UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO

Igor Rizzatti Burigo Mendes

Open Health**:** uma análise das repercussões jurídicas da implementação do sistema no Brasil sob a ótica da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)

Florianópolis/SC
2022

Igor Rizzatti Burigo Mendes

Open Health: uma análise das repercussões jurídicas da implementação do sistema no Brasil sob a ótica da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)

Trabalho de Conclusão de Curso submetido ao curso de Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Orlando Celso da Silva Neto, Dr.

Florianópolis/SC

2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Rizzatti Burigo Mendes, Igor
Open Health: uma análise das repercussões jurídicas da implementação do sistema no Brasil sob a ótica da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) / Igor Rizzatti Burigo Mendes ; orientador, Orlando Celso da Silva Neto, 2022.
68 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Graduação em Direito, Florianópolis, 2022.

Inclui referências.

1. Direito. 2. Proteção de dados pessoais. 3. Open Health. 4. Lei Geral de Proteção de Dados Pessoais (LGPD). I. Celso da Silva Neto, Orlando. II. Universidade Federal de Santa Catarina. Graduação em Direito. III. Título.

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS JURÍDICAS

COORDENADORIA DE MONOGRAFIA

ATA DE SESSÃO DE DEFESA DE TCC (VIRTUAL)

(Autorizada pela Portaria 002/2020/PROGRAD)

Aos 7 dias do mês de dezembro do ano de 2022, às 11 horas e 00 minutos, foi realizada a defesa pública do Trabalho de Conclusão de Curso (TCC), no modo virtual, através do link "https://meet.google.com/cow-obqf-kwt" intitulado "*Open Health*: uma análise das repercussões jurídicas da implementação do sistema no Brasil sob a ótica da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)", elaborado pelo acadêmico Igor Rizzatti Burigo Mendes, matrícula nº 18100957, composta pelos membros Orlando Celso da Silva Neto, Paulo Vitor Petris Tambosi e Amanda de Medeiros Zimmermann, abaixo assinados, obteve a aprovação com nota 9,5 (nove virgula cinco), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

(X) Aprovação Integral
( ) Aprovação Condicionada aos seguintes reparos, sob fiscalização do Prof. Orientador

Florianópolis, 07 de dezembro de 2022.

ICP-Edu
Documento assinado digitalmente
Orlando Celso da Silva Neto
Data: 07/12/2022 15:08:08-0300
CPF: ***.014.309-**
Verifique as assinaturas em https://v.ufsc.br

Dr. Orlando Celso da Silva Neto (ASSINATURA DIGITAL)
Professor Orientador

ICP-Edu
Documento assinado digitalmente
Paulo Vitor Petris Tambosi
Data: 07/12/2022 13:37:30-0300
CPF: ***.218.609-**
Verifique as assinaturas em https://v.ufsc.br

Paulo Vitor Petris Tambosi (ASSINATURA DIGITAL)
Membro de Banca

GOV.BR
Documento assinado digitalmente
AMANDA DE MEDEIROS ZIMMERMANN
Data: 09/12/2022 10:10:06-0300
CPF: ***.775.189-**
Verifique as assinaturas em https://v.ufsc.br

Amanda de Medeiros Zimmermann (ASSINATURA DIGITAL)
Membro de Banca

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS JURÍDICAS

COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado "*Open Health*: uma análise das repercussões jurídicas da implementação do sistema no Brasil sob a ótica da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)", elaborado pelo acadêmico "Igor Rizzatti Burigo Mendes", defendido em 07/12/2022 e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 9,5 (nove virgula cinco), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 07 de dezembro de 2022

ICP-Edu
Documento assinado digitalmente
Orlando Celso da Silva Neto
Data: 07/12/2022 17:22:59-0300
CPF: ***.014.309-**
Verifique as assinaturas em https://v.ufsc.br

Dr. Orlando Celso da Silva Neto
Professor Orientador

ICP-Edu
Documento assinado digitalmente
Paulo Vitor Petris Tambosi
Data: 07/12/2022 13:36:58-0300
CPF: ***.218.609-**
Verifique as assinaturas em https://v.ufsc.br

Paulo Vitor Petris Tambosi
Membro de Banca

GOV.BR
Documento assinado digitalmente
AMANDA DE MEDEIROS ZIMMERMANN
Data: 09/12/2022 10:11:04-0300
CPF: ***.775.189-**
Verifique as assinaturas em https://v.ufsc.br

Amanda de Medeiros Zimmermann
Membro de Banca

Universidade Federal de Santa Catarina

Centro de Ciências Jurídicas

COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E ORIENTAÇÃO IDEOLÓGICA

Aluno(a): Igor Rizzatti Burigo Mendes
RG: 6.026.208
CPF: 120.112.449-27
Matrícula: 18100957
Título do TCC: *Open Health*: uma análise das repercussões jurídicas da implementação do sistema no Brasil sob a ótica da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)
Orientador: Dr. Orlando Celso da Silva Neto

Eu, Igor Rizzatti Burigo Mendes, acima qualificado, venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 07 de dezembro de 2022.

Documento assinado digitalmente
IGOR RIZZATTI BURIGO MENDES
Data: 07/12/2022 13:20:40-0300
CPF: ***.112.449-**
Verifique as assinaturas em https://v.ufsc.br

_____

IGOR RIZZATTI BURIGO MENDES

Dedico este trabalho a todos que, de alguma forma,
participaram da minha trajetória acadêmica.

RESUMO

A presente monografia tem por objetivo analisar a proposta de instituição de um sistema de *Open Health* no setor de saúde suplementar brasileiro, ventilada pelo Ministério da Saúde em recentes declarações, com base nas diretrizes previstas na Lei 13.709/2018. Em síntese, a proposta de *Open Health* consiste na criação de um banco de dados pessoais de saúde mantido pelo governo, ao qual seria conferido acesso às operadoras de planos de saúde para que utilizem essas informações com o objetivo de melhorar a qualidade do atendimento aos beneficiários, reduzir custos e aumentar a concorrência. Apesar dos evidentes benefícios, a proposta repercutiu entre a sociedade civil, institutos de pesquisa e entidades de proteção ao consumidor, que demonstraram preocupação com a falta de menção a iniciativas e mecanismos de segurança para assegurar a proteção aos dados pessoais, que são considerados como "sensíveis" por tratarem da saúde dos titulares. Justamente em razão disso é que será realizada uma análise com base na Lei 13.709/2018, também chamada de Lei Geral de Proteção de Dados Pessoais (LGPD), que delimita uma série de regras para tutelar o direito à privacidade e à proteção de dados pessoais — este último, inclusive, incluído como direito fundamental na Constituição Federal de 1988 por meio da Emenda Constitucional nº 115/2022. Assim, a problemática central da pesquisa pode ser sintetizada na seguinte pergunta: "A Lei 13/709/2018 permite a implementação de um sistema de *Open Health* no setor de saúde suplementar brasileiro?". Ao responder a pergunta, também serão expostos os limites legais e possibilidades normativas na instituição de um sistema de dados abertos de saúde, assim como os desafios inerentes à proposta do Ministério da Saúde e suas possíveis soluções.

