CENTRO UNIVERSITÁRIO DE ENSINO SUPERIOR DOM BOSCO – UNDB
CURSO DE DIREITO

ISABEL NAUFEL COSTA

PROTEÇÃO DE DADOS VERSUS SAÚDE PÚBLICA DURANTE A PANDEMIA DE COVID-19 NO BRASIL

São Luís
2022

ISABEL NAUFEL COSTA

PROTEÇÃO DE DADOS VERSUS SAÚDE PÚBLICA DURANTE A PANDEMIA DE COVID-19 NO BRASIL

Monografia apresentada no Curso de Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharela em Direito.

Orientadora: Profa. Ma. Manuela Ithamar Lima

São Luís

2022

Dados Internacionais de Catalogação na Publicação (CIP)
Centro Universitário – UNDB / Biblioteca

Costa, Isabel Naufel

Proteção de dados versus saúde pública durante a pandemia de Covid-19 no Brasil. / Isabel Naufel Costa. __ São Luís, 2022.
62 f.
Orientador: Profa. Ma. Manuela Ithamar Lima.
Monografia (Graduação em Direito) - Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2022.
1. Proteção de dados. 2. Direito à saúde. 3. Pandemia de Covid-19.
4. Direitos fundamentais. I. Título.

CDU 342.7:616-036.21

ISABEL NAUFEL COSTA

PROTEÇÃO DE DADOS VERSUS SAÚDE PUBLICA DURANTE A PANDEMIA DE COVID-19 NO BRASIL

Monografia apresentada ao Curso de Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovada em: 26/06/2022.

BANCA EXAMINADORA

Ma. Manuela Ithamar Lima (Orientadora)

Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB

Ma. Ma. Stephane Hilda Barbosa Lima

Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB

Esp. Bruno Tomé Fonseca

Faculdade Santa Terezinha e Faculdade São Luís.

A minha família, meus apoiadores constantes e
que me fazem sempre querer aprender mais

AGRADECIMENTOS

Esse trabalho é dedicado para diversas pessoas, uma vez que todas elas foram fundamentais para que eu chegasse até a minha formação universitária. A primeira pessoa que eu agradeço é a minha mãe, que foi minha primeira professora, minha maior apoiadora e incentivadora. Ao meu pai que me deu todo o suporte para chegar aqui.

Agradeço também a minha vó, que me ensinou nos meus anos fundamentais, tanto assuntos escolares como na vida. A minha irmã por ser um grande modelo na minha vida, além de me gerar inquietações sobre o direito e fomentar cada vez mais minha vontade de aprender. A minha tia Monica pela constante disponibilidade.

As minhas amigas de faculdade que viraram também amigas de vida, Sara e Isabelle.

A minha orientadora Manuela Ithamar Lima que me incentivou a prosseguir com esse tema e que me ajudou a chegar até aqui.

“A tecnologia não é nem boa, nem ruim e também não é neutra”

Melvin Kranzberg

RESUMO

A Pandemia do vírus Covid-19 trouxe diversos desafios para garantir o Direito a Saúde Pública, criando novos problemas também a para a garantia do Direito à Proteção de Dados pessoais. O presente trabalho reside na tentativa de analisar como ocorre o tratamento dos dados de saúde no contexto da pandemia de Covid-19 no Brasil e se o Direito Fundamental à Proteção de Dados está sendo concretizado nesse contexto, através de uma análise acerca das ferramentas mais utilizadas durante o período e as medidas já tomadas pelo governo utilizadas para minimizar os problemas na proteção de dados, buscando técnicas para implementação de um modelo capaz de ajudar a reduzir o contágio de Coronavírus e ainda assim garantir a proteção de dados. Utilizar-se-á como método hipotético-dedutivo, realizando-se uma análise de diferentes fontes bibliográficas para se chegar a uma conclusão. Para a construção desse trabalho se fez necessária uma pesquisa de cunho bibliográfico, utilizando-se de livros, artigos científicos, legislações e jurisprudências de modo a concluir se o direito à proteção de dados foi concretizado no contexto da pandemia de covid-19. Observou-se que grande parte das normas que regulamentam o direito Proteção de Dados foram cumpridas, entretanto, por vezes deixou de ser cumprido, em especial os casos em que houve conflito entre o direito à Proteção de Dados, havendo um conflito de direito fundamentais. Depreende-se, por fim, que poderiam ser adotadas medidas como a elaboração de normas específicas sobre o tratamento de dados de saúde e a maior fiscalização do cumprimento das normas atuais pelo ANPD.

Palavras-chave: Proteção de dados; direito à saúde; pandemia de Covid-19; direitos fundamentais; LGPD.

ABSTRACT

The Covid-19 virus pandemic brought several challenges to ensure the Right to Public Health, creating new problems as well to guarantee the Right Data Protection. This study aims to analyze how the treatment of health data occurs in the context of the Covid-19 pandemic in Brazil and whether the Fundamental Right to data protection is being implemented in this context, through an analysis of the most used tools during this period and the measures already taken by the government used to minimize problems in data protection, seeking techniques that helps to reduce the contagion of Coronavirus and still guarantee data protection. It will be used as a hypothetical-deductive method, carrying out an analysis of different bibliographic sources such as: books, scientific articles, legislation and jurisprudence in order to conclude whether the right to data protection was implemented in the context of the covid-19 pandemic in Brazil. It was observed that most of the rules that regulate the right to data protection were complied with, although there were still instances that the right was not followed, specifically cases that occurred a conflict between the right to data protection, with a conflict of the right of health. Finally, it appears that measures could be adopted such as the development of specific rules on the treatment of health data and greater inspection of compliance with current rules by the Brazil national data authority.

Keywords: data protection; health data; Covid-19; pandemic; LGPD

LISTA DE SIGLAS

CDC	Código de Defesa do Consumidor
CFM	Conselho Federal de Medicina
DATASUS	Departamento de Informática do SUS
ESD28	Estratégia de Desenvolvimento em Saúde para o Brasil 2020-2028
GPDR	General Data Protection Regulation (Regulamento Geral de Proteção de Dados Europeu)
IBGE	Instituto Brasileiro Geográfico e Estatísticas
HC	Habeas Corpus
LGPD	Lei Geral de Proteção de Dados
MP	Medida Provisória
OCDE	Organização para a Cooperação e Desenvolvimento
OMS	Organização Mundial da Saúde
ONU	Organização das Nações Unidas
PEP	Prontuários Eletrônicos do Paciente
PL	Projeto de Lei
RNDS	Rede Nacional de dados em Saúde
STF	Supremo Tribunal Federal
SUS	Sistema Único de Saúde
WHO	World Health Organization
WMA	World Medical Association

SUMÁRIO

1. INTRODUÇÃO

Em 11 de março de 2020 foi caracterizada a situação de Pandemia do COVID-19 pela Organização Mundial de Saúde. Detectado, pela primeira vez, na China, ainda no ano de 2019, o vírus se espalhou rapidamente por toda a Europa, chegando ao Brasil em 26 de fevereiro de 2020, quando tivemos o primeiro caso confirmado. Tendo esse vírus como característica principal a grande transmissibilidade, associada a possibilidade da pessoa que se contamina com o vírus não apresentar sintomas, não demorou para que o País já em março de 2020 apresentasse curva crescente de casos, tornando-se algumas vezes o centro desse epicentro na Pandemia. As características do coronavírus, assim como o próprio quadro pandêmico instalado, exigiram respostas rápidas, fazendo com que métodos tradicionais, como o mapeamento manual de informações fosse considerado ineficaz no combate ao vírus.

O diagnóstico realizado de maneira mais rápida, com a identificação de possíveis transmissores da doença, assim como o tratamento de dados relativos à COVID-19 mostrou-se um importante aliado para o combate e contenção da pandemia. O uso da tecnologia mostra-se fundamental nesse processo, possibilitando a informação rápida e simultânea a pessoas possivelmente infectadas, além de maior informação ao governo para a tomada de medidas sanitárias, bem como para pesquisadores desenvolverem pesquisas, tratamentos e vacinas.

Não é a primeira vez que a tecnologia é utilizada no combate a contenção de doenças, pode-se citar como principal e mais relevante exemplo o da epidemia do Ebola em 2015. Apesar disso, diferentemente das crises de saúde pública anteriores, a tecnologia evolui bastante e consequentemente apresenta novas possibilidades, bem como novas consequências, entre elas a utilização de dados pessoais em desacordo com normas que regem tal Direito Fundamental.

O presente trabalho visa apresentar uma análise crítica acerca da coexistência do direito fundamental à Proteção de Dados e o Direito à Saúde no contexto da pandemia de COVID-19 no Brasil. É nesse sentido que se busca esclarecer os principais contornos do tratamento dos dados de saúde no Brasil, as normas que regulam a matéria e a jurisprudência sobre esse tópico.

Assim, o objetivo geral do presente trabalho é, então, analisar se o Direito Fundamental à Proteção de Dados foi concretizado frente o Direito à saúde no contexto da pandemia de Covid-19 no Brasil.

A acadêmica optou por esse tema após perceber a importância da proteção dos dados na sociedade atual e dos problemas enfrentados durante a pandemia no que se refere à

proteção da saúde e da vida da população. A utilização de técnicas e ferramentas virtuais ajudaram na contenção da pandemia de Covid-19. Além disso, acredita-se na real possibilidade do surgimento de outras doenças endêmicas e pandêmicas, como consequência da globalização, que exigirão do Brasil, assim como de outros países, a resposta adequada para seu enfrentamento, sem que se descuide do Direito à Proteção de Dados. Logo, a pesquisa busca não só analisar o ocorrido, mas relatar os problemas enfrentados durante o período no que tange a proteção de dados para evitá-los no futuro, diante da infeliz possibilidade de novas endemias.

Este trabalho utilizará o método hipotético-dedutivo, utilizando-se de materiais já disponíveis para tentar responder à pergunta principal do trabalho e atingir seu objetivo, valendo-se dos conteúdos já disponíveis sobre o assunto em questão. Além disso, o método utiliza a estrutura de indagações, seguidas de possíveis respostas, tomando como base deduções e conjecturas, que serão comprovadas, ou não, ao longo do trabalho (GIL, 2008).

A presente pesquisa será descritiva, trazendo sobre o tema em análise as considerações e ponderações já realizadas sobre o tema. A pesquisa será também de cunho bibliográfico, para tanto serão utilizados artigos científicos, matérias de jornais, sites, dissertações, teses e livros publicados, legislação, em especial da Lei Geral de Proteção de Dados - LGPD e as jurisprudências dos Tribunais Superiores.

Nesses termos, o trabalho será desenvolvido em três capítulos, onde o primeiro buscará apresentar uma análise acerca da sociedade atual, também chamada de sociedade da informação, explicando seus principais contornos, bem como o significado dos dados pessoais, a sua importância e a fundamentalidade de sua proteção, nesse cenário social. Ainda nesse capítulo será revelada a amplitude objetiva e subjetiva do direito à Proteção de Dados e a evolução histórica desse direito, demonstrando-se o seu desenvolvimento, utilizando-se, para tanto, de normas e jurisprudência interna e estrangeira.

Estabelecidas tais premissas, no segundo capítulo o estudo se concentra na forma que a atual legislação regula os dados pessoais, em especial os dados sensíveis, categoria a qual pertencem os dados de saúde. Outrossim, serão apresentadas as principais formas como os dados de saúde são coletados na atualidade, pontuando-se as principais formas encontradas na doutrina atual, entre elas os prontuários eletrônicos dos pacientes, a telemedicina e por fim os aplicativos de monitoramento utilizados, e como esses são tutelados durante a pandemia.

No terceiro capítulo será tratado sobre como a LGPD regulamenta especificamente o tratamento dos dados de saúde. Em seguida explicita-se a técnica da ponderação e como essa pode ser utilizada para a resolução da colisão entre direitos fundamentais, analisando-se a técnica a ser utilizada, suas críticas e como essas últimas podem ser minimizadas. Por fim,

conclui-se com a possibilidade de responsabilização civil dos agentes reguladores de dados, caso ocorra a violação do direito à proteção de dados.

2. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NO CONTEXTO DA PANDEMIA

O desenvolvimento tecnológico iniciado desde a Revolução Industrial gerou grande impacto na sociedade, mais recentemente essas transformações passaram a ser percebidas com cada vez mais velocidade na eletrônica, nas telecomunicações, entre outras. Esses impactos podem ser vistos na vida cotidiana nas mais diversas formas, como na utilização de celulares. Com esse desenvolvimento surgem também preocupações inerentes ao mesmo, principalmente relacionadas à privacidade, que terão reflexos também no campo jurídico (DONEDA, 2020). Isso poderá ser observado nos tópicos a seguir:

2.1 A Sociedade Da Informação e os Dados Pessoais

A sociedade passou por profundas e rápidas transformações nas últimas décadas, alavancadas especialmente pelos avanços tecnológicos que passaram a permear todos os aspectos da vida dos indivíduos. Essas mudanças foram percebidas por pesquisadores sociais que passaram a denominar a sociedade atual de sociedade da informação ou sociedade do risco. O conceito de sociedade da informação abarca as transformações técnicas e organizacionais administrativas ocorridas no período pós-industrial (Werthein, 2000).

Esse novo contexto social se caracteriza não só pelo avanço tecnológico, mas principalmente pelo *informacionalismo* que dá novos contornos ao capitalismo. A tecnologia se mostra central pois é através dela que há a criação e desenvolvimento científico, que em um sistema de processamento e comunicação se retroalimenta constantemente. A forma como esses processos ocorrem, acabam facilitando a inserção de um maior número de indivíduos, tornando o processo de criação mais disperso e melhor distribuído por toda a sociedade (CASTELLS, 2002).

Alerta-se que o problema atual não é se adaptar nessa sociedade, mas encontrar defesas para as invasões na esfera privada, que se tornam cada vez mais frágeis. Na atualidade, os processos e a infraestrutura da informação são um dos principais componentes que dificultam essa defesa. Enquanto os indivíduos buscam a proteção sobre seus dados, as instituições públicas e privadas buscam cada vez mais novas formas de coleta e tratamento de informações (RODOTÁ, 2008).

Nesse contexto, o termo “PROTEÇÃO DE DADOS” se populariza cada vez mais. Novas normas para tratar o tema surgem, como, por exemplo, a Lei Geral de Proteção de Dados,

entretanto, a população muito pouco sabe e entende sobre o tema. Logo, diante dessa falta de informação, dificulta-se a proteção desse direito fundamental. Dessa forma, pretende-se inicialmente descrever o seu significado e amplitude.

A partir da década de 1980 houve o incentivo massivo do acesso à internet e do avanço tecnológico (MOURA, 2019, p. 14). Como consequência, a sociedade passou a ficar mais conectada, mudando comportamentos e a forma como as pessoas se relacionam. O uso massivo da tecnologia acaba por gerar uma enorme quantidade de dados, em um sistema que se retroalimenta com informações disponibilizadas pelos usuários. Surge nesse contexto um novo mercado econômico que se abastece de dados disponíveis na internet (ARAÚJO, 2019).

As informações disponibilizadas pelos usuários são as mais diversas e variadas possíveis e criam um sistema que é capaz de conhecer a pessoa mais do que ela mesmo. São exemplos dessas informações: quais são os aplicativos utilizados, os dados pessoais disponibilizados pelos usuários, além do monitoramento de informações quase subconsciente da tomada de decisão, como: "[...] o tempo em que os usuários permanecem conectados, quais as páginas visitadas, quantas e quais as fotos e vídeos foram curtidos e até mesmo a velocidade e a força aplicada ao digitar e interagir com os mais diversos dispositivos eletrônicos" (ARAÚJO, 2019, p. 16).

Os dados nesses cenários seriam as informações colhidas nos meios digitais, porém, mais que isso, seriam tais informações colhidas e organizadas visando garantir vantagens econômicas (ARAÚJO, 2019). A coleta de informações não começou com a popularização da internet, mas se tornou mais prejudicial para a população atualmente, com o aumento da quantidade de dados colhidos (SANTOS, 2019).

A grande quantidade de dados coletados exigiu a criação de novos mecanismos de organização. Chamada de *Big Data*, tal tecnologia serviria para ajudar a classificar os dados, devido a crescente valorização dessas informações, que passaram, inclusive, a ser conhecidas como o "novo petróleo", enquanto a organização dos dados passou a ser chamada de mineração, uma vez que só após esse processo, os dados disponibilizados passam a ter valor similar ao de minérios preciosos (SANTOS, 2019).

A inteligência artificial utilizada pelos programas serve ainda para prever possíveis comportamentos dos usuários, através de técnicas de perfilhamento das informações fornecidas, tomando decisões baseadas nessas informações (KAMARINOU; MILLARD; SINGH, 2017). Tais informações não precisam necessariamente ser corretas ou não, mas apenas se encaixarem em um perfil estabelecido ou desviar desse (MARTINS, 2019).

A Lei Geral de Proteção de Dados trata especificamente da forma como esses dados pessoais serão tratados. Cabe mencionar que existiriam dados que não seriam pessoais, são aqueles que não são passíveis de identificação (MASSENO, 2020). Nesse sentido, cabe mencionar que as legislações atuais têm dificuldade para estabelecer parâmetros para a definição do grau de identificação, ocorrendo inúmeras ocasiões em que dados que seriam teoricamente não identificáveis, acabaram se mostrando identificáveis, ou ainda, trazendo danos para os criadores da informação (SCHWARTZ; SOLOVE, 2011).

