de assegurar sua universalidade e integralidade. Contudo, as transformações tecnológicas e a globalização trouxeram novos desafios, ampliando a interdependência entre Estado, sociedade civil e setor privado na governança da saúde e dos biodados.

O problema de pesquisa — qual a garantia de manipulação adequada dos dados pessoais para fins de avaliação e gestão de riscos à saúde pública, conciliando a preservação da privacidade com a tutela da coletividade — revelou que não se trata de uma oposição entre direitos, mas de uma necessária complementaridade. As hipóteses levantadas foram confirmadas: i) a proteção de dados sensíveis em contextos emergenciais envolve relevantes implicações bioéticas; ii) a dicotomia entre privacidade e direito à saúde é ilusória, sendo possível e imperativo assegurar ambos.

A investigação demonstrou que a LGPD representa um marco jurídico fundamental para a construção de parâmetros de necessidade, adequação e proporcionalidade no

tratamento de dados pessoais, ainda que sua implementação demande maior robustez institucional.

A ADI 6387, por sua vez, assumiu papel paradigmático ao afirmar a proteção de dados como direito fundamental autônomo e ao estabelecer balizas constitucionais para a utilização de informações sensíveis em situações de crise. Essa decisão do Supremo Tribunal Federal consolidou a ideia de que a emergência sanitária não pode justificar a suspensão arbitrária de garantias constitucionais.

Os resultados obtidos indicam que o fortalecimento da proteção de dados não fragiliza a saúde pública; ao contrário, reforça a confiança social necessária para o êxito das políticas sanitárias. A experiência da pandemia mostrou que tecnologias como *Big Data*, inteligência artificial e rastreamento de contatos podem ser instrumentos valiosos de gestão, mas devem operar sob a perspectiva da bioética, da transparência e da *accountability*, evitando a mercantilização e a vigilância abusiva dos corpos.

Nesse sentido, o Direito desempenha papel instrumental, ao oferecer mecanismos normativos e jurisprudenciais para equilibrar inovação tecnológica e dignidade humana. A judicialização da saúde, ampliada também para a proteção de dados, evidencia a confiança no Poder Judiciário como instância de garantia dos direitos fundamentais.

Conclui-se, portanto, que a efetividade do direito à saúde, no Brasil e em âmbito global, depende da articulação entre políticas públicas inclusivas, regulação responsável e práticas éticas de tratamento de dados. A proteção da privacidade e a promoção da saúde não são interesses antagônicos, mas sim pilares complementares de um mesmo projeto civilizatório, comprometido com a cidadania, a igualdade e a dignidade da pessoa humana.

REFERÊNCIAS

BARROSO, Luís Roberto. **Revolução tecnológica, crise da democracia e mudança climática: limites do Direito num mundo em transformação.** Revista Estudos Institucionais, v. 5, n. 3, p. 1262-1313, set./dez. 2019. Disponível em: https://doi.org/10.21783/rei.v5i3.429. Acesso em: 16 ago. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 16 ago. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 16 ago. 2025.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 16 ago. 2025.

BRASIL. Supremo Tribunal Federal (STF). **Ação Direta de Inconstitucionalidade nº 6387 / Distrito Federal – Relator: Ministro Alexandre de Moraes. Julgamento em 07 mai. 2020.** Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5880769. Acesso em: 17 ago. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 17 ago. 2025.

BRASIL. **Pacto Internacional dos Direitos Econômicos, Sociais e Culturais (PIDESC).** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0591.htm. Acesso em: 17 ago. 2025.

CASTELLANO, Guillermo Rodrigo Corredor. ***Aplicaciones de rastreo y monitoreo: del entusiasmo tecnológico al reconocimiento de la autodeterminación informática.*** Revista Direito GV, São Paulo, v. 18, n. 2, e2225, maio/ago. 2022. Disponível em: https://doi.org/10.1590/2317-6172202225. Acesso em: 16 ago. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. ***Judgment of the Court (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof. Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union. Joined Cases C-293/12 and C-594/12.*** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62012CJ0293. Acesso em: 16 ago. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).*** Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Acesso em: 17 ago. 2025.

DA SILVA, Ana Marília Dutra Ferreira; DA SILVA, Carlos Eduardo; DE SIQUEIRA, Mariana MARQUES, Kayo Victor Santos. **Proteção de dados pessoais e direito à privacidade no contexto da pandemia de COVID-19: uma análise das aplicações de *contact tracing* à luz da proporcionalidade.** Revista Direito GV, São Paulo, v. 18, n. 3,

e2232, set./dez. 2022. Disponível em: https://doi.org/10.1590/2317-6172202232. Acesso em: 16 ago. 2025.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Revista dos Tribunais, 2021.

FACHIN, Zulmar Antonio. **O direito fundamental à proteção de dados pessoais: análise da decisão paradigmática do STF na ADI 6.387-DF.** Revista Videre, Dourados–MS, v. 14, n. 29, pp. 298-313, jan./abr. 2022. Disponível em: https://ojs.ufgd.edu.br/index.php/videre/article/view/15629. Acesso em: 16 ago. 2025.