Palavras-chave: Proteção de dados pessoais; Lei 13.709/2018; Lei Geral de Proteção de Dados Pessoais (LGPD); *Open Health*; Direito fundamental à proteção de dados;

ABSTRACT

This monograph aims to analyze the proposal to establish an Open Health system in the Brazilian supplementary health sector, aired by the Ministry of Health in recent statements, based on the guidelines provided by the Law 13.709/2018. In summary, the Open Health proposal consists in creating a personal health database maintained by the government, which would be granted access to health plan operators so that they can use this information with the aim of improving the quality of care for beneficiaries, reduce costs and increase competition. Despite the obvious benefits, the proposal had repercussions among civil society, research institutes and consumer protection entities, which showed concern about the lack of mention of initiatives and security mechanisms to ensure the protection of personal data, which are considered as “sensitive” because they deal with the health of the holders. Precisely for this reason, an analysis will be carried out based on Law 13.709/2018, also called the General Law for the Protection of Personal Data (LGPD), which delimits a series of rules to protect the right to privacy and the protection of personal data. — the latter included as a fundamental right in the Federal Constitution of 1988 through Constitutional Amendment nº 115/2022. Thus, the central problem of the research can be summarized in the following question: “Does Law 13/709/2018 allow the implementation of an Open Health system in the Brazilian supplementary health sector?”. When answering the question, the legal limits and normative possibilities in the institution of an open health data system will also be exposed, as well as the challenges inherent to the proposal of the Ministry of Health and its possible solutions.

Keywords: Personal data protection; Law 13.709/2018; General Law for the Protection of Personal Data; Open Health; Fundamental right to data protection;

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANS	Agência Nacional de Saúde Suplementar
API	*Application Programming Interface*
BC	Banco Central
CADE	Conselho Administrativo de Defesa Econômica
CDR	*Consumer Data Right*
CMA	*Competition and Market Authority*
CMN	Conselho Monetário Nacional
CNSP	Conselho Nacional de Seguros Privados
CNS	Conselho Nacional de Saúde
EC	Emenda Constitucional
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados Pessoais
MP	Medida Provisória
ONU	Organização das Nações Unidas
OPS	Operadoras de Planos de Saúde
PEC	Proposta de Emenda Constitucional
PL	Projeto de Lei
RNDS	Rede Nacional de Dados em Saúde
STF	Supremo Tribunal Federal
SUSEP	Superintendência de Seguros Privados

SUMÁRIO

1 INTRODUÇÃO

A criação dos meios de comunicação em grande escala, tendo como principal representante a *internet*, e o surgimento de novas tecnologias da informação representaram uma virada de chave importante para a vida na sociedade moderna. Se as relações interpessoais até o século passado ocorriam de forma predominantemente analógica e presencial, o desenvolvimento tecnológico exponencial no século XXI fez com que passássemos a compor a chamada "sociedade da informação", responsável pelo fim das barreiras físicas como um empecilho para o progresso.

Nesse contexto, o estudo da proteção dos dados pessoais assume uma posição de extrema relevância, principalmente diante do desenvolvimento informático e da efervescência tecnológica em que a sociedade está inserida, o que é confirmado pela utilização cada vez maior do *Big Data* e do *Big Analytics* — ferramentas capazes de tratar dados pessoais de forma mais volumosa, rápida e diversificada. Em complemento, a aplicabilidade das novas tecnologias está presente em todos os setores da sociedade, desde a criação de novas soluções de mercado para empresas de telecomunicação, até a concepção de sistemas informacionais para que sejam armazenados os dados pessoais de saúde de pacientes tratados em hospitais. Todos esses fatores justificam a escolha do tema e a sua atualidade, visto que estamos cada dia mais imersos em um mundo tomado por dados.

Dessa forma, a temática do direito à proteção de dados pessoais será central para o presente trabalho, que terá o objetivo analisar as repercussões jurídicas da implementação de um sistema de *Open Health* no setor de saúde suplementar, conforme divulgou o Ministério da Saúde, de modo a demonstrar as limitações legais, as possibilidades normativas e os desafios dessa iniciativa sob a ótica da Lei 13.709/2018 ou Lei Geral de Proteção de Dados Pessoais (LGPD).

O estudo será desenvolvido a partir do método de abordagem dedutivo, partindo de princípios já reconhecidos como verdadeiros e indiscutíveis para se alcançar conclusões específicas, sob o alicerce de bibliografias especializadas nacionais – prioritariamente doutrinárias. A metodologia de trabalho será a descritiva, que utilizar-se-á da análise bibliográfica e hermenêutica/lógica para chegar ao resultado pretendido.

Ademais, o trabalho será dividido em três capítulos, de modo a detalhar cada tema proposto para permitir uma compreensão geral sobre o objeto da pesquisa. Em um primeiro momento, optou-se por apresentar as experiências do Brasil e do mundo com os sistemas de dados abertos, tendo especial enfoque no *Open Finance* e no *Open Insurance*. Em complemento, será abordada a proposta de implementação de um sistema de *Open Health* na saúde suplementar, que foi veiculada como parte da agenda regulatória do Ministério da Saúde e representa uma medida de alta relevância ao cenário de proteção de dados pessoais brasileiro por meio do impacto a milhões de cidadãos.

Em seguida, passar-se-á ao estudo sobre a LGPD, como uma forma de situar o leitor acerca dos pilares da doutrina de proteção de dados brasileira. Inicialmente, será apresentado um histórico da proteção de dados pessoais com o traçado de uma linha do tempo desde a paradigmática decisão do Tribunal Constitucional da Alemanha no caso da lei do censo de 1983, até a positivação da proteção de dados como direito fundamental na Constituição Federal de 1988 por meio da Emenda Constitucional nº 115/2022. Ato contínuo, serão apresentados os principais conceitos da LGPD, tendo especial enfoque nos dispositivos legais que tratam sobre os dados pessoais sensíveis relacionados à saúde.