Observa-se que os avanços tecnológicos, cada vez mais, fazem com que seja possível a realização da identificação de a quem pertencem os dados, através de métodos que anteriormente não eram possíveis. Ao lado desse avanço tecnológico, se tem também a escalada de dados, que seria o aumento posterior da quantidade de informações disponibilizadas, a facilitar a identificação do detentor dos dados (MASSENO, 2020). Existem, também, dados passíveis de reidentificação, apesar de processos de anonimização, o que seria igualmente problemático (SCHWARTZ; SOLOVE, 2011).

Cita-se como exemplo dessa problemática o caso do *Netflix Prize*, no qual houve a reidentificação de dados da plataforma da Netflix, apesar da inclusão de dados falsos, que combinados com dados obtidos em outras plataformas, com informações disponibilizadas pelos próprios usuários, foram capazes de fazer a identificação dos usuários. A fim de que as normas não se tornassem tautológicas, a solução foi criar um parâmetro de elasticidade para a definição de dados não pessoais, como aqueles que precisam de um mínimo de esforço para identificar a quem pertenciam os dados (BIONI, 2019).

Apesar dos dados não pessoais se mostrarem importantes pelo potencial poder de lesionar os direitos pessoais dos usuários, o presente trabalho foca nos dados pessoais. Tais dados são definidos pela Lei como aqueles identificados e passíveis de identificação (BRASIL, 2018). Apesar de, em regra, a legislação não se mostrar suficiente para conceituar os institutos por ela tratados, observa-se que nesse caso, a definição encontra-se de acordo com a melhor doutrina (BIONI, 2019).

Os dados tratados na LGPD podem ser divididos em dados pessoais e dados pessoais sensíveis (BRASIL, 2018). Esses dados podem ainda ser divididos de outras formas, utilizando-se como critérios: a informação disponível, a quem pertencem os dados, ou a forma de tratamento dos mesmos. A LGPD cita alguns tipos de dados, entre eles: os dados pessoais, dados pessoais sensíveis, dados anonimizados, dados pseudo-anonimizados e dados de crianças e adolescentes (MARTINS, 2019). A distinção se revela importante, a depender da classificação, para observar o nível de proteção que uma informação deva receber ou mesmo

para que se observe se a pessoa é capaz de consentir em quais informações podem ser recolhidas, uma vez que algumas pessoas não possuem capacidade de consentimento, como por exemplo as crianças (SOUSA; FRANCO, 2020).

2.2 A fundamentalidade do Direito à Proteção de Dados na sua dupla dimensão

Após a abordagem realizada acerca do que seriam os dados e a necessidade de sua proteção, se faz necessário entender o que estaria englobado pelo Direito à Proteção de Dados. O Direito à Proteção de Dados no Brasil foi consagrado pela emenda constitucional n. 115, que inseriu no art. 5° da Constituição, o inciso LXXIX: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". A inclusão de tal direito no art. 5º da Constituição Federal aponta, em princípio, a vontade do legislador em garantir status de direito fundamental ao Direito à Proteção de Dados (BRASIL, 2022a).

A doutrina pátria leciona sobre a existência de uma dupla dimensão dos direitos fundamentais, existindo uma dimensão objetiva e outra subjetiva. Sarlet, que é dos autores que mais se dedicou ao assunto, revela que a dimensão subjetiva dos direitos fundamentais garante ao indivíduo a qualidade de sujeito de direitos, que podem ser juridicamente exigíveis na esfera judicial (SARLET, 2019).

A dimensão subjetiva dos direitos fundamentais é importante por regular a forma como tais direitos influenciam as relações jurídicas (FERREIRA; BRANCO, 2021). Diferentemente do que ocorria no começo das formulações sobre o tema, atualmente entende-se que esses direitos não são mais exigíveis somente em relação ao Estado, mas também na regulação entre os particulares (SARLET, 2019). Pode-se imaginar nesse cenário, por exemplo, o Direito à Proteção de Dados da população frente às empresas de coleta e tratamento de dados pessoais.

A concepção do aspecto subjetivo dos direitos fundamentais é anterior à concepção do aspecto objetivo (MARTINS, 2019). Enquanto inicialmente os direitos fundamentais subjetivos representavam a sua exigibilidade frente ao Estado, estando relacionado ao movimento liberal e a primeira geração de direitos fundamentais, atualmente superou-se essa concepção, sendo inclusive anacrônica a utilização do termo *direitos subjetivos públicos*, antes designado para tratar o tema (SARLET, 2019).

Atualmente, o aspecto subjetivo compreende os direitos fundamentais em sentido amplo, regulando a relação entre o titular, o objeto e o destinatário do direito. Nesse sentido, Sarlet (2019) adiciona que estariam abrangidos por esse aspecto:

> (a) o espaço de liberdade da pessoa individual não se encontra garantido de maneira uniforme; (b) a existência de inequívocas distinções no que tange ao grau de exigibilidade dos direitos individualmente considerados, de modo especial, considerando-se os direitos a prestações sociais materiais; (c) os direitos fundamentais constituem posições jurídicas complexas, no sentido de poderem conter direitos, liberdades, pretensões e poderes da mais diversa natureza e até mesmo pelo fato de poderem dirigir-se contra diferentes destinatários (SARLET, 2019, p. 444).

Noutro giro, a dimensão objetiva dos direitos fundamentais é representada pelas normas que a preveem, mas não se restringem a mera codificação, formando os princípios mais importantes do direito, influenciando todo o ordenamento jurídico e servindo de parâmetro para as normas infraconstitucionais. (SARLET, 2019). Essa dimensão possui três funções relevantes, quais sejam: a eficácia/efeito irradiante, a constitucionalização do direito e sua aplicação na esfera privada e por fim o dever geral de efetivação do direito por parte do Estado (SARLET, 2020). Cabe mencionar que a efetivação desses direitos pelo Estado compreende ainda a proteção preventiva.

A esfera objetiva ainda está diretamente ligada a valores básicos para ditar ações positivas do Estado nos três poderes, fornecendo diretrizes para os órgãos legislativos, judiciários e executivos e não ligada somente com o direito particular de um indivíduo. A efetivação dos direitos pode ser realizada de diversas formas, entre elas a criminalização de condutas, a determinação do dever de indenização, a punição em atos administrativos e a atuação concreta do poder público, entre outros (DONEDA *et al*., 2021).

Ingo Sarlet trata especificamente sobre a dupla dimensão em relação ao Direito Fundamental à Proteção de Dados. Nesse sentido ele esclarece que a dimensão subjetiva envolve as disposições que envolvam a coleta, armazenamento, tratamento, utilização e transmissão de dados pessoais. Tal dimensão ainda abrange o direito do titular ao acesso e ao conhecimento sobre seus dados, ao tratamento, a utilização e ao não compartilhamento de seus dados, com ninguém, além daquele para quem deu seu consentimento. O titular tem também o direito de saber quem realiza o tratamento dos seus dados, para quais finalidades são coletados e por fim, tem ele o direito à retificação ou mesmo exclusão dos dados armazenados (SARLET, 2020).

Alguns apontamentos realizados por Sarlet (2020) acerca do tema acabaram ficando desatualizados, em decorrência da promulgação da Emenda Constitucional n. 115 em 2022. O autor lecionava que, embora os direitos do titular dos dados não possuíssem previsão constitucional, era possível extrair da LGPD, nos seus artigos 17 e 18, alguns direitos de ordem subjetiva. No primeiro artigo, atribui-se a toda pessoa natural a titularidade sobre seus dados, garantindo-lhe, ainda, o direito à liberdade, à intimidade e à privacidade. No artigo 18, a LGPD

garante ao titular dos dados o direito de obter informações sobre seus dados e sobre seu tratamento do agente controlador, não ficando limitada a esses artigos, uma vez não possui caráter taxativo (DONEDA *et al*., 2021).

2.3 A regulamentação da proteção de dados no Brasil

Conforme já mencionado no tópico anterior, atualmente, o Direito à Proteção de Dados encontra assento na Constituição Federal, no art. 5º, LXXIX, inserido pela Emenda n. 115/2022. A recente constitucionalização da matéria, revela como o Direito à Proteção de Dados é recente no nosso ordenamento jurídico. De fato, esse é um novel direito que surge em razão das mudanças tecnológicas ocorridas na sociedade, conforme já comentado. A sua construção veio sendo feita inicialmente pela doutrina e pelos pesquisadores, até que em 2018 o legislador brasileiro aprovou a Lei Geral de Proteção de Dados, marco desse direito. Momento relevante nesse contexto foi também a decisão histórica do Supremo Tribunal Federal na ADI 6388, conforme se demonstrará a seguir.

A Doutrina Clássica Constitucional classificava o Direito à Proteção de Dados, antes da Emenda Constitucional n. 115, em regra, como um Direito Fundamental Implícito. Isso acabava colocando-o em uma posição de menor atenção, relegado à sombra do Direito à privacidade. Autores como Tavares (2020) revelam que o Direito à privacidade no Brasil é adotado de forma ampla, abarcando diversos outros Direitos, como a intimidade e a personalidade da pessoa humana.

Observa-se que, a maioria dos autores constitucionalistas ainda não tinha introduzido a separação dos Direitos acima referidos, antes da inclusão do Direito à Proteção de Dados no rol de direitos fundamentais do art. 5° da Constituição. Entretanto, essa divisão dos direitos já era encontrada em algumas obras, que já antecipavam a recente mudança constitucional dada à matéria. A obra de Ingo Sarlet, de 2019, já trazia em separados tais Direitos. O autor decidiu tratar do assunto na época, baseado no art. 5.º, XII da CF/88, que garante o sigilo à comunicação dos dados, desse modo garantia um status de Direito Constitucional Implícito ao Direito à Proteção de Dados, semelhante ao direito à privacidade.

Sobre o assunto, Bioni (2019) divergia, explicando que devido a importância que os dados pessoais têm atualmente, eles estariam mais ligados aos Direitos da Personalidade. É importante falar que a personalidade aqui tratada não se refere a personalidade jurídica, mas aquela de formação do sujeito enquanto indivíduo.

Assim, o Direito à Proteção de Dados derivaria não especificamente do Direito à privacidade, mas surgiria como uma resposta às normas ou atos de alguns Estados e, posteriormente, companhias privadas, coletoras de dados da população, mais relacionado, assim, ao direito à autodeterminação, derivado do Direito a Personalidade, surgido antes mesmo da internet e das mais recentes preocupações com a coleta e a utilização de informações pessoais. A divergência sobre o fundamento do Direito à Proteção de Dados pode ser melhor entendida, caso observe-se a sua história.

O Direito à Proteção de Dados teve desenvolvimento lento. Inicialmente pode-se citar o caso *Olmstead v. United States*, de 1928, da jurisprudência norte-americana. No caso que tratava sobre buscas não autorizadas e utilização de grampo telefônico, discutiu-se a necessidade de atualização da quarta emenda da Constituição Americana para que as novas realidades tecnológicas fossem por ela alcançadas. Apesar disso, o entendimento de que a quarta emenda deveria ser aplicada também para ameaças tecnológicas, ficando reconhecida a proteção constitucional para o conteúdo de telefones e celulares, só ocorreu em 1967 com o julgamento de *Carpenter v. United States* (DONEDA *et al*., 2021).

Nas décadas seguintes foi possível observar uma maior preocupação com a tecnologia e sobretudo com o que tais inovações poderiam significar para a privacidade da população. Uma dessas inovações foi o aumento na capacidade de processamento de dados, o chamado *big data*, que gerou o aumento da valorização dos dados pessoais e suas aplicações no mercado. Nos anos 1970 diversas foram as leis criadas nos países da União Europeia que passaram a regular essa área do direito. A começar pela Alemanha, países como Suécia, França e Espanha também criaram normas sobre esse tema.

Mostra-se importante trazer à discussão gerada pelo caso do censo alemão realizado em 1983 (*Volkszählungsurteil*). Tal pesquisa censitária trazia perguntas de cunho pessoal e até íntimo, que estariam à disposição do governo, sem informar quem teria acesso a essas informações, para o que elas poderiam ser utilizadas ou por quanto tempo ficariam disponíveis. A memória, ainda recente, dos horrores cometidos na segunda guerra mundial acabou por gerar temor na população, que se insurgiu com a disponibilização de informações a seu respeito. A situação foi parar na Corte Constitucional Federal Alemã, através de Ação ajuizada por associações civis, na qual restou reconhecido o "Direito Fundamental à autodeterminação informativa". Foi determinada a suspensão do censo e a realização de um novo recenseamento com novas regras, além de garantir-se proteção das informações já concedidas, além da proibição da transmissão irrestrita das mesmas aos diversos órgãos do governo (MENKE, 2015).

A Corte Alemã cooperou com a construção de diretrizes para a afirmação do Direito à Proteção de Dados, em diversas outras decisões importantes. Em 2008, também na Corte Constitucional Federal Alemã, reconheceu-se como Direito Fundamental a "garantia da confidencialidade e da integridade dos sistemas técnicos-informacionais". Segundo Menke (2015), este seria um desdobramento do Direito à autodeterminação informativa. O reconhecimento veio através de uma reclamação constitucional que se insurgia contra a possibilidade do acesso remoto de computadores de cidadãos que tivessem sendo investigados.

A proteção de dados na Europa é regulada por diversos dispositivos, desde os anos 1950, possuindo ainda ampla jurisprudência sobre o assunto. Nesse sentido, o direito à privacidade em sentido amplo estava garantido na Convenção Europeia de Direitos, enquanto a Carta de Direitos Fundamentais da União Europeia, traz de forma mais pormenorizada esse direito em seu artigo 8º. Tal artigo garante a proteção de dados pessoais, fixando que:

> "1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito; 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação; 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente." (União europeia, 2000)

A preocupação europeia sobre a proteção de dados culminou com a promulgação da *General Data Protection Regulation* (GDPR). Esse foi o estopim para diversos outros Países criassem normas sobre proteção de dados, incluindo a Lei Geral de Proteção de Dados brasileira, que possui muitas similaridades com aquela. A criação de legislação específica sobre o assunto, em todo o mundo, mostra a relevância do tema, assim como a crescente preocupação sobre o mesmo. Entretanto, pode-se afirmar que a preocupação com a Proteção dos Dados no Brasil tem existência anterior, como pode ser observado em diversas normas esparsas, que de alguma forma trataram sobre o tema: o Código de Proteção do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação e o Marco Civil da Internet. Gonçalves (2019) relata que na década de 1990 o Judiciário Brasileiro já mostrava preocupação com a coleta indiscriminada de dados.

A LGPD é a primeira norma brasileira a tratar especificamente sobre a proteção de dados, entretanto, pode-se afirmar que a preocupação com a Proteção dos Dados no Brasil tem existência anterior. Isso pode ser observado em diversas normas esparsas, que de alguma forma trataram sobre o tema: o Código de Proteção do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, a Lei Carolina Dieckmann e o Marco Civil da Internet.

Enquanto o Código do Consumidor foi responsável por regular em seu art. 43 o tratamento do banco de dados dos consumidores, a Lei do Cadastro Positivo foi criada visando a formação de um banco de dados, de modo a facilitar a tomada de crédito a partir da análise dos dados socioeconômicos do indivíduo ou pessoa jurídica, introduzindo a necessidade de consentimento para o compartilhamento de dados e a possibilidade de responsabilidade civil, no caso de vazamento de dados. Em 2012, em face do vazamento de fotos íntimas da atriz Carolina Dieckmann, criou-se uma lei, visando proteger informações e mídias de natureza sensível, através da criminalização de condutas relacionadas à invasão de dispositivos (ANDRÉA; ARQUITE; CAMARGO, 2020).

O Marco Civil da Internet, criado pela Lei 12.965/2014 foi criado visando a regulação das relações na internet. Nessa norma, deu-se destaque para a liberdade de expressão, a privacidade e a neutralidade da rede. Destacam-se, nessa Lei em seu artigo 3°, o direito à proteção dos dados pessoais. Fica clara a importância da norma para o desenvolvimento da regulação ao Direito à Proteção de Dados. A norma, entretanto, não tratava corretamente sobre o consentimento, que ficou estabelecido como mera ficção jurídica (COSTA, 2018).

A jurisprudência pátria também já discute há algum tempo a proteção de dados. Gonçalves (2019) relata que na década de 1990 o Judiciário Brasileiro já mostrava preocupação com a coleta indiscriminada de dados. Mais recentemente, o STF decidiu sobre temas relacionados à proteção de dados, proferindo decisões que em regra iam contra o Direito à Proteção de Dados. Nesse sentido, cabe ressaltar o HC n. 91867/PA, de relatoria do Min. Gilmar Mendes, de 2012, no qual tratava sobre a licitude de uma prisão, que teve como fundamento para sua decretação os registros telefônicos do réu. Nesse caso foi decidido pelo não reconhecimento de inviolabilidade sobre dados armazenados nos aparelhos eletrônicos. A referida tese reconhecia a existência de um direito ao sigilo das comunicações, mas não dos dados em si, como pode ser observado abaixo:

> [...] Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. **A proteção constitucional é da comunicação de dados e não dos dados** [...] (BRASIL, 2012)

Reconhecida a devida importância da referida decisão, que fora utilizada inclusive como fundamento em outros julgados, cabe registrar que a mesma parece ter sido superada tanto pela legislação, quanto pela própria jurisprudência da Suprema Corte. Em maio de 2020 o Supremo Tribunal Federal proferiu decisão histórica na qual restou entendido a existência do direito fundamental autônomo à proteção de dados. O caso tratava sobre a constitucionalidade

da Medida Provisória n. 954/2020, que determinava o compartilhamento de dados pelas empresas de telefonia com o instituto IBGE, para produção estatística durante a pandemia de COVID-19 (BRASIL, 2020f).