FONT, Jorge Luis Ordelin; BOFF, Salete Oro. ***El uso de las aplicaciones tecnológicas para el enfrentamiento del COVID-19 en América Latina – ¿Quo vadis?*** Revista de Direito Sanitário, São Paulo, v. 23, n. 1, e0008, 2023. Disponível em: https://doi.org/10.11606/issn.2316-9044.rdisan.2023.186259. Acesso em: 16 ago. 2025.

GEMIGNANI, Daniel. **As diversas perspectivas da colisão de direitos humanos na era digital: elementos para a compreensão e para a solução de aparentes antinomias.** Revista do Tribunal Regional do Trabalho da 15ª Região, Campinas, n. 63, pp. 1 - 332, jul./dez. 2023. Disponível em: https://www.stj.jus.br/webstj/Institucional/Biblioteca/artigo/Detalhe.asp?seq_revista=350. Acesso em: 16 ago. 2025.

HAIKAL, Victor Auilo. **Análise Crítica da Proteção de Dados Pessoais Durante o Período de Contingência da COVID-19**. Revista Eletrônica de Direito do Centro Universitário Newton Paiva. Belo Horizonte. n. 43. jan./abr. 2021. pp. 293-313. Disponível em: https://revistas.newtonpaiva.br/redcunp/wp-content/uploads/2021/06/DIR43-17.pdf. Acesso em: 17 ago. 2025.

MARTINS, Guilherme Magalhães; BASAN, Arthur Pinheiro; FALEIROS JÚNIOR, José Luiz de Moura**. O direito fundamental à proteção de dados pessoais e a pandemia da COVID-19.** Revista Eletrônica de Direito do Centro Universitário Newton Paiva, Belo Horizonte, n. 43, pp. 232-255, jan./abr. 2021. Disponível em: https://revistas.newtonpaiva.br/redcunp/wp-content/uploads/2021/06/DIR43-14.pdf. Acesso em: 16 ago. 2025.

OLIVEIRA, Diogo Luís Manganelli. **Telemedicina no Brasil: ameaças à proteção de dados pessoais em decorrência da flexibilização da pandemia e da regulamentação precária.** Revista de Direito Sanitário, São Paulo, v. 22, n. 2, e0011, 2022. Disponível em: https://doi.org/10.11606/issn.2316-9044.rdisan.2022.176159. Acesso em: 16 ago. 2025.

PICCOLI, Ademir Milton; LUNARDI, Fabrício Castagna; CLEMENTINO, Marco Bruno Miranda (Coord.). **Inovação judicial: fundamentos e práticas para uma jurisdição de alto impacto.** Brasília: Enfam, 2021. 510 p. ISBN 978-65-88022-07-8. Disponível em: https://www.enfam.jus.br/wp-content/uploads/2021/12/Livro-Inovacao-judicial.pdf. Acesso em: 16 ago. 2025.

PINHEIRO, Guilherme Pereira; PINHEIRO, Alexandre Pereira. **COVID-19 e geolocalização: entre a saúde e a proteção de dados pessoais.** Revista Jurídica da

Presidência. Brasília, v. 24 n. 132 Fev./Abr. 2020 p. 245-268 Disponível em: https://doi.org/10.20499/2236-3645.RJP2022v24e132-2252. Acesso em: 16 ago. 2025.

PINHEIRO, Patricia Peck Garrido *et al*. **Direito Digital Aplicado 4.0**. 6. ed. São Paulo: Revista dos Tribunais, 2024.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais – Comentários à Lei nº 13.709/2018 (LGPD).** 4.ed. São Paulo: Saraiva, 2022.

PRUX, Oscar Ivan; PIAI, Kevin Henrique de Sousa. **Opacidade algorítmica e o *credit scoring* no mercado de consumo.** Revista de direito do consumidor, v. 29, n. 132, pp. 143-165, nov./dez. 2020. Disponível em: https://dspace.mj.gov.br/handle/1/3544. Acesso em: 16 ago. 2025.

SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. 2.ed. Rio de Janeiro: Forense, 2023.

SMANIO, Gianluca Martins. **A busca reversa por dados de localização na jurisprudência do Superior Tribunal de Justiça: análise crítica do RMS 61.302/RJ.** Revista Brasileira de Ciências Policiais, Brasília, Brasil, v. 12, n. 5, pp. 49–76, 2021. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/840/. Acesso em: 16 ago. 2025.

UNESCO. **Declaração Universal sobre Bioética e Direitos Humanos.** Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000146180_por. Acesso em: 17 ago. 2025.

WANG, Daniel Wei Liang; ARRUDA, Ana Luiza Gajardoni de Mattos; DE OLIVEIRA, Bruno da Cunha; DOS SANTOS, Ezequiel Fajreldines; MORIBE, Gabriela Tiemi; HECK, Leonardo Nochang; ESTEVES, Luiz Fernando Gomes; PEDRO; Marcela Pereira. **O STF e as medidas para prevenção e tratamento da covid-19.** Revista Direito GV, São Paulo, v. 19, e2336, 2023. Disponível em: https://doi.org/10.1590/2317-6172202336. Acesso em: 16 ago. 2025.