Por fim, no último capítulo será promovida a conexão entre o *Open Health* e a LGPD para que se determinem os limites legais e possibilidades normativas a serem observados no momento da implementação de um sistema de dados abertos no setor de saúde suplementar. Ademais, serão apresentados os principais desafios, de ordem lógica e organizacional, vivenciados pelo setor de saúde, que representam empecilhos à instituição do *Open Health*, assim como propostas para a sua eventual solução.

2 OS SISTEMAS DE DADOS ABERTOS NO BRASIL E NO MUNDO

Segundo dados da Organização das Nações Unidas (ONU)[1], atualmente existem 5,3 bilhões de usuários da *internet* ao redor do mundo — número que tem crescido com o passar dos anos. Só em 2022, o acesso às redes cresceu 7% em comparação com 2021. No mesmo sentido, uma pesquisa conduzida pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação demonstrou que a *internet* foi acessada por 81% da população brasileira no ano de 2021[2].

Essas informações demonstram que o mundo virtual está cada vez mais presente na vida atual, de modo a promover uma verdadeira hiperconectividade na sociedade moderna. Danilo Doneda entende o desenvolvimento da tecnologia, a partir de sua penetração no cotidiano da sociedade, passou a influenciar diretamente a forma como trabalhamos, nos relacionamos, distribuímos o nosso tempo e, em linhas gerais, vivemos[3].

Diante disso, percebe-se que a criação de soluções de mercado e a promoção de inovações direcionadas ao ambiente digital são cruciais para o progresso em um mundo tomado por relações interpessoais vistas pela tela dos *smartphones*, computadores e televisões. É nesse contexto que se inserem as iniciativas de dados abertos, que buscam viabilizar o compartilhamento de dados entre os atores de determinado setor da sociedade para, dentre outros objetivos, oferecer produtos e serviços mais adequados e personalizados à realidade de cada pessoa, tendo como base os seus dados pessoais.

Nesse contexto, o presente capítulo busca contextualizar o leitor acerca dos sistemas de compartilhamento de dados nos diversos setores da economia — finanças, seguros e saúde —, de modo a fazer com que se compreenda a real

[1] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. **Onu News**. [S.L], 16 set. 2022. Disponível em: https://news.un.org/pt/story/2022/09/. Acesso em: 10 out. 2022.

[2] SILVA, Vitor Hugo. 81% da população brasileira acessou a internet em 2021, diz pesquisa. **G1**. São Paulo, 21 jun. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/06/21/81percent-da-populacao-brasileira-acessou-a-internet-em-2021-diz-pesquisa.ghtml. Acesso em: 10 out.2022.

[3] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 45.

dimensão dessas iniciativas, que têm o potencial de impactar bilhões de pessoas ao redor do mundo.

Assim, em um primeiro momento, será realizada uma análise do *Open Finance* e do *Open Insurance* enquanto sistemas de compartilhamento de dados pessoais já regulamentados no Brasil, que podem servir como referencial para a compreensão do *Open Health*. Para isso, será realizada a análise da origem desses sistemas de dados abertos, das regulamentações que os instituíram e de suas vantagens e desvantagens.

Em seguida, numa segunda abordagem, será analisada a proposta de implementação do *Open Health* compartilhada pelo Ministério da Saúde por meio do ministro Marcelo Queiroga, que demonstrou a inclusão do assunto na agenda regulatória brasileira como uma prioridade do atual governo. Ainda, serão expostos os principais motivos pelos quais o estudo sobre a implementação de um sistema de *Open Health* necessita ser diferente das demais iniciativas de dados abertos, tendo especial enfoque nas normativas específicas do setor de saúde suplementar.

2.1 SURGIMENTO E CARACTERÍSTICAS DOS SISTEMAS DE COMPARTILHAMENTO DE DADOS

2.1.1 *Open Finance* (Sistema Financeiro Aberto)

O *Open Finance*, também chamado de sistema financeiro aberto, foi regulamentado inicialmente através da Resolução Conjunta nº 1/2020, ainda sob a denominação de *Open Banking*, tendo o Banco Central (BC) e o Conselho Monetário Nacional (CMN) como principais comandantes da iniciativa. O termo *Open Banking* permaneceu vigente até 2 de maio de 2022, quando entrou em vigor a Resolução Conjunta nº 4/2022, que alterou, dentre outros dispositivos, o nome do sistema para *Open Finance.*

Em síntese, o *Open Finance* consiste no “compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas”, conforme se extrai do artigo 2º, I da Resolução Conjunta nº 4/2022. Em outras palavras, o sistema permite a comunicação entre instituições financeiras por meio do acesso aos dados pessoais financeiros dos usuários que consentirem com a sua participação no *Open Finance*.

Esse compartilhamento de informações, por sua vez, é realizado através de uma API (Interface de Programa de Aplicações ou *Application Programming Interface*, em inglês), que funciona como uma linguagem para permitir que *softwares* de diferentes instituições financeiras e instituições de pagamentos se comuniquem[4].

De acordo com a página eletrônica do *Open Finance*[5], o seu propósito é "trazer inovação ao sistema financeiro, promover a concorrência, e melhorar a oferta de produtos e serviços financeiros", de modo que o titular de dados pessoais tenha controle sobre as suas próprias informações e tenha poder de decisão sobre a sua forma de tratamento — se irá participar, quem irá acessar os dados, quais dados serão compartilhados, entre outros. Dessa forma, o contorno regulatório do *Open Finance* é pensado para garantir que o consumidor financeiro esteja em posse de seus dados pessoais, e não as instituições financeiras ou o governo[6].

Antes de se adentrar nas especificidades do sistema, faz-se necessário expor o cenário nacional e internacional que serviu como propulsor para a criação do *Open Finance* no Brasil*.* O movimento dos sistemas financeiros abertos surge no século XXI, inserido em um contexto de ampla digitalização da vida cotidiana e da crescente dependência dos meios digitais para a vida em sociedade, sejam eles utilizados para trabalho (reuniões por vídeo chamada, captação de clientes, utilização de serviços de armazenamento em nuvem, etc) ou para motivos pessoais (consultas médicas, navegação em redes sociais, conversa com entes queridos, etc).