O caso da referida ação se assemelhava ao precedente histórico alemão, sendo que a maior diferença foi o fato da decisão brasileira tratar sobre a utilização de dados obtidos através de ferramentas tecnológicas. A Medida Provisória n. 954/2020 previa o compartilhamento dos dados coletados pelas empresas de telefonia (nome, endereço e número de telefone de todos os cidadãos brasileiros, usuários dos serviços de telefonia fixa e móvel), com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE (BRASIL, 2020h). A referida Medida falhava em seguir as diretrizes fixadas na LGPD, não sendo clara quanto à finalidade do compartilhamento dos dados, tampouco quanto ao tempo que esses dados ficariam sob a tutela do Estado, além de não demonstrar a capacidade de proteger tais dados.

A decisão foi quase unânime com dez votos a favor da declaração de inconstitucionalidade da MP n. 954/2020, contando apenas com um voto contra, proferido pelo Ministro Marco Aurélio. Foi confirmada a suspensão da eficácia da medida provisória em medida cautelar concedida pela Ministra Rosa Weber, relatora das Ações Diretas de Inconstitucionalidade n. 6.387, 6.388, 6.389, 6.390 e 6.393 que versavam sobre esse assunto.

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. **1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.** 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. **Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de**

> **avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades**. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. **Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel**. 11. Medida cautelar referendada [grifo nosso] (BRASIL, 2020k)

Em 10 de fevereiro de 2022 foi promulgada a emenda constitucional n. 115, garantindo o status de direito fundamental explícito ao Direito à Proteção de Dados, ao incluir o inciso LXXIX ao artigo 5° da Constituição, que garante o Direito à Proteção de Dados, inclusive nos meios digitais (BRASIL, 2022a). A emenda ainda determinou a competência da União para legislar sobre matéria de proteção e tratamento de dados e o dever de organizar e fiscalizar a proteção e o tratamento de dados.

Os direitos fundamentais estão presentes, na Constituição Federal, em sua maioria dentro de um catálogo, disposto no art. 5º da Constituição/88. Apesar da existência desse catálogo, a Constituição permitiu a existência de outros direitos para além daqueles dispostos no artigo 5º, através da cláusula de abertura, denominação dada ao § 2º desse mesmo dispositivo (SARLET; MARINONI; MITIDIERO, 2017). Nesse sentido, o Direito à Proteção de Dados poderia ser considerado um direito fundamental implícito caso a emenda constitucional 115 não tivesse sido aprovada, dotado de igual proteção.

3. COLETA E ARMAZENAMENTO DE DADOS DURANTE A PANDEMIA

O desenvolvimento da tecnologia, voltado ao tratamento de dados, levou à criação de diversas inovações tecnológicas, que foram sendo incorporadas no dia a dia das pessoas e possuem um papel relevante na atualidade. Essas inovações passaram a ser aplicadas em diversas áreas, entre elas a medicina, ganhando ainda mais relevo e importância no contexto da pandemia, no qual foi necessário a realização do isolamento social. A utilização de ferramentas tecnológicas, envolvendo o tratamento de dados, na área médica, em regra traz consigo a necessidade do tratamento de dados sensíveis, que exigem um maior cuidado. No presente capítulo buscar-se-á revelar o significado de dados sensíveis e explicitar as principais formas de tratamento desses dados no contexto da medicina no contexto da Pandemia de COVID-19.

3.1 A utilização de dados pessoais na pandemia: os dados sensíveis

As constantes inovações tecnológicas exigiram que a lei de regulamentação de dados tivesse grande base principiológica, de forma a abarcar as mais diversas situações surgidas a cada instante. Segundo Pinheiro (2019) os princípios que norteiam a matéria seriam: A boa-fé, a finalidade do tratamento, a compatibilidade do tratamento com as finalidades informadas ao titular; a garantia aos titulares de consulta facilitada e gratuita sobre a forma do tratamento; a transparência aos titulares; a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais, a prestação de contas, pelo agente, e a adoção de medidas capazes de comprovar a proteção de dados pessoais.

Os princípios acima mencionados são usados no tratamento de dados pessoais. Porém, alguns desses dados podem precisar de proteção mais específica, tendo em vista o maior potencial lesivo ao seu titular. Denominados de dados sensíveis, estão muito relacionados ao Direito à dignidade humana, em especial as suas manifestações da privacidade, identidade pessoal e vedação de discriminação (KONDER, 2019; WERMUTH; CARDIN; MAZARO, 2022). A maior proteção ocorre por meio de regras mais rígidas sobre o consentimento, através da ampliação das medidas a serem tomadas pelos agentes de dados, previstas em lei e pelo aumento do controle da autoridade administrativa sobre o tratamento de dados (KORKMAZ, 2019).

Os dados pessoais seriam informações mais gerais como: nome, gênero, modelo do celular (MARTINS, 2019), enquanto os dados sensíveis são aqueles de caráter mais íntimo, podendo citar como exemplo: convicção religiosa, informações de saúde, etc, vide os dispostos

no art. 5°, II da LGPD. Tais dados trazem maior vulnerabilidade aos seus titulares, em face do potencial uso discriminatório que podem ter, representando verdadeiro risco ao direito da dignidade da pessoa humana, em especial aquelas pertencentes aos grupos minoritários (BIONI, 2020, p.119).

É possível ver a influência do Regulamento Geral de Proteção de Dados – GDPR (que regula a matéria na União Europeia) na legislação brasileira no que se refere à proteção dos dados sensíveis, uma vez que as duas definem similarmente o tópico:

> Ambas os regulamentos possuem a mesma definição, considerando como sensíveis dados sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (MARTINS, 2019, p. 635)

Tal rol é apenas exemplificativo, não excluindo a possibilidade de outros dados com o potencial discriminatório poderem ser considerados sensíveis. Citam-se como exemplos de dados que não estão dispostos no rol do art. 5º, II, mas que podem ser considerados sensíveis: a) Dados da localização geográfica, b) hábitos de compra, c) histórico de pesquisa, entre outros. Esses dados, em contextos distintos, podem gerar grande prejuízo para seus titulares, por isso a lei estabelece outras regras para sua proteção, visando evitar a discriminação (KONDER, 2019; MULHOLLAND, 2018). As diferenças entre o tratamento concedido aos dados pessoais e aos dados pessoais sensíveis podem ser observadas na Seção II, do capítulo 2 da LGPD, entre os art. 11 a 13.

Cabe fazer menção ao fato de que nem todos os dados sensíveis são pessoais (KONDER, 2019). Isso ocorre através de técnicas utilizadas para excluir critérios de identificação do titular dos dados, conforme já mencionado no tópico inicial do presente trabalho. Para tanto, se faz necessária a exclusão não só das informações que ativamente identificam o usuário, mas também as chamadas pegadas/rastros eletrônicos, sendo esses últimos também considerados como informações pessoais. Técnicas como essa ajudam a proteger os titulares dos dados, apesar de sozinhas muitas vezes não serem suficientes para proteção de dados.

A necessidade do consentimento em relação ao tratamento de dados de saúde se mostra fundamental, visto o grau de sensibilidade das informações desses dados, nessas situações, como já registrado anteriormente (BRASIL, 2018). Existiriam, entretanto, algumas situações em que o consentimento poderia ser relativizado, como nas situações relacionadas: "ao cumprimento de obrigações legais por parte do controlador, à garantia da segurança do titular, a prevenção à fraude, a execução de políticas públicas, a proteção da vida/incolumidade

física, assim como a tutela da saúde" (PINHEIRO, 2018, p. 52). Seria necessário apenas que os usuários fossem informados pelos controladores acerca do uso que os seus dados estariam tendo, nesses casos.

As consequências da utilização de dados pessoais durante a pandemia, por alguns governos, já se mostraram desastrosas. Em alguns países houve a retenção de dados para além daqueles que se referiam a saúde e o bem-estar populacional, sendo tais informações compartilhadas com a polícia (IENCA; VAYENA, 2020). Outra consequência possível é a discriminação de alguns indivíduos, com base nas informações recolhidas. O governo Sul Coreano realizou o compartilhamento de informações pessoais e sensíveis de algumas pessoas infectadas, sem autorização das mesmas, a fim de informar possíveis exposições de pessoas ao vírus. Tais informações incluíam: perfil demográfico, local de trabalho, por onde a pessoa andou e com quem aquela pessoa tinha ligações sociais, levando ao reconhecimento de quem seriam esses indivíduos pelos seus pares (BROUGH; MARTIN, 2020).

Surgem, no cenário da pandemia, legislações sobre o tema, como a Lei Federal 13.979/2020, conhecida como a "Lei da Quarentena" que determina as possibilidades de atuação do Ministério da Saúde para a contenção da pandemia (BRASIL, 2020c). O Brasil aprovou ainda o Decreto 10.212/2020, derivado do Regulamento Sanitário Internacional criado pela Organização Mundial da Saúde (OMS), que entre outras medidas, visava garantir os direitos fundamentais dos indivíduos. Sobre esse regulamento, Bioni *et al*. (2020) esclarece:

> Tal Regulamento dedica especial atenção à proteção de dados pessoais. Seu artigo 45 dispõe que as informações de saúde devem ser mantidas em sigilo e processadas anonimamente, mediante balizas de leis nacionais. Seu Parágrafo 1º prevê que os Estados podem tratar dados pessoais "quando isso for essencial para os fins de avaliação e manejo de um risco para a saúde pública", garantindo que os dados pessoais sejam (i) processados de modo justo e legal, e sem outros processamentos desnecessários e incompatíveis com tal propósito, (ii) adequados, relevantes e não excessivos em relação a esse propósito, (iii) acurados e, quando necessário, mantidos atualizados, garantindo-se que todas as medidas razoáveis serão tomadas para garantir que dados imprecisos ou incompletos sejam apagados ou retificados; e (iv) conservados apenas pelo tempo necessário. (BIONI *et al*., 2020, p. 12)

O Regulamento determina ainda que deve haver o compartilhamento de informações de pessoas infectadas (BRASIL, 2020b). Cabe mencionar que apesar de se reconhecer a importância de normas autorizadas do compartilhamento de dados durante crises sanitárias, também não se pode esquecer a insegurança jurídica que tais normas podem gerar para a população, ao não estabelecer os limites para a utilização e compartilhamento de dados, como foi o caso do Decreto 10.212/2020. Destaca-se que o compartilhamento de informações entre órgãos públicos muito já ocorreu, apesar da legislação atual determinar que os dados colhidos deverão ter apenas o uso informado, não devendo ser compartilhados, a menos que

haja expressa previsão para tanto (BRASIL, 2018). A crescente quantidade de informações que o governo possui, pode ser um problema, caso não usada corretamente, adiciona-se a isso que:

> Hoje, o Poder Público é considerado o maior detentor de dados e informações dos cidadãos. São dados provenientes de controles de acesso aos órgãos e departamentos públicos, câmeras em rodovias e vias de circulação, uso da biometria e de reconhecimento facial para identificação, bases de dados cadastrais como a do Sistema Único de Saúde (SUS), dos Censos Demográficos e Educacionais, de Programas de Assistência Social, como Bolsa Família, entre outros (GONÇALVES, 2019, p. 41-42).

3.2 Os contornos da saúde eletrônica e seus principais usos

3.2.1 Prontuários Eletrônicos do Paciente (PEP)

A coleta de dados dos pacientes pode ocorrer de diversas formas, dentre elas, uma das principais a ser mencionada é o prontuário, que remonta há milhares de anos, sendo recomendados desde o séc. 5 AC. para indicar o curso da doença e apontar suas possíveis causas (GÓES; MARUCO; DA SILVA, 2021). Até o século XIX se mostravam bastante precários, mas com a transferência dos cuidados dos enfermos dos religiosos para os médicos, cada vez ganharam importância, tornando os registros mais rigorosos (PATRÍCIO *et al*, 2011).

Como era de se esperar, esse instrumento passou por diversas modificações ao longo do tempo, sendo que uma das primeiras novidades tecnológicas adotadas pela medicina, nesse aspecto, foram os prontuários eletrônicos dos pacientes (PEP), que na década de 1970, passaram a ser implementados e incentivados nos Estados Unidos, e mais utilizados a partir dos anos 1990 no Brasil (PATRÍCIO *et al*, 2011).

O PEP surge inicialmente não só como mera consequência da informatização, mas de um esforço de troca de informações entre agentes do setor da saúde, da necessidade de padronização das informações coletadas por eles e principalmente na busca pela melhoria do atendimento ao paciente (PATRÍCIO *et al*, 2011). Atualmente o documento é de realização obrigatória pelos médicos, vide a Resolução CFM nº 1.638/2002.

A implementação do PEP trouxe várias vantagens, entre elas estão: melhor integração entre a equipe de saúde, maior autonomia dos profissionais de saúde e ampliação da corresponsabilização no cuidado dos pacientes. Os prontuários eletrônicos permitem ainda que os documentos sejam acessados mais facilmente por outros médicos, em situação e tempo distintos, reduzindo a duplicidade de exames, além de evitarem desgastes e perda dos documentos (PATRÍCIO *et al*, 2011; TOLEDO, 2021).

Estudos também demonstraram pontos em que os PEPs ainda precisam de melhorias, entre elas: a capacitação dos profissionais de saúde para utilização plena dos prontuários, tendo em vista que frequentemente são subutilizados. Outro entrave ocorre em face da necessidade de grande investimento financeiro para a sua utilização (XAVIER *et al*, 2021).

Os PEPs junto a outras informações de saúde podem ser compilados em um repositório de informações e compartilhados entre profissionais de saúde e instituições. São os chamados Registros Eletrônicos de Saúde – RES (ISO, 2012). As informações do RES podem ser organizadas de duas principais formas. Na primeira, a estrutura é feita a partir de um único prontuário para cada paciente, enquanto na segunda é criada uma estrutura que aceita vários prontuários para um único paciente, os reunindo em um sistema comum. Esses dois modelos são utilizados em países como os Estados Unidos e Australia.

No Brasil, os PEP passaram a ser desenvolvidos na década de 1990. Em 1999 o Ministério da Saúde propôs um modelo contendo as informações mínimas que esse documento deve conter, visando a integração de vários sistemas (TOLEDO et al., 2021). Após a promulgação da Constituição Federal de 1988 do Brasil, foi criado o Sistema Único de Saúde (BRASIL, 1988) que, lentamente, vem incorporando a utilização dos PEPs. Destaca-se na incorporação dessa e outras tecnologias o papel do Departamento de Informática do SUS, Secretaria do Ministério da Saúde, voltada para os avanços tecnológicos no SUS.

Atualmente, tanto a esfera da saúde pública, como da saúde suplementar atuam de forma semelhante no que se refere ao armazenamento de dados dos pacientes, com a utilização de diferentes sistemas de informação para tratamento de dados (DALLARI; MONACO, 2021). Na saúde suplementar, cada agente de saúde pode escolher um sistema de informação para utilizar, enquanto o SUS utiliza sistemas criados pelo Estado ou contratados por ele. Coelho Neto e Chioro (2021) revelam a existência de pelo menos 54 sistemas de base nacional atualmente. Além disso, cada ente governamental utiliza um sistema diferente, essa divisão pode ser observada pela utilização de diferentes sistemas de informação na saúde de atenção básica, sendo utilizados o SISAB e do e-SUS APS, além de sistemas que visam a integração nacional desses dados.

Vale destacar que atualmente se encontra em fase de desenvolvimento e implementação pelo Ministério da Saúde a criação de um único sistema que pretende reunir as informações colhidas pela rede pública e pela rede suplementar (Brasil, 2020g). A Estratégia de Desenvolvimento em Saúde para o Brasil 2020-2028 (ESD28) foi criada para substituir o plano de desenvolvimento de 2016 a 2019. Sendo parcialmente reestruturado com a chegada da pandemia (DALLARI; MONACO, 2021; BRASIL, 2022b).

Estabelecido pelo decreto 1.434, de 28 de maio de 2020, o ESD28 prevê entre outras coisas a instituição do Programa Conecte SUS, que tem como metas a informatização da atenção à saúde, além da "integração dos estabelecimentos de saúde públicos e privados e dos órgãos de gestão em saúde dos entes federativos, para garantir o acesso à informação em saúde necessário à continuidade do cuidado do cidadão" (BRASIL, 2020i).

O programa Conecte SUS também prevê a criação da Rede Nacional de Dados em Saúde - RNSD (BRASIL, 2020i). A RNDS é descrita como uma plataforma que irá permitir a interoperabilidade entre os órgãos públicos e privados de saúde, garantindo o acesso das informações de saúde dos pacientes a qualquer momento que se mostre necessário (BRASIL, 2020g). A RNDS consiste em um Registro Eletrônico em Saúde (RES), que pode conter o registro de um ou mais indivíduos, nesse caso, conterá o registro da população brasileira.