Atualmente, a presença cada vez maior dos cidadãos nos ambientes virtuais fez com que a prestação de serviços digitais e a criação de novas soluções tecnológicas, direcionadas para facilitar a experiência do consumidor, sejam elementos fundamentais a qualquer empresa esteja inserida em mercados competitivos, sendo que as empresas participantes do mercado financeiro não fogem à regra. Em complemento, a crise causada pela pandemia de Covid-19 fez com que os serviços bancários, mais do que nunca, fossem utilizados pela via digital, tendo em vista a necessidade repentina de se evitar o contato físico para frear a disseminação

[4] TAVARES, Letícia Becker. O papel do Banco Central na implementação do *Open Finance* no Brasil. In: CRAVO, Daniela Copetti; JOBIM, Eduardo; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Direito público e tecnologia**. São Paulo: Editora Foco, 2022. p. 287.

[5] Banco Central. **Open Finance Brasil**. Disponível em: https://openfinancebrasil.org.br/. Acesso em: 10 out. 2022.

[6] TAVARES, 2022, p. 287-288.

do vírus. Todos esses elementos fizeram com que o mercado financeiro e bancário voltasse os olhos para a necessidade de se valorizar os meios digitais e entendê-los como uma porta de entrada para novos usuários e uma ferramenta de fidelização dos antigos.

Nesse contexto de transformação digital da economia, a União Europeia, um bloco econômico agregador de 27 países europeus, foi a primeira a regulamentar o *Open Finance* no mundo por meio da Diretiva de Serviços de Pagamento UE 2015/2366, também conhecida como *Second Payment Services Directive* ou "PSD2"[7]. A regulamentação, pioneira na forma de se pensar os serviços financeiros abertos, foi concebida para prover o fundamento legal ao desenvolvimento do mercado de pagamentos eletrônicos na União Europeia, de modo a estabelecer regras para os serviços de pagamento e, ao mesmo tempo, um alto nível de proteção ao consumidor[8].

Além de estabelecer diversos direitos aos consumidores inseridos na cadeira de serviços financeiros, a PSD2 determinou as obrigações a serem seguidas pelas instituições financeiras ao abrirem as APIs direcionadas ao compartilhamento de informações com outras instituições financeiras. Atualmente, de acordo com dados do site Open Banking Tracker[9], as cinco maiores economias da UE[10] — Alemanha, França, Itália, Espanha e Holanda — possuem, somadas, 1521 instituições prestadoras de serviços financeiros e 336 APIs abertas e funcionais.

Além da União Europeia, também são relevantes as iniciativas de outros países, como Reino Unido, Austrália e Hong Kong. No Reino Unido, a adoção do *Open Finance* foi promovida pela *Competition and Market Authority* (CMA), a autoridade concorrencial britânica, entidade análoga ao Conselho Administrativo de Defesa Econômica (CADE) do Brasil[11]. Para promover a regulamentação do *Open Finance*, a CMA criou um órgão chamado de *Open Finance Implementation Entity* (OBIE), que

[7] TAVARES, 2022, p. 291.

[8] EUR-LEX: ACCESS TO EUROPEAN UNION LAW. **Revised rules for payment services in the EU**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366. Acesso em: 10 out. 2022.

[9] BANQ. **Open Banking Directory and PSD2 API Tracker**. Disponível em: https://openbankingtracker.com/. Acesso em: 10 out. 2022.

[10] COUNTRYECONOMY.COM. **Dados econômicos e demográficos da União Europeia**. Disponível em: https://pt.countryeconomy.com/paises/grupos/uniao-europeia. Acesso em: 10 out. 2022.

[11] TAVARES, 2022, p. 292.

atualmente é controlado pela CMA e financiado pelos nove bancos com mais relevância no Reino Unido — Royal Bank of Scotland, Santander, Barclays, HSBC, Lloyds, Nationwide, Danske Bank, Allied Irish Banks e Bank of Ireland[12]. Por esse motivo, o *Open Finance* foi objeto de regulamentação com enfoque no viés concorrencial e bancário, tendo em vista a forte influência dos bancos durante todo o processo regulatório. No momento, o Reino Unido possui 164 prestadores de serviços financeiros e 194 APIs ativos, o que demonstra a relevância de sua participação no mercado de *Open Finance*.

Por sua vez, o processo da criação de um sistema financeiro aberto na Austrália foi encabeçado pela *Australian Competition & Consumer Commission* com a criação do *Consumer Data Right* (CDA), que não é destinado exclusivamente ao mercado financeiro, mas também aos outros setores da economia que possam aproveitar a infraestrutura de compartilhamento de dados pessoais. Por ser promovido por uma entidade de proteção aos consumidores, o CDA possui um claro enfoque na proteção ao consumidor e aos seus dados pessoais durante todo o processo de compartilhamento de informações entre as instituições financeiras.

De modo a contemplar a experiência do Reino Unido, com foco no viés concorrencial, e da Austrália, com foco no viés consumerista, Hong Kong trouxe as diretrizes para a instituição do *Open Finance*, em 2018, por meio do *Open API Framework for the Hong Kong Banking Sector*, que representou um esforço conjunto do governo e de entidades do mercado financeiro.

Trazendo a discussão para a experiência do Brasil, a iniciativa de se criar o *Open Finance* teve início muito antes da elaboração e publicação da Resolução Conjunta nº 1/2020, tendo o setor privado como protagonista em um primeiro momento. Ainda em 2017, o Banco do Brasil lançou uma plataforma para desenvolvedores de *software* chamada de "BB *for developers"*, que continha a possibilidade de inclusão de APIs para promover a comunicação entre os sistemas envolvendo informações dos seus correntistas. Na época, foi realizada a seleção de cinco aplicações envolvendo APIs, cujas soluções propostas hoje fazem parte da infraestrutura de *Open Finance* da instituição. Contudo, a iniciativa do Banco do Brasil, por mais que tenha sido pioneira em âmbito nacional, possuía uma limitação clara: um

[12] Ibid.

sistema de dados abertos, que pressupõe o compartilhamento de dados entre instituições financeiras, depende da participação de mais instituições financeiras.[13]

Em razão da falta de movimentação do setor privado brasileiro em direção a um sistema financeiro aberto, que dependia do rompimento de inércia por parte dos principais representantes do mercado financeiro e bancário brasileiro, o *Open Finance* entrou na agenda regulatória do Banco Central. Por meio do Comunicado nº 33.455, de 24 de abril de 2019, a entidade expôs a sua vontade de implementar um sistema de *Open Finance* no Brasil após ter realizado diversas conversas informais com representantes do mercado financeiro: bancos, instituições de pagamento, *fintechs*, cooperativas de crédito, entre outros. No texto do comunicado, o Banco Central informou a sua intenção de equilibrar aspectos consumeristas, concorrenciais, regulatórios e de proteção de dados para criar uma regulamentação completa, já levando em conta as experiências internacionais, principalmente, do Reino Unido e da Austrália[14].