A plataforma permitiria o acesso mais fácil dos dados dos pacientes, que estariam disponíveis para os profissionais, em qualquer lugar, com acesso à internet, visando garantir o melhor tratamento possível ao paciente e evitando, ainda, a repetição de exames. As inovações no sistema de saúde mostram-se importantes para lidar com endemias, por fornecer um sistema mais fácil de comunicação de doenças de notificação obrigatória, tal qual o utilizado para notificação de COVID-19 (NUNES; MA; FILHO, 2021).

A RNDS prevê a utilização de tecnologias como *blockchain*, que em teoria garante um grau de segurança maior. O *blockchain* é formado por uma cadeia de informações, adicionando-se um novo "bloco de informações" a cada nova transação. Nesse sentido, cada PEP representaria um novo bloco a ser inserido em uma cadeia de informações. Essas transações são criptografadas e verificados por outros computadores conectados a rede, somente após a verificação dos outros computadores a nova transação é adicionada. Como os blocos estão conectados não é possível alterá-los, o que torna tal sistema mais confiável e seguro. (NUNES; MA; FILHO, 2021).

O sistema de *blockchain* ainda pode ser personalizado para permitir que os usuários podem utilizá-lo (NUNES; MA; FILHO, 2021). Porém, a utilização de sistemas descentralizados apresenta muitas dificuldades. Nesse sentido, a Autoridade de Dados da União Europeia implementou mecanismos de certificação, para proteção dos dados confidenciais e dados sensíveis (CAMARA *et al*., 2021).

A RNDS também prevê a criação de certificação digital para o acesso aos PEPs e RES, tal qual a realizada na Europa, visando evitar o acesso de agentes de saúde não ligados ao tratamento do paciente, além de impedir o acesso de pessoas desautorizadas aos documentos, protegendo, até mesmo das tentativas de ataques cibernéticos. Os certificados ou chaves podem

ser emitidos pelo sistema de Chaves Públicas Brasileiras (ICP-Brasil) ou outros padrões reconhecidos. Além disso há a necessidade de treinamento dos profissionais da saúde para a utilização das plataformas, de forma a evitar erros humanos e também como lidar com falhas no sistema. Isso tudo deve ser aliado a outras práticas como o monitoramento constante e atualização de práticas para garantir a segurança, como a realização de duplo *back-up* e restrições de acesso (DALLARI; MONACO, 2021).

O sistema *blockchain* não é isento de críticas, uma vez que a impossibilidade de alterar dados também pode criar problemas, como a impossibilidade de retificação de informações e a impossibilidade do titular de excluir informações, direito previsto na LGPD (CAMARA *et al*, 2021). Autores como CAMARA *et al*., (2021) e Nunes; Ma e Filho (2021) indicam a possibilidade de sistemas diferentes, não isentos de crítica, não podendo-se falar no momento de um sistema sem falhas a ser adotado.

3.2.2 Telemedicina

A utilização de ferramentas eletrônicas na área da saúde no Brasil ocorre desde os anos 1980 (MARTINS; TELLES, 2021), ganhando muito destaque com a chegada da pandemia de COVID-19, como tentativa de evitar o rápido alastramento da doença. Uma ferramenta que passou a ser bastante usada foi a da telessaúde/e-saúde, que se tornou muito popular. A telessaúde pode ser definida como:

> Telessaúde é o termo usado em atividades, serviços e sistemas de saúde realizados à distância, por meio de tecnologias da informação e da comunicação, visando a promoção de saúde, controle de doenças e tratamento de saúde, bem como educação, tratamento e pesquisa na área da saúde[1] (WHO, 1997, p. 10) [tradução livre]

Uma das principais atividades da telessaúde hoje é a telemedicina. A telemedicina é definida pelo art. 3º da Lei nº 13.989 como: "o exercício da medicina mediado por tecnologias para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção de saúde" (BRASIL, 2020d). Similarmente, a Organização Mundial da Saúde define essa prática como: "O atendimento médico realizado por profissionais da saúde, com o intermédio de telecomunicação, para o tratamento, diagnóstico e prevenção de doenças, etc". (WHO, 1997).

A medicina de forma remota já era utilizada desde o século XX, através de correspondência para o tratamento de pacientes em locais muito distantes. Posteriormente, nos

[1] Health tekmatics is a composite term for health-related activities, services and systems, carried out over a distance by means of information and communications technologies, for the purposes of global health promotion, disease control and health care, as well as education, management, and research for health

anos 70, com a popularização dos microcomputadores, a telemedicina passou a ganhar novos contornos, passando a ser intermediada agora por meios eletrônicos (SCHULMAN; CAVET, 2021).

Um dos principais documentos, sobre o assunto, é a declaração de Tel Aviv sobre responsabilidades e normas éticas na utilização da telemedicina. Realizada pela Associação Médica Mundial (WMA, 1999), referida declaração, apesar de revogada pela WMA General Assembly, Pilanesberg, South Africa, 2006, estabeleceu conceitos para termos comuns usados na telemedicina:

> 5. A habilidade médica de usar a telemedicina depende do acesso a tecnologia, variando em partes do mundo. Sem ser exaustivo, a seguinte lista descreve os usos mais comuns da telemedicina no mundo hoje.
> 1. Interação entre um médico e um paciente que está em área isolada ou sem acesso a um médico no local. Podendo ser chamada de tele assistência, sendo restrita a circunstancias bem especificas
> 2. Interação entre medico e paciente, cujas informações médicas são transmitidas eletronicamente (pressão, eletrocardiograma, etc) para o médico, para o monitoramento de sua condição. Podendo ser chamado de tele monitoramento [...]
> 3. Interação na qual o paciente procura aconselhamento medico diretamente a um médico, utilizando qualquer forma de telecomunicação, incluindo a internet. Podendo ser chamada de tele consulta
> 4. Interação entre dois médicos: um presente com o paciente e outro que é especialista [tradução livre] (WMA, 1999)

No Brasil, a telemedicina começou a ser usada na década de 1980, ganhando mais adeptos na década seguinte, quando foi regulamentada pelo CFM, através da Resolução nº 1.643/2002. Sua utilização inicial era destinada a conferências de médicos e discussão de casos (MARTINS; TELLES, 2021). Depois passou a ser utilizada, ainda, para o atendimento de pacientes em áreas remotas (MAGALHAES, 2019).

Em 2018, o CFM editou a resolução n. 2227/2018 que regulamentava especificamente a telemedicina e o tratamento de dados nessa área que, entretanto, foi logo revogada, devido às pressões da classe médica. Posteriormente, a Resolução nº 1.643/2002 e a LGPD regularam novamente o assunto (SCHULMAN, CAVET, 2021). Outros países possuem normas específicas para regular as normas de tratamento de dados relativos à saúde, como, por exemplo, os Estados Unidos que, através do *Health Insurance Portability and Accountability Act - HIPPA* (DONEDA, 2021), cuida especificamente do assunto. Existem ainda países como a Coreia do Sul, que possuem legislação específica para o gerenciamento de dados durante endemias. No caso da Coréia do Sul, o tratamento de dados de saúde durante endemias foi regulamentado antes mesmo da pandemia de COVID-19, por meio do *Contagious Disease Prevention and Control Act - CDPCA*, (PARK; CHOI; KO, 2020).

Como já mencionado anteriormente, a pandemia de COVID-19 se mostrou um fator importante para a popularização da telemedicina, que passou a ser uma opção viável para evitar a contaminação durante esse período, que exigia o distanciamento social (GÓES; MARUCO; DA SILVA, 2021). Nesse sentido, a telessaúde está presente em 75% dos hospitais particulares, incluindo a teleconsulta, telemonitoramento e teleorientação (ANAHP, 2020).

Durante a pandemia foi editada a Lei nº 13.989/2020 que trata especificamente sobre a telemedicina durante a pandemia. Cabe mencionar que apesar dessa Lei autorizar o uso da telemedicina, essa já era permitida por diversas outras normas, podendo-se mencionar a Resolução n. 1.643/2002 da CFM. Entretanto, ainda é possível vislumbrar lacunas normativas sobre a regulamentação de práticas envolvendo a telessaúde, em especial da teleconsulta, que ainda enfrenta resistência (SCHULMAN; CAVET, 2021).

Algumas das práticas relacionadas à telessaúde causam preocupação quanto à segurança dos dados dos pacientes, dentre elas, o uso do WhatsApp e ferramentas similares como meio de troca de informações entre médicos e pacientes, autorizada pelo Parecer nº 14/2017 do Conselho Federal de Medicina (CFM, 2017). Tal parecer referenda a possibilidade do uso de WhatsApp para: tirar dúvidas de pacientes e requisitar informações entre médicos, até de grupos fechados de especialistas ou do corpo clínico de uma instituição ou cátedra, entre outras utilizações. Apesar dessa orientação do CFM, deve-se mencionar que o WhatsApp não apresenta elevado grau de segurança, podendo a conta do médico ou do paciente sofrer invasões e consequentemente os dados do paciente também (GÓES; MARUCO; DA SILVA, 2021).

A telemedicina, apesar de se mostrar como ferramenta importante na facilitação do contato entre médicos e pacientes no momento da pandemia, enfrenta algumas dificuldades para seu uso: a falta de acesso de parte da população de condição socioeconômica menos favorável, notadamente a que mais precisa de assistência; a inexistência de regulamentação e padronização do serviço oferecido, o analfabetismo tecnológico de parte dos médicos e pacientes, a redução da autonomia do paciente no tratamento e a dificuldade de triagem de pacientes (CAMILO *et al*., 2021).

Além dessas dificuldades, existem, ainda, riscos relacionados à proteção de dados, intrínsecos aos meios eletrônicos utilizados para possibilitar a comunicação na telemedicina, razão pela qual deve-se manter cautela com a sua utilização (MARTINS; TELLES, 2021). Schulman e Cavet (2021) listam algumas situações onde foi possível observar a falha na proteção de dados de saúde:

> Na Inglaterra, noticiou-se o acesso de dados de pacientes por auditores governamentais do Departamento de Saúde e Serviços Humanos da Inglaterra, por laptops, enquanto estavam sentados em estacionamentos de hospitais (TAITSMAN,

> GRIMM, AGRAWAL, 2013), pelo uso de redes de wifi não seguras (TAITSMAN, GRIMM, AGRAWAL, 2013). Já nos Estados Unidos, foram roubados 78.8 milhões de registros de pacientes (O'FLAHERTY, 2018), com dados como nome, endereço, número do seguro social e data de nascimento. Na Alemanha, um hospital teve os dados sequestrados, causando a morte de um paciente (BBC, 2000). (SCHULMAN; CAVET, 2021, p. 882)

Outra preocupação, que surge no tratamento de informações de saúde, diz respeito aos impactos econômicos que o compartilhamento das informações pode trazer ao seu titular, vez que o uso desses dados pelas Seguradoras poderia acarretar em um tratamento seletivo/discriminatório dos usuários de planos de saúde, com base nas informações que os planos de saúde teriam acesso (SCHULMAN; CAVET, 2021; GÓES; MARUCO; DA SILVA, 2021). Nesse sentido, a Lei Geral de Proteção de Dados trouxe proibição expressa da utilização de dados para não realizar contrato com um beneficiário ou excluí-lo, conforme fixa o art. 11, par. 5º (BRASIL, 2018).

Existia ainda a preocupação de que fosse dada preferência do atendimento médico na modalidade remota pelos planos de saúde, visando cortes de gastos. Tal priorização reduziria a humanização do atendimento, podendo inclusive colocar em risco a saúde do próprio paciente (MARTINS; TELLES, 2021).

Por outro lado, a escolha do atendimento remoto como modalidade preferencial não pareceu implicar necessariamente em redução de custos para o cliente-usuário, já que o valor do plano não pode ser mudado somente em decorrência dessa preferência conforme o entendimento:

> Obrigação de fazer. Plano de saúde. Antecipação de tutela indeferida. Pretensão de redução pela metade do valor das mensalidades. Argumento de que o serviço de telemedicina, prestado devido à pandemia de COVID- 19, seria inferior ao contratado. Inadmissibilidade. Limitação da agravada quanto aos atendimentos presenciais, oferecidos apenas em caso de emergência ou urgência, em análise perfunctória, se mostra adequada, considerando a recomendação de isolamento social. Ausência de abusividade ou onerosidade excessiva. Suposta diminuição da renda familiar não demonstrada. Probabilidade do direito não configurada. Agravo desprovido.20 (SÃO PAULO, 2020)

Já foi discutida também a possibilidade de teleperícia, nesse sentido, o TRF4 foi favorável a possibilidade desta prática durante a pandemia, conforme ementa abaixo:

> EMENTA RECURSO INOMINADO. PREVIDENCIÁRIO. BENEFÍCIO POR INCAPACIDADE. AUXÍLIO-DOENÇA. PROVA TÉCNICA SIMPLIFICADA. TELEMEDICINA. TELEPERÍCIA. PANDEMIA. CORONAVÍRUS. POSSIBILIDADE. (...). 3. Apesar da vedação contida no art. 92 do Código de Ética Médica, reforçada pelo Parecer n. 03/2020 do Conselho Federal de Medicina - CFM, a Lei n. 13.989/20 autorizou o uso da telemedicina - conceito no qual se insere a teleperícia - durante a crise causada pelo coronavírus (SARS-CoV-2). 4. O Conselho Nacional de Justiça - CNJ, por meio da Resolução n. 317, de 30 de abril de 2020, determinou que "as perícias em processos judiciais que versem sobre benefícios previdenciários por incapacidade ou assistenciais serão realizadas por meio eletrônico, sem contato físico entre perito e periciando, enquanto perdurarem os

> efeitos da crise ocasionada pela pandemia do novo Coronavírus" (art. 1º). Os atos normativos infralegais do CFM ficaram superados pela Lei n. 13.989/20 e, também, pela Resolução do CNJ. 5. Recurso não provido. (BRASIL, 2020l)

3.2.3 Aplicativos de Monitoramento

A pandemia foi responsável não só pela mudança de algumas práticas, mas também pela introdução de outras, como por exemplo a utilização de aplicativos para coleta de dados de possíveis infectados e também rastreamento de possíveis novas contaminações.

O monitoramento de infectados e reconstrução de seus passos, para saber outros possíveis contaminados, durante crises de saúde pública, já acontece há muito tempo, sendo inicialmente realizado manualmente. Entretanto, com uma população muito grande e o alto nível de contágio do COVID-19, o monitoramento manual se demonstra difícil de realização (ZHAO *et al*, 2020). Atualmente, a utilização dos aplicativos se revela como uma atualização desse procedimento fundamental (SHEN; WEI; LI, 2020; WANG; LIU, 2020)

Os aplicativos de celular são capazes de realizar o rastreamento de pessoas contaminadas de maneira mais rápida, assim como das pessoas com quem manteve contato, ou simplesmente esteve próximo, uma vez que depende apenas da aproximação dos celulares para que seja realizado, necessitando de uma menor quantidade de trabalhadores para funcionar (SHEN; WEI; LI, 2020). Cita-se, por exemplo, o caso de uma pessoa que anda dentro de um ônibus que, provavelmente, não saberia informar no rastreamento manual o nome e contato dos envolvidos, sendo essa uma situação em que o monitoramento digital poderia ser mais eficiente.

Os aplicativos de celular que realizam monitoramento da pandemia de coronavírus e rastreamento de possíveis pessoas infectadas baseiam-se em 2 tipos de tecnologia. A primeira é a de geolocalização, enquanto a segunda baseia-se em tecnologia *bluetooth*, há ainda aplicativos que utilizam uma combinação das duas anteriores.

A tecnologia de geolocalização (GPS) funciona através da coleta constante das informações de GPS do celular dos usuários, funcionando como um sistema de monitoramento. Caso um dos usuários teste positivo, é possível verificar-se quem teve contato com ele, através da comparação de informação fornecida por todos os outros usuários, notificando as pessoas que lhe estiveram próximas durante o período de contágio (WANG; LIU, 2020).

Existe, nesse sistema, a possibilidade de dois tipos de modelo dentro do sistema GPS, o centralizado e o descentralizado. O centralizado seria aquele que manda as informações diretamente para quem esteve em contato com a pessoa, enquanto o descentralizado apenas

mostraria onde pessoas contaminadas estiveram, cabendo aos outros usuários observarem se estiveram ou não naquelas áreas (WANG; LIU, 2020).

O modelo descentralizado aparenta respeitar mais a privacidade do usuário, uma vez que só compartilha as informações depois de já terem sido anonimizadas e só as obtém depois de prévia autorização da pessoa, não tendo o acesso a priori de pessoas saudáveis.

Por outro lado, o modelo de rastreamento por *bluetooth* não coleta a localização dos usuários. O rastreamento ocorre da seguinte forma: primeiro os APPs distribuem tokens aleatórios e que são guardados no dispositivo dos usuários. Depois, caso os usuários se encontrem, eles automaticamente trocam informações sobre seus tokens, para guardar o contato[2]. Quando os usuários testam positivo e fornecem essa informação ao aplicativo, as pessoas que estiveram em contato com ele são notificadas, podendo ocorrer de diferentes formas, a depender do APP (ZHAO, *et al*, 2020; WANG; LIU, 2020).

Os modelos de rastreamento por *bluetooth* podem ser, assim como o rastreamento por GPS, centralizados ou descentralizados. Nos modelos centralizados os usuários mandam as informações para os servidores que analisam o risco de contaminação entre os usuários e os avisam caso exista um risco de contaminação (SHEN; WEI, LI, 2020). Já no modelo descentralizado, o usuário manda à central apenas o contato que teve com os outros usuários. A central, então, atualiza sua base de dados, que deverá ser baixada periodicamente pelos usuários, que poderão observar nos seus celulares se tiveram contato com alguém infectado.

É preciso ter em mente que no Brasil, existem pelo menos 4 APPS de monitoramento e o presente trabalho foca apenas naquele lançado pelo Ministério da Saúde chamado "Coronavírus – SUS", que foi criado com base no modelo desenvolvido pela Apple em parceria com o Google e que utiliza *bluetooth* para funcionar (JUNEIDI, 2020), utilizando uma abordagem descentralizada (ALMEIDA *et al*, 2020).

O portal do DATASUS (BRASIL, 2020j) esclarece alguns pontos sobre o funcionamento do aplicativo, entre eles que, no Brasil, apenas o Ministério da Saúde obteve licença "para usar a funcionalidade desenvolvida pelo Google e pela Apple". Revela, também, que o aplicativo consegue fazer o rastreamento de indivíduos a uma distância de 1,5 a 2 metros, devendo o tempo mínimo de contato ser de cinco minutos entre smartphones que tenham o aplicativo instalado. Por fim, fornece informações sobre a proteção de dados, afirmando que os dados são criptografados e as informações dos usuários são salvas localmente nos seus smartphone, ficando disponíveis por 14 dias.

[2] Esse encontro é chamado por muitos como handshake (aperto de mãos) e produz um "timestamp". Esse último guarda informações como: o usuário e a distância e o tempo em que estiveram juntos (ZHAO, et. al, 2020).

O aplicativo Coronavírus-SUS fornece além do *contact tracing* (rastreamento de infectados), informações importantes como sintomas da doença, informações de contagio e prevenção. Atualmente o aplicativo ainda conta com informações contra *fake News*. Essas últimas se mostraram um relevante problema para a redução da contaminação da Covid-19 no Brasil (FALCÃO; SOUZA, 2021).

Destaca-se ainda a maior participação da população com a utilização de medidas como essa, ajudando o Estado na coleta dos dados e aproximando o cidadão das discussões públicas (COELHO *et al*., 2020). Entretanto, no Brasil houve pouca utilização por parte da população, menos de 1% utilizava o *app* até 10/11/2020 (BRASIL, 2020h). O coronavírus-SUS não se mostra tão claro na divulgação de informações quanto aplicativos similares utilizados em outros países (TAGIAROLI, 2021), além de já ter reportados problemas de utilização, como a impossibilidade de anexar resultados positivos de COVID (KNOTH, 2022)

A orientação da organização mundial da saúde ainda defende o rastreamento, considerando as informações, obtidas com tal técnica, importantes para determinar se as políticas públicas estão funcionando (WHO, 2021). A utilização de aplicativos como o Coronavírus-SUS teria maior efetividade quando cerca de 60% da população os utilizassem, apesar de já ajudar na redução da pandemia com percentuais menores (HINCH, *et al*, 2020).

Não se olvida que a utilização de ferramentas como essa acabam por revelar o abismo social que a população brasileira vive, excluindo as pessoas que não tem acesso à tecnologia (COELHO *et al*., 2020). Cita-se, por exemplo, as populações ribeirinhas e nativas, que em sua maioria não teriam acesso a esse e outros recursos (NUNES, 2021; MONDARDO, 2020).

4 A LEGITIMIDADE DO TRATAMENTO DE DADOS PESSOAIS EM MATÉRIA DE SAÚDE: POSSIBILIDADE E LIMITES

O desenvolvimento tecnológico permitiu as aplicações da tecnologia acima mencionada, não sendo essas as únicas possibilidades de utilização, surgindo novas ferramentas constantemente. Diante dessa popularização, passou-se a olhar mais para as normas que regulam essas ferramentas, sua aplicação no caso concreto e quais as consequências de possíveis violações ao Direito à Proteção de Dados. Busca-se abordar as principais normas no sistema jurídico brasileiro que buscam proteger os dados relacionados à saúde

4.1 A LGPD e sua aplicação aos dados de saúde

A Lei Geral de Proteção de Dados – LGPD é atualmente a principal norma de regulação de dados no Brasil. Ela é também o instrumento que determina a forma como os dados de saúde são tratados. É preciso ter em mente que essa é uma norma geral, tratando de maneira ampla os mais diversos tipos de dados, dispondo ainda de conceitos comuns relacionados ao tema de proteção de dados.

Os conceitos básicos em conjunto com os princípios estabelecidos pela LGPD são a base para o tratamento de dados no País. A maioria das definições e conceitos afetos ao tema estão contidos na mesma, como por exemplo o conceito de dados sensíveis e dados pessoais, usados no presente trabalho. Para além do já mencionado, a Lei estabelece os principais contornos do Direito à Proteção de Dados, estabelecendo que tipo de dados são por ela regulados ou não, a quem ela irá ser aplicada, assim como as penalidades pelo seu descumprimento.

A LGPD baseia-se na necessidade do consentimento do titular, no que se refere aos seus dados, para coleta, produção, recepção, classificação, armazenamento, compartilhamento, enfim para o tratamento de dados. Esse consentimento deve ser livre e motivado, devendo, para tanto, o agente de tratamento de dados deixar claras as finalidades no trato dos dados (PINHEIRO, 2018). A importância do consentimento vem gradualmente aumentando, como explica Bioni (2019). Segundo o autor, durante a evolução do Direito à Proteção de Dados, este passou por várias fases, nas quais o elemento do consentimento se mostrou central, ganhando cada vez mais destaque a partir da emissão de dois importantes documentos pela Organização para a Cooperação e Desenvolvimento (OCDE), sendo eles: o *privacy guidelines* em 1980 e *declaration on transborder data flows* em 1985.

Não obstante seja o consentimento do titular uma categoria de máxima importância no tratamento de dados, observa-se que, paradoxalmente, é cada vez mais difícil para os indivíduos tomarem decisões sobre os seus dados de forma livre e consciente. Isso decorre da arquitetura dos sistemas de informação, que trabalham de modo a fragilizar a tomada de decisões dos titulares dos dados, que são direcionados a focar em recompensas imediatas que, aliadas à sobrecarga de decisões a serem tomadas pelos indivíduos e ao desconhecimento sobre como se proteger no ambiente tecnológico, culmina em decisões que nem sempre refletem a vontade consciente do indivíduo. Tudo isso acaba por colocar a população em geral em uma situação de hipervulnerabilidade (BIONI, 2019).

Cabe, ainda, mencionar que as abordagens atuais sobre a proteção de dados foram influenciadas pelos documentos jurídicos criados pela OCDE, o *privacy guideline* e o *declaration on transborder data flows*. Ocorre que a LGPD e a GDPR, partindo de referidas normas, acabaram por apresentar soluções para alguns dos problemas nelas detectados acerca dos obstáculos encontrados para que se desse o consentimento dos titulares de forma consciente e livre. Isso pode ser percebido através da tentativa de aumentar o controle efetivo do titular dos dados, através da garantia de acesso aos seus dados coletados, assim como a liberdade para modificá-los e eliminá-los. Nesse sentido, também se deu maior ênfase na obrigação do controlador de resguardar a proteção dos dados por ele tratados. Em vários artigos da Lei Geral de Proteção de Dados - LGPD é possível identificar a preocupação do legislador com tal matéria, merecendo destaque os art. 9º e 46, da LGPD, cuja transcrição cabe fazer:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - Finalidade específica do tratamento;
> II - Forma e duração do tratamento, observados os segredos comercial e industrial;
> III - Identificação do controlador;
> IV - Informações de contato do controlador;
> V - Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - Responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.
> [...]
> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018)

Por outro lado, os limites da proteção de dados também são influenciados pelos atores econômicos, que lucram com a venda dos dados pessoais, e a quem não interessa tanto a proteção dos dados, mas a maior liberdade no seu tratamento. Quando o titular dos dados não aceita as condições postas para utilização de serviços ou aquisição de bens, pode acabar por ter

negado o acesso aos mesmos (DONEDA, 2020). Para além disso, a lógica atual do mercado baseia o consentimento a contratos de adesão, que não são o instrumento adequado para regular essa relação, onde se tem o direito fundamental à proteção de dados a exigir um tratamento que possibilite ao titular de dados realizar escolhas que não cabem em um contrato de adesão e onde muitas vezes acontece uma verdadeira renúncia a esse direito fundamental, que não poderia ser renunciado. Tal problema pode ser observado, por exemplo, nos aplicativos de monitoramento, mencionados no capítulo dois, o aplicativo "Coronavírus – SUS" requer o consentimento do usuário através de contrato de adesão, para sua utilização, de forma que a vontade do titular de dados e por consequência o seu direito fundamental à proteção de dados acaba reduzido.

A LGPD ainda estabelece em seu art. 5°, XII, que o consentimento deve ser uma manifestação livre, informada e inequívoca a partir da qual o titular concorda com o tratamento de seus dados para determinada finalidade (BRASIL, 2018). Nessa perspectiva, o titular deve ter a sua disposição todas as informações necessárias, para fundamentar as suas escolhas, de preferência com termos simples; devendo também ter preservado o seu poder de negociação, para que o seu consentimento se dê de forma livre, contrariando os processos de tudo ou nada; além disso a finalidade do tratamento dos dados deve ser explícita, revelando a sua finalidade, de forma que a manifestação do titular seja inequívoca (DONEDA, 2020). Por fim, há ainda a necessidade da manifestação ser expressa, podendo ser realizada através de declaração por escrito ou ação positiva que autorize, além de haver uma real possibilidade de recusa, sem prejuízo ao titular do direito (GROSSI, 2020).

O consentimento será válido apenas para os dados que são de coleta necessária e para aquela finalidade mencionada ao titular, sendo nulo o consentimento quando o acordo for de cláusulas genéricas e abstratas. A análise do consentimento é de obrigação dos agentes de tratamento de dados pessoais, que devem observar os pontos acima mencionados, para saber se o consentimento foi válido.

As exigências acima mencionadas estão alinhadas com os princípios estabelecidos na própria LGPD. O princípio da finalidade, por exemplo, afirma que a determinação da finalidade dos dados coletados deve ser avisada de maneira prévia, já o princípio da necessidade, estabelece que só serão coletados o mínimo de dados possíveis, necessários para a atividade desenvolvida.

O consentimento também se mostra muito importante na esfera pública, devendo seguir as principais regras mencionadas, como pode ser visto no art. 23 da LGPD, no qual fica fixado que o tratamento de dados pelas pessoas jurídicas de direito público (dispostas no art. 1° da Lei nº 12.527) deve observar a finalidade pública, o interesse público, visando executar as

competências legais e cumprir as atribuições do serviço público. Para tanto, é necessário que sejam informadas as hipóteses que autorizam o tratamento de dados no exercício de sua competência, devendo ainda garantir informações claras e atualizadas sobre a finalidade dos procedimentos que são utilizados, de preferência em seu site. Deve ainda indicar um encarregado para ficar responsável pelo tratamento dos dados pessoais.

Entretanto, existem algumas circunstâncias que o consentimento pode ser relativizado, como pode ser visto no artigo 7°, em seu inciso II, sendo essas situações fortemente relacionadas aos dados de saúde. Isso será possível, por exemplo, nos casos de: "**proteção da vida ou da incolumidade física do titular ou de terceiros**" [grifo nosso] ou ainda na "**tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária**" [grifo nosso] (BRASIL, 2018).

A Lei dá maior permissibilidade para relativização do consentimento pelo poder público em outros incisos, além de trazer outras disposições específicas sobre o tratamento de dados pelo poder público no capítulo IV: "Do tratamento de dados pessoais pelo poder público". Nesse capítulo, fica estabelecido quais pessoas jurídicas poderiam tratar os dados pessoais de forma diferenciada. Tal disposição se aplica a: União, Estados, Distrito Federal e Municípios, vide o art. 23 da LGPD, além das empresas públicas e sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas (BRASIL, 2018).

Conforme se depreende dos artigos acima, o legislador estabeleceu uma ampla margem de atuação do poder público no tratamento de dados, especialmente quando ligados à saúde pública. Essa amplitude da atuação estatal resulta em uma limitação ao Direito Fundamental à Proteção de Dados, revelando clara colisão de direitos fundamentais, conforme se discute em seguida.

Existem ainda outras situações em que a utilização dos dados de saúde é regulada pela LGPD, entre elas destaca-se o uso de dados para a pesquisa, conforme pode ser visto no art. 11, II, c da LGPD, no qual é determinada a anonimização desses dados sempre que possível. A anonimização é um processo no qual realiza-se a exclusão ou supressão de identificadores, que possibilitem a identificação de um indivíduo (MACHADO; DONEDA, 2019). Para chegar a esse resultado, podem ser adotadas diferentes técnicas, como a supressão, a generalização, à randomização e a pseudoanonimização (BIONI, 2020).

Porém, a anonimização do titular dos dados não é um processo infalível, no sentido de que a sua reidentificação é sempre uma possibilidade. Dessa forma, o dado anonimizado é sempre um dado passível de identificação e assim, em tese seria um dado pessoal. Essa é a ideia contida no conceito expansionista dos dados. No caso de países que adotam o entendimento da

teoria expansionista, e ao lado disso fixam uma dicotomia entre dados pessoais e dados anônimos, surge a necessidade da criação de um filtro para que nem todos os dados anônimos fossem considerados pessoais, evitando-se que as normas se tornassem tautológicas. Esse filtro foi a razoabilidade, adotado pela LGPD e também pela GDPR (BIONI, 2020; MACHADO; DONEDA, 2019).

A razoabilidade refere-se nesse cenário no esforço razoável que alguém teria que dispor para encontrar a quem pertence o dado em questão (BIONI, 2020). Caso fosse facilmente possível a reidentificação, o dado, apesar de anonimizado, ainda seria considerado dado pessoal. Caso fosse demandado um esforço considerável para reidentificação, ainda que a mesma acontecesse, o dado seria considerado anônimo. O direito europeu através da Diretiva 95/46/EC estabeleceu como critérios a serem utilizados para realizar a reversão: os custos, tempo de trabalho dispendido para reidentificação, as tecnologias disponíveis no momento, os riscos de falha e o descumprimento de dever de confidencialidade.

Destaca-se a possibilidade da necessidade de não anonimização de dados para a realização de algumas pesquisas. Diante desse cenário, começou-se a cogitar algumas opções, entre elas o fortalecimento dos tratamentos de seguranças aplicados, visando a maior proteção desses dados ou a utilização da pseudoanonimização, que possibilita a reversão do processo de anonimização dos dados a partir de chaves de reidentificação (GUANAES, *et al*., 2018). Cabe-se adicionar que, em regra, os dados anonimizados não são considerados dados pessoais, enquanto os pseudo-anonimizados são, uma vez que existe a possibilidade de reversão do processo de maneira mais simples e consequentemente de identificação do titular dos dados (ALMEIDA *et al*., 2020).

4.2 A utilização da proporcionalidade na resolução de conflitos em matéria de dados de saúde.

Existem situações nas quais pode haver uma violação ao direito fundamental da proteção de dados, ainda que com observância à LGPD. Isso ocorre em situações onde o consentimento do titular é limitado de alguma forma, seja pela ausência das informações necessárias para tomada de decisão, seja pela ausência de espaço para manifestação de sua vontade (nos casos de contrato de adesão). No Brasil, durante a pandemia, conforme já mencionado em capítulos anteriores, foi feito uso de aplicativos para contenção e monitoramento da pandemia, cabendo destaque, entre eles o Coronavírus-SUS. Através desse aplicativo foram coletados dados sensíveis da população, que ao compartilhar tais dados, o fazia

através de contrato de adesão, onde o espaço negocial esteva suprimido. Não obstante a finalidade da coleta de tais dados tenha sido amplamente divulgada, cabe registro que a plataforma foi desenvolvida em parceria com empresas estrangeiras (Apple e Google), que também passaram a ter acesso a tais dados.

Nesses casos, seria possível vislumbrar a existência de verdadeiro conflito de direitos fundamentais, tendo em vista que tanto o Direito à Proteção de Dados como o Direito à Saúde são Direito Fundamentais. A colisão de direitos fundamentais é uma temática muito importante, por tratar dos direitos mais importantes e fundamentais para a sociedade, sendo assunto que a matéria constitucional muito debate, estabelecendo para tantos algumas possibilidades para a resolução desse tipo de conflito.

Cabe inicialmente fazer diferença entre normas do tipo princípio e as outras do tipo regra. As primeiras têm amplo caráter interpretativo, enquanto as segundas representam comandos a serem seguidos. Sobre o assunto Sarlet (2017) leciona que: as regras funcionam em um sistema de tudo ou nada, enquanto os princípios são mais abstratos podendo ser atingidos em diversos graus. Os princípios são mandados de otimização, o que significa que devem ser realizados na maior medida do possível (FERREIRA, BRANCO, 2021).