Ainda em 2019, o tema foi objeto de discussão com a sociedade civil através da Consulta Pública nº 73/2019, de 28 de novembro de 2019, que recepcionou sugestões e comentários sobre as minutas da resolução, tendo como objetivo disciplinar a implementação do *Open Banking* por parte de instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central. Como resultado da Consulta, o Conselho Monetário Nacional e o Banco Central publicaram a já mencionada Resolução Complementar nº 01/2020, que assentou as bases para o *Open Finance* em solo brasileiro e previu um cronograma de implementação gradual, dividido em quatro etapas.

Na primeira fase, iniciada em 01/02/2021, as instituições financeiras puderam compartilhar, de forma pública e padronizada, as informações sobre seus canais de atendimento, produtos e serviços. Em seguida, na segunda fase, iniciada em 13/08/2021, o consumidor pôde compartilhar os seus dados pessoais com instituições financeiras de sua preferência ao consentir com o tratamento das suas informações

[13] GUIMARÃES, Olavo. Concorrência bancária e o *Open Banking* no Brasil. **Revista de defesa da concorrência**, Brasília, vol. 9, pg. 129, jun. 2021. Disponível em: https://www.bnb.gov.br/s482-dspace/bitstream/123456789/880/1/2020_INET_01.pdf. Acesso em: 10 out. 2022.

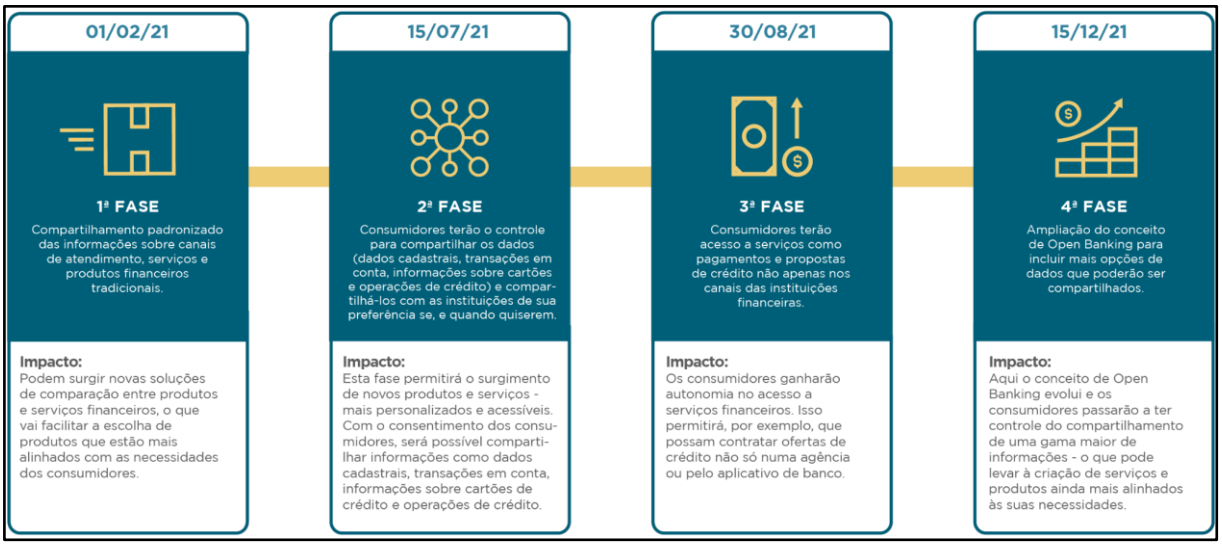
[14] TAVARES, 2022, p. 293

para finalidades específicas e destacadas. Dentre esses dados, estão informações sobre transações em conta, dados cadastrais e operações de crédito.

Na terceira fase, com início em 29/10/2021, surge a possibilidade do compartilhamento dos serviços de iniciação de transações de pagamento e do encaminhamento de propostas de operação de crédito diretamente ao consumidor. Essa etapa tem o fim de oportunizar o surgimento de novas soluções e ambientes, mais fáceis e convenientes ao consumidor, para o acesso a serviços financeiros e a tomada de crédito. Por fim, na quarta fase, que teve início em 15/12/2021, os consumidores poderão compartilhar ainda mais dados financeiros, se comparada à segunda fase. Nessa etapa, foi oportunizado o compartilhamento de dados envolvendo a contratação de operações de câmbio, seguros, previdência privada e investimento, tendo a finalidade criar produtos e serviços financeiros cada vez mais condizentes com a realidade dos consumidores.

Para melhor compreensão da implementação faseada do *Open Finance*, na imagem abaixo, retirada do sítio eletrônico “Open Finance Brasil”, evidenciam-se todas as etapas:

Figura 1 - Linha do tempo de implementação do *Open Finance* no Brasil



Fonte: Sítio eletrônico “Open Banking Brasil”

Dentre os benefícios do *Open Finance*, é possível listar o aumento de concorrência no ecossistema bancário e financeiro, que se justifica pela facilidade de ingresso de novas empresas e produtos no mercado por conta da maior facilidade no

acesso a informações sobre os consumidores financeiros, assim como a melhora no atendimento ao cliente e nos serviços prestados em razão do acréscimo na competição[15]. Nesse sentido, também se verifica a redução dos custos bancários em benefício do consumidor, visto que as instituições financeiras estão buscando outras formas de atrair os consumidores em virtude do aumento da concorrência[16]. Esse movimento já pode ser observado por meio do oferecimento de contas digitais sem anuidade, cartões de crédito com limite pré-aprovado e programas de milhas gratuitos. Por fim, é visível que o consumidor sairá muito mais satisfeito, já que não está mais restrito a algumas poucas instituições financeiras para ser cliente e pode migrar com mais facilidade entre elas por meio da dinâmica de compartilhamento de dados proposta pelo *Open Finance*[17].