No presente caso, ambas as normas em foco são do tipo princípio, uma vez que são dotadas de alto grau de abstração, não prevendo de forma expressa como serão garantidos os direitos por ela elencados. Como é comum, tais direitos tiveram seus contornos definidos pelas normas infraconstitucionais, como é o caso da supramencionada Lei Geral de Proteção de Dados (LGPD), razão pela qual é perfeitamente possível que mesmo seguindo as definições estabelecidas em lei se esteja desrespeitando o direito fundamental à Proteção de Dados, ocorrendo choque entre os direitos em tela, devendo-se focar por isso no conflito entre os direitos fundamentais.

Cabe relembrar aqui as características dos direitos fundamentais, quais sejam: a historicidade, universalidade, limitabilidade, concorrência, irrenunciabilidade, inalienabilidade, imprescritibilidade. Todos os direitos fundamentais devem ser aplicados a todos, por isso absolutos, porém todos os direitos são passíveis também de limites, por isso passíveis de limitações. Cita-se como exemplo o direito fundamental à reunião que dispõe no mesmo artigo que prevê tal direito a sua limitação. Falar que o limite é constitucional e que na situação da LGPD a limitação é infraconstitucional.

As regras do tipo norma teriam como método de resolução, métodos mais objetivos, enquanto as normas do tipo princípio utilizam métodos mais subjetivos, uma vez que não há hierarquia entre normas constitucionais (BARROSO, 2020). Isso requer mais atividade

intelectual do intérprete para resolver o conflito. Conforme leciona Canotilho, os embates entre direitos fundamentais acabam muitas vezes desaguando em problemas econômicos, sociais, culturais, que não competem somente ao direito, sendo necessária uma abordagem multifocal (SARLET; MARINONI; MITIDIERO, 2017).

Um dos principais expoentes no que se refere ao estudo da colisão de direitos fundamentais é o alemão Robert Alexy. Sobre os conflitos de normas do tipo princípio, ele explica: que quando um princípio permite algo que é proibido por outro, um dos princípios terá que ceder em face do outro. Não implica, entretanto, na declaração de invalidade do princípio ou a necessidade de uma cláusula de exceção, somente significa que em face de um conflito concreto, um princípio terá preponderância sobre o outro (ALEXY, 2015).

Um dos principais pontos da teoria do autor é a que trata sobre o sopesamento, também conhecido como ponderação. O autor estabelece equações que representam situações onde direitos fundamentais entram em conflito entre si, quais sejam: **a)** P1 P P2, **b)** P2 P P1; **c)** (P1 P P2) C; **d)** (P2 P P1) C. Nessas premissas "P1 e P2" representam direitos fundamentais do tipo princípio; o "P" significa Prepondera e o "C" representa condição, que seria a ação violadora de um preceito fundamental. O autor, em seguida, elimina as situações "a" e "b", tendo em vista que nenhum princípio tem preponderância sobre o outro na presente ordem constitucional em abstrato, havendo eficácia horizontal entre si, sendo possível, apenas, haver preponderância de um princípio em relação ao outro em um caso concreto, situações previstas nas hipóteses "c" e "d".

Dessas proposições decorreria a chamada lei da colisão, sendo definida por Alexy como: "As condições sob as quais um princípio tem precedência em face de outro constituem o suporte fático de uma regra que expressa a consequência jurídica do princípio que tem precedência" (ALEXI, 2015, p. 99). Em síntese, a regra representa que sempre que uma ação for proibida por violar um direito fundamental (c), um direito fundamental deverá prevalecer em face de outo. A lei de coalisão será a regra que determina qual princípio terá validade em face do outro.

A ponderação em si deriva do princípio da proporcionalidade, se dividindo em três subprincípios: adequabilidade, necessidade e proporcionalidade em sentido estrito[3], que devem ser aplicados em etapas. Inicialmente se aplicam os princípios da adequação e da necessidade, tendo como objetivo a otimização dos direitos fundamentais em conflito, buscando aplicá-los na sua maior medida possível. Nesse momento, se deverá buscar, entre as soluções encontradas

[3] suitability, of necessity, and of proportionality in the narrow sense

para resolver os problemas, aquelas que não impliquem na exclusão completa de um dos princípios em conflito, considerando-se essas as soluções mais adequadas.

Em relação ao princípio da necessidade, deve-se procurar, entre as possíveis alternativas, aquela capaz de garantir o direito fundamental estabelecido na equação como p1 e, simultaneamente, aquela que menos interfira negativamente em relação ao direito fundamental disposto na equação como P2 e vice-versa. Por fim, se aplica o princípio da proporção em sentido estrito, que é resumido pelo autor como: "O grau máximo de descumprimento ou prejuízo a um princípio, maior a importância de satisfazer o outro"[4] (ALEXY, 2003, p. 136). Nessa fase deverão ser observadas as soluções encontradas, que devem ser valoradas, de forma que se observe qual a mais indicada ao caso concreto e em que grau ela deverá ser aplicada.

Entre os principais críticos à teoria da ponderação de Alexy, encontra-se Habermas, que defende que teoria da ponderação não utiliza de fundamentos jurídicos para resolver os conflitos, mas de fundamentos políticos e éticos. Entende com isso que a ponderação esvazia os princípios de seus valores fundamentais e os diminui a valores que guiarão as decisões, acarretando em decisões falhas. O autor respondeu às críticas de Habermas em artigo de 2003, afirmando que as conclusões elaboradas Habermas não seriam conclusões lógicas das críticas oferecidas à sua teoria, afirmando, ainda, que o método utilizado não seria subjetivo, uma vez que apresenta uma estrutura definida para chegar ao resultado da resolução de conflitos (ALEXY, 2003). Outros autores como Sieckmann fizeram críticas a partes mais específicas da técnica criada por Alexy, sugerindo a sua complementação, através da criação de conceitos e parâmetros mais definidos, como a criação de conceituação de otimização e resultado ótimo, além de sugerir a melhor delimitação dos pesos aplicados no caso (GAVIÃO FILHO; LORENZONNI, 2019).

A técnica de Alexy já foi muito utilizada pelo Supremo Tribunal Federal, como destaca Barroso (2020), mas também não é unanimidade na nossa Corte Constitucional. Barroso (2020) esclarece que atualmente utilizam-se alguns elementos para reduzir o grau de subjetividade e arbitrariedade das decisões, como: a utilização de uma norma constitucional ou legal como fundamento da decisão tomada, a elaboração de parâmetro que possa generalizado para ser usado em casos semelhantes e a preservação do núcleo essencial dos direitos em conflito.

[4] The greater the degree of non-satisfaction of, or detriment to, one principle, the greater the importance of satisfying the other.

No decorrer do presente estudo, evidenciou-se a colisão de direitos fundamentais da saúde e da proteção de dados, nos casos do uso dos aplicativos de coleta de dados que não apresentavam ferramentas para que os titulares de dados fornecessem o seu consentimento, sendo necessária a aplicação do princípio da ponderação.

Assim, o primeiro passo para aplicação da técnica da ponderação seria o uso do subprincípio da adequação, quando eliminar-se-ia a exclusão do aplicativo das plataformas ou ignorar-se-iam os problemas quanto ao fornecimento do consentimento. Em seguida, seria necessário observar as soluções conforme o subprincípio da necessidade. Aqui parece que a solução mais adequada seria fornecer técnicas adequadas para o consentimento dos titulares do direito e a retirado do aplicativo das plataformas digitais até a implementação dessa mudança. Após tais mudanças, caso o usuário e titular dos dados quisesse utilizar o aplicativo e não concordasse, por exemplo, em fornecer seus dados para a utilização em pesquisas e criação de políticas públicas, deveria ser observado o desejo do titular. Tal solução parece se adequar ainda ao princípio da proporção em sentido estrito.

A decisão estaria baseada nos princípios da LGPD, dispostos no art. 2° e em especial o art. 7°, inciso primeiro da Lei. É possível imaginar a criação de regra que excluísse os aplicativos das plataformas digitais e de sites da internet que coletem dados sensíveis que não possuem mecanismos adequados para manifestação do consentimento até que fosse regularizada a presente falha. Após tais mudanças, restaria garantido o Direito à Proteção de Dados e o consentimento livre e motivado. Ainda estariam preservados os núcleos essências dos direitos em questão, uma vez que ainda poderia ocorrer o rastreamento de infectados e sua notificação, além de monitoramento da pandemia, com a observância também do Direito à Proteção de Dados.

Cabe, entretanto, o registro de outra observação feita por Alexy (1999), sobre a força vinculante dos princípios fundamentais e de como apenas os princípios que tem procedimentos que possam ser verificados por tribunais são *justiciaveis*, enquanto aqueles que não sejam passíveis de análise, em caso de violação, ficariam reservadas ao âmbito político e moral. Não há dúvida de que os princípios têm força vinculante e de que os Tribunais Brasileiros têm o dever de julgar se houve ou não violação a um direito fundamental.

4.3 A responsabilização pela violação do direito a proteção de dados.

A modernização e introdução das novas ferramentas tecnológicas no dia a dia e em especial na área da saúde se mostram cada vez mais comuns. Como já mencionado em tópicos

anteriores, essas ferramentas podem ser utilizadas de diversas formas, seja nas modalidades remotas da telessaúde/e-saúde, como a teleconsulta, tele-assistência, teleperícia., seja pela inclusão de plataformas de dados de saúde ou de aplicativos de monitoramento, entre outras.

Apesar do grande avanço e da importância desses recursos para auxiliar no cuidado da saúde, é preciso ter em mente que com a sua utilização a população é exposta a riscos em relação aos seus dados pessoais, o que ocorre também em face do valor cada vez maior que os dados possuem na atualidade, virando potencial produto no mercado legal ou ilegal, onde podem ser utilizados para influenciar o consumo, a produção, a propaganda, é o chamado *data-driven economy* (SCHULMAN, CAVET, 2021).

Diante da demanda do mercado pelos dados pessoais, esses passaram a ser cada vez mais desejados. Em decorrência disso, os vazamentos de dados se mostram cada vez maiores e mais frequentes, conforme Machado *et al*. (2019). Em 2018 os vazamentos nos Estados Unidos chegaram a 654 bilhões de dólares e 2,4 bilhões de usuários tiveram seus dados expostos. Dentre esses, quase 20 milhões de dados divulgados foram de instituições que prestavam serviço à saúde. Além disso, *hackers* roubaram os dados de 10 mil pacientes do setor de pesquisa do Massachusetts General Hospital

O Brasil não é estranho à ocorrência de problemas na proteção de dados dos seus cidadãos. Em 2017 ocorreu o vazamento de dados do Cartão Nacional de Saúde do SUS, nos quais foram divulgados nome, endereço, além do nome dos pais de milhares de usuários do serviço. Em 2020, ataque de hackers divulgou dados de 200 milhões de pacientes (G1, 2021). Em 2021, novo ataque foi realizado contra o Ministério da Saúde, dessa vez envolvendo as informações das pessoas vacinadas, exigindo um pagamento para o resgaste das informações, que, entretanto, foram recuperadas (NAÍSA, 2021).

Leis como a GDPR e a LGPD preveem multas, como incentivos para que as empresas privadas invistam em segurança, buscando garantir maior proteção aos dados, evitando incidentes como os acima citados. Essas medidas punitivas, dispostas no art. 52, 53 e 54 da LGPD, passaram a vigorar a partir de 1º de agosto de 2021, como determina a Lei nº. 14.010/2020 (BRASIL, 2020e). Cabe mencionar que a condenação em âmbito administrativo e civil não exclui a possibilidade de condenação penal, com base na Lei 12.737/2012, tampouco excluem, em muitas situações, a necessidade do controle constitucional, no que se refere à violação do Direito à Proteção de Dados, especialmente no que tange aos direitos sensíveis.

A responsabilidade civil no que concerne à proteção de dados vai ser especial, uma vez que a LGPD estabeleceu normas mais específicas sobre o assunto. A LGPD estabelece os contornos da responsabilidade, fixando em seu art. 42: “O controlador ou o operador que, em

razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo." (BRASIL, 2018). O mesmo artigo, no § 3° prevê ainda a possibilidade de ação coletiva nesse tipo de ação.

A responsabilidade civil na LGPD não é clara ao definir o tipo de responsabilidade, podendo ser entendido que é subjetiva ou objetiva a depender do momento (SCHULMAN; CAVET, 2021). A doutrina majoritária parece defender que se trata de caso de responsabilidade objetiva, apesar de haver correntes contrárias defendendo a teoria subjetiva (MARTINS; TELLES, 2021), enquanto outros autores como Bioni e Dias (2020) preferem não se apegar a essas classificações, sendo a favor de uma responsabilidade do tipo gradiente, já que durante os debates legislativos acabou-se criando divergências que levaram a norma a não ser completamente objetiva.

A LGPD ainda institui a possibilidade de exclusão da responsabilização quando o dano for exclusivo da vítima ou de terceiros, conforme o art. 43. A verificação da regularidade do tratamento de dados será feita observando se foram utilizadas as medidas de segurança adequadas e necessárias disponíveis no momento dos acontecimentos, como pode ser extraído do art. 44. O Brasil lançou, inclusive, um guia de boas práticas sobre a proteção de dados para auxiliar as empresas e instituições a se adequarem a LGPD (2020a).

Quando houver caso de incidente de segurança, em casos em que a atividade desenvolvida for atividade de risco, Schulman e Cavet (2021) defendem a aplicação da súmula 479 do STJ. Tal súmula afirma que é responsabilidade das instituições financeiras fraudes e ataques praticados por terceiros. Entretanto a LGPD parece já ter sido clara quanto a esse tipo de responsabilização, sendo essa excluída apenas quando comprovada a implementação de ferramentas que garantam a segurança dos dados, à época do dano ocorrido.

Sobre o assunto Bioni e Dias (2020) revelam que a LGPD adotou técnica legislativa dúbia, estabelecendo no seu art. 44 que haverá responsabilização quando houver tratamento irregular por parte do agente, porém falhando ao conceituar o que seria o tratamento irregular. O tratamento irregular, segundo o art. 44, caput, os agentes responderão quando não fornecerem a segurança que o titular dele pode esperar, enquanto o art. 46 afirma será quando o agente deixar de adotar as medidas de segurança aptas a proteger os dados pessoais, o que não necessariamente significam o mesmo.

Adiciona-se que além da divergência acima mencionada, trata-se de circunstâncias pouco delimitadas. Quanto às medidas adotadas que seriam suficientes para proteger os dados pessoais, estas deveriam ser aquelas potencialmente suficientes para garantir a segurança ou

para de fato proteger a segurança dos dados? Caso seja entendido que só as medidas que de fato protegem, não significaria que sempre que houver vazamento de dados haverá a responsabilização do agente? Já no que se refere à expectativa de proteção do titular, já está claro que essa deve se basear em uma expectativa juridicamente legítima, tal qual o disposto no CDC em normas semelhantes, que entretanto também possuem um alto grau de subjetividade, e no caso da Proteção de Dados pouco se tem jurisprudência, por se tratar de um novel direito. Tais pontos poderão ser mais delimitados em casos concretos pelos Tribunais (BIONI; DIAS, 2020).

A Lei ainda faz referência a ideia de *Privacy by design* em seu art. 46, § 2°. Isso significa em síntese que medidas de proteção de dados devem ser previstas e tomadas desde o desenvolvimento do projeto (VILELA, 2021). Essa técnica tem como um dos princípios ser proativa, buscando prever e prevenir incidentes a proteção de dados (ROCHA, 2021). A plataforma de RNDS estaria de acordo com a LGPD baseada no fato que teria sido criada em torno da referida legislação e seguindo tal técnica (DALLARI; MONACO, 2021).

Cabe mencionar que o SUS não estaria necessariamente isento de sanções financeiras. Aragão e Schiocchet (2020) defendem a ideia que o Estado pode sofrer as sanções acima mencionadas, dispostas no art. 52 da LGPD, podendo essa chegar a R$ 50.000.000,00. Tais medidas se revelam importantes após os sucessivos vazamentos de dados. Não se nega essa possibilidade, entretanto, se mostra contraditória a penalização do órgão quando um dos problemas que leva a situação atual de falha na proteção dos dados de segurança é a própria falta de recursos enfrentada por várias dessas instituições.

Diante da existência do cabimento de multa, conforme as situações acima listadas, deve-se observar o disposto no artigo 52, § 1°, para ajudar a determinar a aferição do valor aplicado nas penalidades. O supracitado define os parâmetros para a definição dos valores a serem pagos pelo infrator, quais sejam: A gravidade e a natureza das informações e a violação dos direitos pessoais da pessoa afetada; A boa-fé do infrator; a vantagem obtida ou pretendida pelo infrator; a condição financeira do infrator; se o infrator é reincidente; a extensão do dano causado; a cooperação do infrator; a existência de mecanismos e procedimentos utilizados para evitar ou minimizar os danos gerados; a adoção de boas práticas e governança de dados; a posterior adoção de medidas corretivas; a proporcionalidade entre o dano e a sanção (BRASIL, 2018).