Por outro lado, dentre os principais desafios enfrentados pelo *Open Finance*, a segurança da informação se mostra como a principal preocupação ao se implementar um sistema financeiro aberto. O processo de compartilhamento de dados pessoais entre instituições financeiras deve ser seguro e confiável, de modo a serem empregadas tecnologias e medidas direcionadas à prevenção das violações de dados. Essa preocupação não deve ser tomada apenas com base no necessário respeito ao titular de dados pessoais, mas também com fundamento na Lei Geral de Proteção de Dados Pessoais (LGPD), em especial nos princípios da segurança[18] e da prevenção[19].

2.1.2 *Open Insurance* (Sistema de Seguros Aberto)

O *Open Insurance*, também chamado de sistema de seguros aberto, é uma iniciativa desenvolvida e conduzida no Brasil pela Superintendência de Seguros Privados (Susep), tendo o *Open Finance* como uma forte inspiração. Em síntese, o *Open Insurance* visa operacionalizar o compartilhamento de dados entre entidades

[15] CAVALCANTE, Eric. O novo paradigma tecnológico do setor financeiro nacional: a implantação do *Open Banking* no Brasil. **Radar: tecnologia, produção e comércio exterior**, Brasília, vol. 66, p. 20, ago. 2021. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/10726/1/radar_n66.pdf. Acesso em: 10 out. 2022.
[16] Ibid.
[17] Ibid.
[18] Art. 6º, VII da Lei 13.709/2018.
[19] Art. 6º, VIII da Lei 13.709/2018.

autorizadas e credenciadas pela Susep, tendo como objetivos principais o estímulo à inovação no mercado de seguros, o aumento da concorrência entre as empresas e, por consequência, a melhoria na prestação de serviços e oferecimento de produtos aos consumidores. Esse compartilhamento é realizado por meio de APIs, que promovem a integração dos diferentes sistemas existentes no mercado de securitização. Em seu sítio eletrônico, a Susep conceitua o *Open Insurance* da seguinte forma:

> O Open Insurance, ou Sistema de Seguros Aberto, é a possibilidade de consumidores de produtos e serviços de seguros, previdência complementar aberta e capitalização permitirem o compartilhamento de suas informações entre diferentes sociedades autorizadas/credenciadas pela Susep, de forma segura, ágil, precisa e conveniente. Para entregar esses benefícios ao consumidor, o Open Insurance operacionaliza e padroniza o compartilhamento de dados e serviços por meio de abertura e integração de sistemas, com privacidade e segurança.

Inicialmente, o *Open Insurance* foi regulamentado no Brasil pela Resolução do Conselho Nacional de Seguros Privados (CNSP) nº 415/2021, que determinou os aspectos gerais da implementação do sistema de seguros aberto. Dentre os objetivos apresentados na resolução, destaca-se (i) a promoção da concorrência, (ii) o incentivo à inovação, (iii) ter o cliente como o principal beneficiado e (iv) tornar seguro, ágil preciso e conveniente o compartilhamento padronizado de dados com fundamento na Lei Geral de Proteção de Dados Pessoais e outras legislações aplicáveis. Em análise desses objetivos, é perceptível que a Susep tem o intuito de promover o equilíbrio entre a inovação no setor de seguros e a proteção de dados pessoais, de modo a fomentar uma abordagem do *Open Insurance* focada no consumidor enquanto sujeito de direitos. Essa ideia é reforçada pelos princípios previstos na mesma resolução, como os princípios da transparência, da segurança e privacidade de dados e do tratamento não discriminatório, que deixam claro a harmonização e alinhamento entre sistema de seguros aberto e a LGPD.

Ato seguinte, por meio da Circular nº 635/2021, a Susep apresentou as diretrizes práticas para a implementação das obrigações descritas na Resolução nº 415/2021. De forma semelhante ao que ocorreu com o *Open Finance*, a implementação do *Open Insurance* é prevista em três fases, de modo a cadenciar a etapa de adequação para que as entidades integrantes do setor de seguros consigam

se adaptar às mudanças previstas e os consumidores tenham tempo para assimilar a inovação no mercado de seguros. Na primeira etapa, desenvolvida entre dezembro de 2021 e junho de 2022, as seguradoras puderam compartilhar informações sobre seus canais de atendimento, produtos e serviços oferecidos, de modo a garantir padronização e transparência para que os consumidores possam tomar decisões mais assertivas. Na segunda etapa, que será iniciada em setembro de 2022 e terá o seu fim em junho de 2023, os consumidores do mercado de seguros poderão compartilhar os seus dados pessoais entre as instituições participantes do *Open Insurance*, o que será realizado apenas mediante o seu consentimento para tanto. Por fim, a terceira etapa, que tem o início previsto para dezembro de 2022 e fim em junho de 2023, possui o escopo de efetivação de serviços com os ajustes necessários para a efetivação do compartilhamento de dados entre instituições credenciadas pela Susep.

A linha do tempo abaixo, retirada do sítio eletrônico da Susep, demonstra a ordem das etapas, assim como as datas previstas para o início e término de cada uma delas:

Figura 2 - Linha do tempo de implementação do *Open Insurance* no Brasil

Fonte: Sítio eletrônico da Susep sobre o *Open Insurance*

De forma semelhante ao retratado sobre o *Open Finance*, o *Open Insurance* também possui os seus benefícios e desafios. Dentre os seus pontos positivos, é preciso destacar o aumento da competitividade do setor com o ingresso de novas empresas em um mercado altamente concentrado. Isso se torna possível por meio do compartilhamento de dados entre as diferentes empresas do setor de seguros, de

modo a se promover uma maior facilidade de migração por parte dos consumidores e forçar a melhora no atendimento aos segurados. De acordo com Solange Vieira, ex-superintendente da Susep, enquanto nos Estados Unidos da América existe uma seguradora para cada 75 mil habitantes, no Brasil existe uma empresa de seguros para cada 1 milhão e 700 mil brasileiros, o que demonstra a utilidade do *Open Insurance* como uma ferramenta para se quebrar essa concentração[20].

Por outro ponto de vista, o *Open Insurance* também enfrenta o desafio de garantir com que os dados pessoais compartilhados entre as instituições do setor de seguros sejam tratados em conformidade com a LGPD, o que pressupõe a tomada de medidas jurídico-técnico-administrativas para cumprir as diretrizes previstas em lei.