5 CONCLUSÃO

O presente trabalho teve como principal objetivo esclarecer se o Direito Fundamental à Proteção de Dados estava sendo concretizado frente ao Direito à Saúde no contexto da Pandemia de Covid-19. Para tanto foi realizada uma análise acerca da atuação do Estado, dos agentes de saúde e dos agentes de tratamento de dados afim de se chegar a uma resposta sobre a concretização ou não do Direito à proteção dos dados de saúde nesse cenário.

Foi possível vislumbrar ao longo desse trabalho o significado de dados pessoais, com aprofundamento em especial nos dados sensíveis e de forma ainda mais minuciosa nos dados de saúde. Ficou claro como ocorreu o desenvolvimento doutrinário do Direito à Proteção de Dados e como ele ganhou cada vez mais destaque, culminando na constitucionalização desse direito pela Emenda constitucional n. 115. Apesar disso, destaca-se que desde antes da promulgação dessa emenda, o Direito à Proteção de Dados já era compreendido, por alguns juristas e doutrinadores, como direito fundamental implícito, como pode ser observado inclusive na decisão do STF que entendeu pela existência de um Direito à Proteção de Dados autônomo.

Ao longo do trabalho também foi possível esclarecer algumas das principais formas de tratamento de dados relacionados à saúde, em especial no contexto da pandemia, bem como os dados e essas atividades são reguladas na atualidade. Através da LGPD e também de outras normas como a Lei nº 13.989 que permitiu o uso da telemedicina durante a pandemia de covid-19.

A partir da análise das referidas normas foi possível observar a preferência do legislador pela concretização do direito à saúde em face do Direito à Proteção de Dados. Isso pode ser visto na inexigibilidade do consentimento para o tratamento de dados de saúde, na permissão legal de ferramentas, como o Whatsapp e similares, que apresentam riscos ao Direito à Proteção de Dados. Além das normas, foi possível constatar a mesma tendência nas medidas adotadas pelo poder público, com a criação de um RES nacional no qual não é possível algumas formas de tratamento de dados pelos titulares dos direitos, como a exclusão e a retificação de dados pelos titulares.

O tratamento da maioria dos dados de saúde ocorre em conformidade com a LGPD, o que entretanto não significa dizer que estejam em total conformidade com o texto constitucional, vez que existem situações onde é possível se vislumbrar um conflito entre direitos fundamentais e as normas infraconstitucionais que efetivam tais direitos, à exemplo da LGPD. Conflitos entre o direito de proteção de dados e o direito à saúde, podem ser observados

em situações, como o da ausência de ferramenta adequada para manifestação do consentimento, quando do uso de aplicativos de contenção e monitoramento da pandemia. Não sendo esse, o único conflito existente observado entre direitos fundamentais.

Restaram constatadas, ainda, outras situações de conflito entre o direito constitucional de proteção de dados e o direito à saúde, como a que ocorre no uso da plataforma RNDS (voltada para o compartilhamento dos dados de saúde da população brasileira de forma a melhor atender às demandas na área), no que se refere à impossibilidade de exclusão ou modificação de dados de saúde da plataforma, uma vez que o sistema de informação utilizado torna impossível tais ações. Ocorre que, como já mencionado, a LGPD prevê o direito do titular dos dados realizar tais ações. Concluindo-se pela existência de outro caso de violação do direito fundamental à proteção de dados.

Outro caso encontrado ao longo do trabalho em que foi possível observar o conflito de direitos fundamentais, envolvendo o direito à Saúde e à Proteção de Dados, está relacionado à utilização de dados de saúde na realização de pesquisas. A LGPD prevê a necessidade de anonimização desses dados sensíveis para sua utilização em pesquisa, entretanto, existem situações em que se faz necessária a manutenção de tais dados para garantir a efetividade da pesquisa.

Diante de todos esses exemplos observa-se a já mencionada prioridade dada ao direito à saúde pelo legislador, em detrimento ao Direito à Proteção de Dados. Trata-se de um desamparo ao Direito à Proteção de Dados, que pode ser solucionado com a utilização do método de ponderação pelos tribunais superiores pátrios a fim de evitar um contínuo e massivo desrespeito do Direito à Proteção de Dados em face do direito à saúde. Os tribunais brasileiros são capazes de proferirem decisões garantindo ao mesmo tempo o Direito à Proteção de Dados e à saúde como ocorreu no caso da ponderação realizada no presente trabalho.

Devido a reconhecida crise do judiciário, que possui cada vez mais lides para julgar, pode-se cogitar também a criação de uma norma específica que trate especificamente dos dados de saúde e da utilização de ferramentas nos tratamentos de saúde que envolvam tais dados, sendo outra saída eficaz para o problema da priorização do direito à saúde. A criação das normas como a Lei nº 13.989, que permite de forma ampla e sem muitas delimitações a utilização da telemedicina e do parecer n. 14/2017 do Conselho Federal de Medicina, que autorizava a utilização do whatsapp e de plataformas similares foram importantes em um momento de crise, porém, é imperativo estabelecer diretrizes concretas para tratamento dos dados de saúde, uma vez que na sociedade atual a convivência com as ferramentas tecnológicas se mostra uma realidade. Normas desse tipo já foram criadas em outros países, gerando um impacto positivo.

Outra solução no presente caso se refere a medidas que podem ser tomadas pelo ANPD. Nesse sentido, cabe à autoridade a função fiscalizatória, além de estabelecer diretrizes a serem cumpridas no que se refere à proteção de Dados. A aplicação de medidas punitivas também está relacionada a concretização do Direito à Proteção de Dados em sua dimensão objetiva. Nesse sentido, a aplicação de multas pode levar a utilização de ferramentas ou sistemas de informação que comprometam menos o Direito à Proteção de Dados dos titulares do direito.

O presente trabalho delimitou apenas alguns dos problemas enfrentados na proteção dos dados de saúde na atualidade, que parecem aumentar diante dos constantes avanços da tecnologia e de sua implementação na medicina, podendo-se imaginar a elaboração de pesquisas relacionadas a tais inovações. Citam-se como exemplos: a tomada de decisões automatizadas na área médica, os dados genéticos e a inteligência artificial, essa última possui inclusive Projeto de Lei em Tramitação (PL 21/2020). Podem ser realizadas pesquisas também sobre as consequências da plataforma RNDS, que já estará em funcionamento nos próximos anos e do "*commission health data space*" pela União Europeia, que também está em progresso, para o Direito à Proteção de Dados.

REFERÊNCIAS

ALEXY, Robert. Colisão de direitos fundamentais e realização de direitos fundamentais no estado de direito democrático. **Revista da Faculdade de Direito**, n. 17, 1999.

ALEXY, Robert. Constitutional rights, balancing, and rationality. **Ratio Juris**, vol. 16, n. 2, jun. 2003. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-9337.00228. Acesso em: 07 mai. 2022.

ALEXY, Robert. **Teoria dos direitos fundamentais**. 2. ed. São Paulo: Malheiros Editores, 2015. (Teoria e direito público).

ALMEIDA, Bethania de Araujo *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciênc. Saúde coletiva**, Rio de Janeiro, v. 25, supl. 1, p. 2487-2492, 2020. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em 29 Out. 2020.

ANDRÉA, Gianfranco Faggin Mastro; ARQUITE, Higor Roberto Leite; CAMARGO, Juliana Moreira. PROTEÇÃO DOS DADOS PESSOAIS COMO DIREITO FUNDAMENTAL: a evolução da tecnologia da informação e a lei geral de proteção de dados no brasil. **Revista de Direito Constitucional e Internacional**, [s. l], v. 121, p. 115-139, set. 2020. Bimestral. Disponível em: https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/revistas-especializadas/rdci-121-gianfranco-andrea-e-outros.pdf. Acesso em: 18 maio 2022.

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do sistema único de saúde. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, [s.l.], v. 14, n. 3, p. 692-708, 29 set. 2020. Instituto de Comunicação e Informação Cientifica e Tecnológica em Saúde. http://dx.doi.org/10.29397/reciis.v14i3.2012. Disponível em: https://homologacao-reciis.icict.fiocruz.br/index.php/reciis/article/view/2012. Acesso em: 10 maio 2022.

ARAÚJO, Priscila Maria Menezes de. **A utilização de dados pessoais sensíveis na formação do perfil comportamental de pessoas naturais e o potencial dano aos seus titulares**. 2019. 99 f., il. Trabalho de Conclusão de Curso (Bacharelado em Direito) — Universidade de Brasília, Brasília, 2019. Disponível em: https://bdm.unb.br/handle/10483/25207. Acesso em: 20 abr. 2021.

ASSOCIAÇÃO NACIONAL DE HOSPITAIS PRIVADOS (ANAHP). Nota técnica observatório anahp, 3º trimestre, 2020, disponível em: https://conteudo.anahp.com.br/nt-observatorio-anahp-

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 9. ed. São Paulo: Saraiva Educação, 2020. p. 576.

BEZERRA, Selene Maria. Prontuário Eletrônico do Paciente: uma ferramenta para aprimorar a qualidade dos serviços de saúde. **Revista Meta: Avaliação**, v. 1, n. 1, p. 73-82, 2009.

Disponível em: https://revistas.cesgranrio.org.br/index.php/metaavaliacao/article/view/12. Acesso em: 12 março. 2022.

BIONI, Bruno *et al*. Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: **Data Privacy Brasil**, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**. São Paulo, ano, v. 21, p. 191-201, 2020. Disponível em: https://www.researchgate.net/profile/Bruno-Bioni/publication/352799291_Compreendendo_o_conceito_de_anonimizacao_e_dado_anonimizado/links/60da1d77a6fdccb745f09360/Compreendendo-o-conceito-de-anonimizacao-e-dado-anonimizado.pdf. Acesso em: 25 maio. 2022.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica**. com, v. 9, n. 3, p. 1-23, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: 11 maio 2022.

BRASIL. Advocacia Geral da União. Comitê Central de Governança de Dados. **Guia de boas práticas**: lei geral de proteção de dados (LGPD). 2. ed. Distrito Federal (DF): [s.n.], 2020a. 69 p. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 22 abr. 2021.

BRASIL. Agência Nacional de Saúde Suplementar. Tabela 1: Beneficiários de planos privados de saúde, por cobertura assistencial (Brasil – 2011-2021). Disponível em: https://www.ans.gov.br/perfil-do-setor/dados-gerais. Acesso em 15 jan 2021

BRASIL. **Constituição (1988).** Constituição, de 5 de outubro de 1988. Brasília: [s.n]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 abr. 2022

BRASIL. **Decreto nº 10.212**, de 30 de janeiro de 2020b. Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10212.htm. Acesso em: 27 mar. 2022.

BRASIL. **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022a. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.. . Brasília, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais.. Acesso em: 14 mar. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 14 ago. 2018. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 abr. 2021.

BRASIL. **Lei nº 13.979**, de 06 de fevereiro de 2020. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Brasília, 07 fev. 2020c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 27 mar. 2022.

BRASIL. **Lei nº 13.989**, de 15 de abril de 2020. Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2). Brasília, 15 de abril de 2020d. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L13989.htm. Acesso em: 25 jan. 2022.

BRASIL. **Lei nº 14.010**, de 10 de junho de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). [s.l], 8 set. 2020e**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 11 maio 2022.

BRASIL. **Medida Provisória nº 954**, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, 17 abr. 2020f. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 27 mar. 2022.

BRASIL. Ministério da Saúde. **A RNDS e a Transformação Digital**. 2022b. Disponível em: https://www.gov.br/saude/pt-br/assuntos/rnds/rnds-e-a-transformacao-digital/rnds-e-a-transformacao-digital. Acesso em: 28 mar. 2022.

BRASIL. Ministério da saúde - DATASUS. **Estratégia de Saúde Digital para o Brasil 2020-2028**. Brasília: [s.n.], 2020g. 128 p. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 12 fev. 2022.

BRASIL, Ministério da Saúde. **Pedido de acesso a dados brutos de utilização do aplicativo Coronavírus SUS - Pedido 25072019246202094**. [s.l]: 2020h. Disponível em: http://www.consultaesic.cgu.gov.br/busca/dados/Lists/Pedido/Item/displayifs.aspx?List=0c839f31-47d7-4485-ab65-ab0cee9cf8fe&ID=1483284&Web=88cc5f44-8cfe-4964-8ff4-376b5ebb3bef. Acesso em: 4 abr. 2022.

BRASIL. Ministério Da Saúde. **Portaria nº 1.434**, de 28 de maio de 2020. Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. [s.l], 29 maio 2020i. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=29/05/2020&jornal=515&pagina=231. Acesso em: 27 mar. 2022.

BRASIL. Ministério da saúde - DATASUS. **Aplicativo Coronavírus-SUS vai alertar contatos próximos de pacientes com Covid-19**: Os cidadãos vão participar ativamente no controle da doença, com apoio de tecnologia para alertar sobre exposição a novos infectados. [s.l]: DATASUS, 31 jul. 2020j. Disponível em: https://datasus.saude.gov.br/aplicativo-coronavirus-sus-vai-alertar-contatos-proximos-de-pacientes-com-covid-19/. Acesso em: 4 abr. 2022.

BRASIL. STF. **Habeas Corpus nº 91867**. Relator: Min. Gilmar Mendes. Brasília, 24 de abril de 2012. HC 91867. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2534858. Acesso em: 14 maio 2022.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6388**. Relator: Min. Rosa Weber. Brasília, DF, 07 de maio de 2020k. Brasília, 12 nov. 2020h. p. 1-154. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895166. Acesso em: 14 maio 2022.

BRASIL. Tribunal Regional Federal da 4ª Região. **Recurso Cível nº 50184917020194047205**, Segunda Turma Recursal. Relator: HENRIQUE LUIZ HARTMANN. Santa Catarina, 22 de outubro de 2020l. TRF-4 - Recurso Cível: 50184917020194047205 SC 5018491-70.2019.4.04.7205. Disponível em: https://trf-4.jusbrasil.com.br/jurisprudencia/1109985185/recurso-civel-50184917020194047205-sc-5018491-7020194047205/inteiro-teor-1109985234. Acesso em: 14 abr. 2022.

BROUGH, Aaron R.; MARTIN, Kelly D. Consumer privacy during (and after) the COVID-19 pandemic. **Journal of Public Policy & Marketing**, v. 40, n. 1, p. 108-110, 2021. Disponível em: https://journals.sagepub.com/doi/full/10.1177/0743915620929999. Acesso em: 14 maio 2022.

CAMARA, Maria Amália Arruda *et al*. Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da lei geral de proteção de dados. **Cadernos Ibero-Americanos de Direito Sanitário**, [s.l.], v. 10, n. 1, p. 93-112, 18 mar. 2021. http://dx.doi.org/10.17566/ciads.v10i1.657. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/657. Acesso em: 29 maio 2022.

CAMILO, Vinícius César de Oliveira *et al*. Telemedicina e fatores limitantes para seu exercício no Brasil e no mundo durante a pandemia de Covid-19: uma revisão integrativa. **Conjecturas**, [s.l.], v. 21, n. 6, p. 866-882, 8 dez. 2021. União Atlântica de Pesquisadores. http://dx.doi.org/10.53660/conj-409-211. Disponível em: https://doi.org/10.53660/CONJ-409-211. Acesso em: 10 maio 2022.

CASTELLS, Manuel. **A sociedade cm rede**: economia, sociedade e cultura. 6. ed. São Paulo: Paz e Terra, 2002. 698 p. Tradução: Roneide Venâncio Majer.

COELHO NETO, Giliate Cardoso; CHIORO, Arthur. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil? **Cadernos de Saúde Pública**, v. 37, p. e00182119, 2021. Disponível em: https://www.scielosp.org/article/csp/2021.v37n7/e00182119/. Acesso em: 15 mar. 2022.

COELHO, Akeni Lobo *et al*. A utilização de tecnologias da informação em saúde para o enfrentamento da pandemia do Covid-19 no Brasil. **Cadernos Ibero-Americanos de Direito Sanitário**, v. 9, n. 3, p. 183-199, 2020. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/709 . Acesso em: 20 abr. 2021.

CONSELHO FEDERAL DE MEDICINA (CFM - Brasil). **Parecer CFM Nº 14**. É permitido o uso do Whatsapp e plataformas similares para comunicação entre médicos e seus pacientes, bem como entre médicos e médicos, em caráter privativo, para enviar dados ou tirar dúvidas, bem como em grupos fechados de especialistas ou do corpo clínico de uma instituição ou cátedra, com a ressalva de que todas as informações passadas tem absoluto caráter confidencial e não podem extrapolar os limites do próprio grupo, nem tampouco podem circular em grupos recreativos, mesmo que composto apenas por médicos. Brasilia, 27 de abr. de 2017. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/BR/2017/14. Acesso em: 25 abr. 2021.

CONSELHO FEDERAL DE MEDICINA (CFM - Brasil). **Resolução nº 1.643**. Define e disciplina a prestação de serviços através da Telemedicina. Brasília: [s.n], 2002. Disponível em: https://abmes.org.br/arquivos/legislacoes/Resolucao-CFM-1643-2002-08-07.pdf. Acesso em: 14 maio 2022.

CONSELHO FEDERAL DE MEDICINA (CFM - Brasil). **Resolução nº 2.227**. Define e disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias. Brasília: [s.n], 2018. Disponível em: https://abmes.org.br/arquivos/legislacoes/Resolucao-CFM-2227-2018-12-13.pdf. Acesso em: 14 maio 2022.

COSTA, Mariana Monteiro da. **A era da vigilância no ciberespaço e os impactos da nova lei geral de proteção de dados pessoais no Brasil**: reflexos no direito à privacidade. 2018. 91 f. TCC (Graduação) - Curso de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: https://pantheon.ufrj.br/handle/11422/8252. Acesso em: 22 maio 2022.

DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). **LGPD na saúde**. 1 ed. São Paulo: ThomsonReuters, 2021.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo *et al*. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

FALCÃO, Paula; SOUZA, Aline Batista de. Pandemia de desinformação: as fakes news no contexto da Covid-19 no Brasil. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, v. 15, n. 1, 2021. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2219. Acesso em: 4 abr. 2022

G1. **Megavazamento de dados de 223 milhões de brasileiros**: o que se sabe e o que falta saber. **G1: Últimas notícias**. [s.l], p. 1-13. 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 10 maio 2022.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2008.

GAVIÃO FILHO, A. P.; LORENZONNI, P.C. Propostas de desenvolvimento da ponderação: uma análise das críticas de Sieckmann sobre a teoria dos princípios de Alexy. **NOMOS: Revista do Programa de Pós-Graduação em Direito da UFC**, Fortaleza, v. 39, n. 1, p. 209-226, jan./jun. 2019.

GÓES, Elizabeth Trombini; MARUCO, Fábia de Oliveira Rodrigues; DA SILVA, Vinícius Donato Saviano Teodoro. A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO EXERCÍCIO PROFISSIONAL NA ÁREA DA SAÚDE. **Revista Jurídica On-line**, v. 1, n. 1, p. 6-21, 2021.

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal**: desafios, modelos e principais impactos com a nova Lei. Brasília, 2019. Dissertação (Mestrado em Direito) – Centro Universitário de Brasília (UniCEUB), 2019.

GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados**: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Editora Fi, 2020. [livro eletrônico]

GUANAES, Paulo (org.). **Marcos legais nacionais em face da abertura de dados para pesquisa em saúde**: dados pessoais, sensíveis ou sigilosos e propriedade intelectual. Rio de Janeiro: Fiocruz, 2018. 122 p. Grupo de Trabalho em Ciência Aberta da Fiocruz. Disponível em: https://www.arca.fiocruz.br/handle/icict/28838. Acesso em: 10 maio 2022.

HINCH, Robert *et al*. Effective configurations of a digital contact tracing app: a report to NHSX. **Retrieved July**, v. 23, 2020.

IENCA, Marcello; VAYENA, Effy. On the responsible use of digital data to tackle the COVID-19 pandemic. **Nature medicine**, v. 26, n. 4, 2020. Disponível em: https://www.nature.com/articles/s41591-020-0832-5%3C. Acesso em: 25 out. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/TR 14639-1:2012**. Health informatics — Personal health records — Definition, scope and context. 1 ed. [s.l]: [s.n.], 2012. 20 p. Disponível em: https://www.iso.org/standard/54568.html. Acesso em: 14 maio 2022.

JUNEIDI, Salaheddin J. Covid-19 Tracing Contacts Apps: Technical and Privacy Issues. **Int. J. Advance Soft Compu. Appl**, v. 12, n. 3, 2020. Disponível em: https://www.researchgate.net/profile/Salaheddin_Juneidi/publication/344156198_Covid-19_Tracing_Contacts_Apps_Technical_and_Privacy_Issues/links/5f7e0221299bf1b53e15d90f/Covid-19-Tracing-Contacts-Apps-Technical-and-Privacy-Issues.pdf. Acesso em: 25 out. 2020.

KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine Learning with Personal Data. In: LEENES, Ronald *et al* (ed.). **Data Protection and Privacy**: the age of intelligent machines. Portland: Hart Publishing, 2017. Cap. 4. p. 89-114. (Computers, Privacy and Data Protection).

KNOTH, Pedro. Coronavírus - SUS não valida teste positivo de COVID para alerta de exposição: Aplicativo do Ministério da Saúde para monitorar a pandemia no Brasil não permite que usuários validem teste positivo de COVID-19 e avisem contatos próximos. **Terra**, [s.l], p. 1 -4, 27 jan. 2022. Disponível em: https://www.terra.com.br/noticias/tecnologia/coronavirus-sus-nao-valida-teste-positivo-de-covid-para-alerta-de-exposicao,85296e32e6809ac9547da22654ef1c679186qlmj.html. Acesso em: 4 abr. 2022.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz daLei 13.709/2018. In: FRAZÃO, Ana; GUSTAVOTEPEDINO; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019. Cap. 1. p. 445-463.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, v. 998, p. 99-125, 2019. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/58203675/Protecao_de_dados_pessoais_e_criptografia-with-cover-page-v2.pdf?Expires=1654374684&Signature=Af0cI30Q7YYWJZeIz24jCOIq5q9cHOmYeTlagM~o0PC1qtDnb3jkF6HnYH0fEsQo2QVvjPTXTnruKhf9gW8BXsjHyckqZ-wyc6GonvSxUbb4A8IE4imdJj1R7okIYzb-9rylAa9ifA3T8OGI64GvBsArGArZt3PHLxHBor8tX~9OaQ2zVHFNPc3U~9ITt2LL81cOziKC6R1jcpW0AaPz6iiIlBk1Yu2IJCUzMsSXvOg~faOO2vy2mgFc8eY7iBqjyOiZUc-wDJmhfYh48urCKCFYnSwRFQTBCxWJ2Efb4YpvbdtViCLjZncN8aZitQveFHpJMLkLSvpBNjTRkerp4g__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 20 maio 2022.

MACHADO, Rodrigo *et al*. Vazamentos de Dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. **Anais da XVII Escola Regional de Redes de Computadores** (Errc 2019), [s.l.] 17, p. 154-159, 16 set. 2019. Sociedade Brasileira de Computação - SBC. http://dx.doi.org/10.5753/errc.2019.9230. Disponível em: https://sol.sbc.org.br/index.php/errc/article/view/9230. Acesso em: 10 maio 2022.

MAGALHAES, George Geraldo. Inovação tecnológica na saúde: A proteção de dados sensíveis na telemedicina. In: 10th **International Symposium on Technological Innovation**. 2019. Disponível em: http://www.api.org.br/conferences/index.php/ISTI2019/ISTI2019/paper/view/890. Acesso em: 12 mar 2021.

MARTINS, Guilherme Magalhães; TELLES, Carlos André Coutinho. A telemedicina na saúde suplementar e a responsabilidade civil do médico no tratamento de dados à luz da lgpd. R**EI- Revista Estudos Institucionais**, v. 7, n. 1, p. 182-197, 2021. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/608. Acesso em: 12 mar 2021

MARTINS, Pedro. Categorizando Dados em um Contexto de Big Data: Em defesa de uma abordagem funcional. In: **XXIII Congresso Ibero-Americano de Direito e Informática**.

2019. Disponível em: https://www.researchgate.net/publication/336242873_CATEGORIZANDO_DADOS_EM_UM_CONTEXTO_DE_BIG_DATA_EM_DEFESA_DE_UMA_ABORDAGEM_FUNCIONAL/citations. Acesso em: 20 abr. 2021.

MASSENO, Manuel David. NA BORDA: dados pessoais e não pessoais nos dois regulamentos da união europeia. In: WACHOWICZ, Marcos (org.). **Proteção de dados pessoais em perspectiva**: LGPD e RGPD na ótica do direito comparado. Curitiba: Gedai, Ufpr, 2020. p. 126-145.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 16. ed. São Paulo: Saraiva Educação, 2021. Série IDP

MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Direito, Inovação e Tecnologia**, v. 1, p. 205-230, 2014.

MONDARDO, Marcos. Povos indígenas e comunidades tradicionais em tempos de pandemia da Covid-19 no Brasil: **Finisterra**, p. v. 55 n.o 115 (AOP) (2020): Número especial: COVID19, 2020. Disponível em: https://revistas.rcaap.pt/finisterra/article/view/20364. Acesso em: 4 abr. 2022.

MOURA, Clarissa Maria Lima; BARZA, Eugênia Cristina Nilsen Ribeiro (Orient.). **Dados pessoais como ativo na economia digital**: a tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos. 2019. 58 f. TCC (graduação em Direito) - Faculdade de Direito do Recife - CCJ - Universidade Federal de Pernambuco - UFPE - Recife, 2019. Disponível em: https://repositorio.ufpe.br/handle/123456789/37157. Acesso em: 20 abr. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159–180, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 22 maio 2022.

NAÍSA, Letícia. Ataque cibernético ao Ministério da Saúde não foi o 1º: veja outros casos. **Uol: O melhor conteúdo**. São Paulo, p. 1-5. 10 dez. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/12/10/ataque-hacker-ao-ministerio-da-saude-nao-foi-o-primeiro-veja-outros-casos.htm. Acesso em: 10 maio 2022.

NUNES, C. C.; MA, S.; FILHO, M. S. T. Armazenamento descentralizado no Sistema Único de Saúde brasileiro (SUS) usando Interplanetary File System (IPFS) e Blockchain. **Revista de Direito**, [S. l.], v. 13, n. 01, p. 01–25, 2021. DOI: 10.32361/2021130111695. Disponível em: https://periodicos.ufv.br/revistadir/article/view/11695. Acesso em: 4 jun. 2022.

NUNES, Júlia Graziele Santos. Desafios para promoção da saúde da população ribeirinha. **Ariquemes**: [s.n.], 2021. 47 p. Disponível em: https://repositorio.faema.edu.br/handle/123456789/2995. Acesso em: 4 abr. 2022.

PARK, Sangchul; CHOI, Gina Jeehyun; KO, Haksoo. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea — Privacy Controversies. Jama, [s.l.], v. 323, n. 21, p. 2129-2130, 2 jun. 2020. **American Medical Association (AMA)**. http://dx.doi.org/10.1001/jama.2020.6602. Disponível em: https://jamanetwork.com/journals/jama/fullarticle/2765252. Acesso em: 22 out. 2020.

PATRÍCIO, Camila Mendes *et al*. O prontuário eletrônico do paciente no sistema de saúde brasileiro: uma realidade para os médicos? **Scientia Medica** (Porto Alegre), v. 21, n. 3, p. 121-131, 2011. disponível em: https://search.bvsalud.org/portal/resource/en/lil-603941. acessado em:

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018

ROCHA, Thauane Prieto. **Um diálogo sobre a relevância da proteção de dados pessoais e sensíveis nos estabelecimentos de saúde**. 2021. 17 f. Tese (Doutorado) - Curso de Direito, Fundação de Ensino Eurípides Soares da Rocha, São Paulo, 2021. Disponível em: https://aberto.univem.edu.br/handle/11077/2122. Acesso em: 28 maio 2022.

RODOTÀ, Stefano. **A vida na socidade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. Tradução: Danilo Doneda e Luciana Cabral Doneda

SANTOS, Denise dos. **Internet das coisas e big data**: a proteção dos dados pessoais sensíveis. 2019. 35 f. TCC (Graduação) - Curso de Direito, Centro Universitário Unidombosco, Curitiba, 2019. Disponível em: https://juristas.com.br/wp-content/uploads/2020/10/ARTIGO-DENISE-DOS-SANTOS-UNIDOMBOSCO.pdf. Acesso em: 22 abr. 2021.

SÃO PAULO. TJ de São Paulo. **Agravo de Instrumento nº 21476017820208260000**. Relator: Desembargador. São Paulo, 28 de agosto de 2020. Tribunal de Justiça de São Paulo TJ-SP - Agravo de Instrumento: AI 21476017820208260000 SP 2147601-78.2020.8.26.0000 - Interior Teor. São Paulo, 28 ago. 2020. Disponível em: https://tj-sp.jusbrasil.com.br/jurisprudencia/919854667/agravo-de-instrumento-ai-21476017820208260000-sp-2147601-7820208260000/inteiro-teor-919854697. Acesso em: 27 maio 2022.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 14. ed. rev. e atual. - Porto Alegre: Livraria do Advogado, 2019.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017.

SARLET, Ingo Wolfgang. PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NA CONSTITUIÇÃO FEDERAL BRASILEIRA DE 1988. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 14, n. 42, p. 179-218, 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 11 maio 2022. Acesso em: 11 maio 2022.

SCHULMAN, Gabriel; CAVET, Caroline Amadori. A violação de dados pessoais na telemedicina: reparação do paciente à luz da lgpd. **Pensar Acadêmico**, v. 19, n. 3, p. 875-899, 2021. Disponível em: Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: 11 maio 2022. Acesso em: 11 maio 2022.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: Privacy and a new concept of personally identifiable information. **NYUL rev**., v. 86, p. 1814, 2011.

SHEN, Meng; WEI, Yaqian; LI, Tong. Bluetooth-based COVID-19 Proximity Tracing Proposals: An Overview. **arXiv e-prints, p. arXiv**: 2008.12469, 2020. Disponivel em: https://arxiv.org/abs/2008.12469 acessado em:

SOUSA, Zilda A. Goncalves de; FRANCO, Igor da Silveira. Autonomia privada e consentimento de crianças e adolescentes na Lei Geral de Proteção de Dados. In: GROSSI (org.). **Lei Geral de Proteção de Dados**: uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Editora Fi, 2020. Cap. 5. p. 102-132. Recurso eletrônico.

TAGIAROLI, Guilherme. App do SUS que monitora avanço da covid fracassa por falta de uso. **Uol - Tilt: O melhor conteúdo**. São Paulo, p. 1-6. 14 abr. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/04/14/falta-de-politica-nacional-faz-app-do-sus-flopar-no-rastreamento-de-contato.htm. Acesso em: 18 jan. 2022.

TAVARES, André Ramos. **Curso de direito constitucional**. 18. ed. São Paulo: Saraiva Educação, 2020.

TOLEDO, Patrícia Pássaro da Silva *et al*. Prontuário Eletrônico: uma revisão sistemática de implementação sob as diretrizes da política nacional de humanização. **Ciência & Saúde Coletiva**, [s.l.], v. 26, n. 6, p. 2131-2140, jun. 2021. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/1413-81232021266.39872020. Disponível em: https://www.scielo.br/j/csc/a/6V8wyd45cgZQ3ZjXBWXSpry/abstract/?lang=pt. Acesso em: 18 jan. 2022.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. [s.l], 18 dez. 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 18 jan. 2022.

VILELA, Gabriel Badim. **LGPD**: um estudo sobre as principais responsabilidades e penalidades previstas na lei. 2021. 48 f. TCC (Graduação) - Curso de Engenharia de Computação, Escola de Ciências Exatas e da Computação, Pontifícia Universidade Católica de Goiá, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1580. Acesso em: 10 maio 2022.

WANG, Dong; LIU, Fang. Privacy Risk and Preservation For COVID-19 Contact Tracing Apps. **arXiv e-prints, p. arXiv**: 2006.15433, 2020.

WERMUTH, Maiquel Angelo Dezordi; CARDIN, Valéria Silva Galdino; MAZARO, Juliana Luiza. Tecnologias de controle e dados sensíveis: como fica a proteção da sexualidade na lei geral de proteção de dados pessoais?.**Revista Jurídica Luso-Brasileira**, [s.l], v. 3, n. 8, p.

1065-1091, 2022. Disponível em: https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1065_1091.pdf. Acesso em: 22 maio 2022.

ERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, [s.l.], v. 29, n. 2, p. 71-77, ago. 2000. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0100-19652000000200009. Disponível em: https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?lang=pt&format=html. Acesso em: 15 maio 2022.

WORLD MEDICAL ASSOCIATION (WMA) *et al*. World Medical Association statement on accountability, responsibilities and ethical guidelines in the practice of telemedicine. **Adopted by the 51st World Medical Assembly, Tel Aviv, Israel**, 1999. Disponível em: https://www.wma.net/policies-post/wma-statement-on-accountability-responsibilities-and-ethical-guidelines-in-the-practice-of-telemedicine/ . Acesso em: 17 jan. 2022.

WORLD HEALTH ORGANIZATION (WHO). **A health telematics policy in support of WHO's Health-For-All strategy for global health development**: report of the WHO group consultation on health telematics. 11–16 December, Geneva, 1997. Geneva, World Health Organization, 1998.

WORLD HEALTH ORGANIZATION (WHO). **Contact tracing in the context of COVID-19: Interim guidance.** 1 February 2021.[s.l], World Health Organization, 2021. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf?sequence=24&isAllowed=y . Acesso em: 17 jan. 2022.

XAVIER, Andréia Castro Costa; DUQUE, Cláudio Gottschalg. Prontuário eletrônico do paciente: qual a contribuição da arquivística e do Smart Contracts para a sua gestão na Era da Saúde 4.0?. **AtoZ: novas práticas em informação e conhecimento**, v. 10, n. 3, p. 1-10, 2021. Disponível em: https://revistas.ufpr.br/atoz/article/view/81267. Acesso em: 10 maio 2022.

ZHAO, Qingchuan *et al*. On the accuracy of measured proximity of bluetooth-based contact tracing apps. In: **International Conference on Security and Privacy in Communication Networks**. 2020. Disponivel em: http://web.cse.ohio-state.edu/~zhao.2708/assets/securecomm20/SECURECOMM20a.pdf. acesso em: 26 out. 2020.