2.2 PROPOSTA INICIAL PARA A CRIAÇÃO DE UM SISTEMA DE *OPEN HEALTH* (SISTEMA DE SAÚDE SUPLEMENTAR ABERTO)

Em 11 março de 2022, o Ministério da Saúde, por meio de seu ministro Marcelo Queiroga, publicou um artigo de opinião no jornal Folha de São Paulo[21], no qual compartilhou a sua visão inicial sobre a construção de um sistema de *Open Health* no Brasil[22]. No pronunciamento, o ministro destacou que a ideia de um sistema de dados abertos na área de saúde surgiu pela necessidade de aumentar a capacidade de atendimento do sistema de saúde, o que ficou evidente após a experiência marcante e trágica ocorrida durante a pandemia global de Covid-19. Para Marcelo Queiroga, o projeto traria maior eficiência, transparência e concorrência ao sistema de saúde suplementar, permitindo, ainda, que beneficiários negociassem condições mais favoráveis em seus planos sem intermediações. Sendo assim, destacou que a iniciativa seria “questão de tempo, coragem e decisão”.

---

[20] CARVALHO, Sérgio. Das 119 seguradoras autorizadas a operar no Brasil, apenas 10 detém 80% de todo o mercado. **Jornal Nacional dos Seguros.** São Paulo. out. 2019. Disponível em: https://genteseguradora.com.br/das-119-seguradoras-autorizadas-a-operar-no-brasil-apenas-10-detem-80-de-todo-o-mercado/. Acesso em: 10 out. 2022.

[21] QUEIROGA, Marcelo. “Open Health” é uma questão de tempo, coragem e decisão. **Folha de São Paulo**. São Paulo, 5 de março de 2022. Disponível em: https://www1.folha.uol.com.br/opiniao/2022/03/open-health-e-questao-de-tempo-coragem-e-decisao.shtml. Acesso em: 10 out. 2022.

[22] QUEIROGA, 2022.

Muito embora não exista uma definição única, é possível dizer que o *Open Health* consiste em um sistema aberto de compartilhamento de dados de saúde entre os diversos atores do sistema de saúde suplementar, como os pacientes, laboratórios, hospitais, convênios e Operadoras de Planos de Saúde (OPS)[23]. Em síntese, o sistema consistiria na criação de um grande banco de dados que centralizaria os dados de saúde do cidadão, de modo a reunir informações obtidas pelos setores público e privado para permitir resultados mais assertivos e atendimentos mais personalizados[24]. No mesmo sentido, esses dados pessoais também poderiam ser utilizados pelas OPS para oferecer contratos mais adequados à realidade do consumidor, assim como pelos gestores públicos como uma forma de criar políticas públicas na área da saúde com maior efetividade e direcionamento[25].

Apesar da aparente semelhança entre o *Open Health* e os outros sistemas de compartilhamento de dados existentes no Brasil — *Open Finance* e *Open Insurance* —, como destacou o próprio Ministério da Saúde em seu pronunciamento, há de se evidenciar a existência de diferenças significativas.

Os sistemas estão inseridos em mercados distintos, que possuem regras próprias e regulamentações opostas — um exemplo disso é a possibilidade ou a vedação à seleção de risco na contratação de produtos e serviços. No mercado de seguros, por exemplo, a avaliação do perfil risco do condutor de um automóvel, direcionada ao oferecimento de produtos e serviços mais adequados à realidade dos consumidores, é prática comum na precificação e seleção dos contratos, sendo recepcionada pelo Decreto-Lei nº 73/1966, que regulamenta a atividade do sistema nacional de seguros privados. Diante dessa possibilidade, o compartilhamento de dados entre seguradoras, previsto no *Open Insurance*, para verificar o perfil de risco do segurado, tende a consolidar ainda mais a noção de seleção de riscos no mercado de securitização.

Por outro lado, na área da saúde suplementar, a Lei 9.656/1998, que estabelece o regramento específico aos planos e seguros de saúde privados, prevê

[23] CAMPOS, Ricardo; MARANHÃO, Juliano. Considerações sobre a construção de um open health no Brasil. **Jota**. São Paulo, 2 de setembro de 2022a. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/consideracoes-sobre-a-construcao-de-um-open-health-no-brasil-02092022>. Acesso em: 10 out. 2022.

[24] CAMPOS; MARANHÃO, 2022a.

[25] CAMPOS; MARANHÃO, 2022a.

que as OPS não podem deixar de admitir a contratação de seus serviços em razão da idade ou da condição de deficiência do consumidor[26]. Na mesma linha, o artigo 11, § 5º da LGPD determina que a prática é proibida "na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários", assim como estabelece a não discriminação como princípio norteador do tratamento de dados pessoais no ordenamento jurídico brasileiro. De igual forma, o artigo 6º da Constituição Federal de 1988 insere o direito à saúde como direito fundamental, de ordem social. Todas essas disposições legais demonstram que o sistema de saúde suplementar, mesmo sendo composto por entidades privadas, deve entender interesse público inerente aos serviços de saúde como o fio condutor de suas atividades.

Diante do exposto, é evidente que a instituição de um sistema de *Open Health* poderá (e deverá) levar em consideração toda a experiência vivenciada pelos órgãos regulamentadores dos sistemas de dados abertos aplicados aos setores financeiro e de seguros. Todavia, diferente do *Open Insurance* e do *Open Finance*, o *Open Health* enfrenta desafios próprios do setor de saúde, tendo principal enfoque nas questões envolvendo o tratamento de dados pessoais sensíveis, que demandam soluções distintas daquelas propostas pelos sistemas já existentes.

[26] Art. 14 da Lei 9.656/1998.

3 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Na linha do exposto no capítulo anterior, os sistemas de dados abertos possuem especificidades que os definem como únicos em suas áreas de atuação. O *Open Finance* utiliza os dados de usuários do sistema financeiro com o objetivo de oferecer produtos e serviços cada vez mais personalizados, de modo a valer-se de informações como o histórico de transações e a obtenção de crédito para essa finalidade. Já o *Open Insurance*, seguindo a mesma linha do sistema anterior, emprega os dados sobre o perfil dos seus usuários para fornecer contratos mais condizentes com a realidade. Por fim, o *Open Health*, de acordo com a proposta pensada pelo Ministério da Saúde, utilizaria os dados sobre os beneficiários do sistema de saúde suplementar para garantir mais transparência, eficiência e concorrência ao setor de saúde, de modo a possibilitar iniciativas visando a melhoria na qualidade do atendimento ao paciente e a entrada de novas empresas em um mercado ainda protagonizado por poucos.

Todavia, apesar das particularidades de cada um dos sistemas, é visível que todos eles dependem de um elemento comum para a sua existência: dados sobre os seus usuários[27]. Nesse sentido, percebe-se que a discussão sobre políticas de dados abertos, aplicadas em quaisquer áreas — finanças, seguros ou saúde —, necessita da análise das normativas e regulamentações que versam sobre o tratamento de dados pessoais, que têm como sua principal representante a Lei 13/709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

Concebida no cenário legislativo e regulatório brasileiro como uma forma de criar direitos e obrigações ligadas ao tratamento de dados pessoais, a LGPD funciona como uma ferramenta para garantir o uso sustentável das informações ligadas às pessoas naturais, tendo o objetivo de promover o equilíbrio entre o desenvolvimento econômico e o direito à proteção de dados pessoais e à privacidade, entre outros fundamentos descritos no seu artigo 2º. Sobre a necessidade de se olhar para a proteção de dados ao analisar as relações públicas e privadas na modernidade, Regina Ruaro e Gabrielle Sarlet pontuam que essa área do direito representa uma "garantia contra a assimetria relacional que caracteriza o atual cenário globalizado,

[27] IS DATA REALLY THE NEW OIL? **Kenway Consulting.** [S.L]. 10 ago. 2022. Disponível em: <https://www.kenwayconsulting.com/blog/data-is-the-new-oil/>. Acesso em: 10 out. 2022.

hiperconectado em que os gigantes tecnológicos se tornaram hegemônicos e suplantaram a atuação dos Estados”[28].

Dessa forma, a discussão sobre a Lei é imprescindível ao presente estudo, motivo pelo qual se dedica o presente capítulo para a análise de seus principais institutos. Em um primeiro momento, se abordará a origem histórica da disciplina da proteção de dados pessoais e a sua evolução até o patamar atual. Ato seguinte, em um segundo momento, analisar-se-ão os seus principais institutos para a compreensão da dinâmica da proteção de dados pessoais no ordenamento jurídico brasileiro.

3.1 A ORIGEM DA PROTEÇÃO DE DADOS PESSOAIS: DA CORTE CONSTITUCIONAL ALEMÃ À EMENDA CONSTITUCIONAL Nº 115/2022

Apesar de ser novidade ao ordenamento jurídico brasileiro, a construção da disciplina jurídica da proteção de dados pessoais data de muito antes da promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), tendo como principal berço os países localizados em território europeu. No ano de 1970, a Lei de Proteção de Dados do *Land* alemão de Hesse entrou em vigor, sendo tratada por muitos como o primeiro diploma legal que apresentou a proteção de dados inserida em um modelo normativo autônomo — sem relação de codependência com a segurança da informação, privacidade ou sigilo[29]. Ao tomar como inspiração a experiência tida pelo condado de Hesse, outros países europeus coordenaram a criação de leis de proteção de dados em seus próprios territórios, como é o exemplo da Lei de Proteção de Dados sueca de 1973, que foi chamada de *Datalagen*, e da própria Lei alemã de Proteção de Dados de 1977, a *Bundesdatenschutzgesetz*.

Na mesma linha, uma decisão tomada pelo Tribunal Constitucional Federal da Alemanha (*Bundesverfassungsgericht*, em alemão) representou um verdadeiro marco teórico no campo da proteção de dados pessoais. No caso, que é conhecido como o

[28] RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados - Lei 13.709/2018. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 305.

[29] DONEDA, 2021, p. 35.

julgamento da “Lei do Censo”, a corte debateu sobre os riscos da ampla coleta e tratamento de dados pessoais pelo governo alemão por meio da condução do censo populacional de 1983. Em sua decisão, a corte constitucional reconheceu a existência de um direito fundamental à autodeterminação informacional, de modo a inserir o indivíduo como o verdadeiro dono de seus dados pessoais e protagonista na relação de tratamento de seus dados pessoais. Danilo Doneda, ao comentar sobre a paradigmática decisão, entende que[30]:

> Ao reconhecer a centralidade do controle sobre as próprias informações para a proteção da personalidade no contexto do tratamento automatizado de dados, o Tribunal realizou notável trabalho de atualização das garantias fundamentais em vista das circunstâncias tecnológicas da época.

Em 1995, seguindo a forte tradição de proteção de dados cultivada nas décadas anteriores, a União Europeia elaborou a Diretiva 95/46/CE, tendo como objetivo a "proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados”. Em 2016, a Diretiva foi substituída pelo Regulamento UE nº 2016/679, batizado de *General Data Protection Regulation* (GDPR), que inaugurou uma nova era na proteção de dados pessoais ao prever, de forma detalhada e minuciosa, as diretrizes para o seu tratamento e servir como inspiração para diversas outras normativas emergentes no mundo.

Foi nesse contexto de efervescência tecnológica e crescimento do número de leis de proteção de dados ao redor do globo, que começou a se pensar na elaboração de uma lei brasileira para delimitar os direitos e obrigações envolvendo o tratamento de dados pessoais. Soma-se a isso, o fato de que diversas legislações brasileiras, que precederam a LGPD, previam dispositivos versando sobre a proteção aos dados pessoais, como a Lei 12.965/2014 (Marco Civil da Internet), a Lei nº 12.527/2011 (Lei de Acesso à Informação) e a Lei 12.414/2011 (Lei do Cadastro Positivo).

Na linha do movimento global pela proteção aos dados pessoais e da necessidade de se concentrar as normativas brasileiras em único diploma legal, a elaboração de uma lei específica entrou na agenda legislativa. Após amplo debate pela sociedade civil e extenso período de tramitação no Congresso Nacional, a versão final do Projeto de Lei (PL) nº 53/2018 foi aprovada e, em 14 de agosto, sancionada

[30] DONEDA, 2021, p. 37.

para tornar-se a Lei 13.709/2018, que conhecemos como LGPD e representa uma ferramenta, atualmente, indispensável ao se pensar a proteção de dados pessoais em solo brasileiro.

Não obstante, apesar de ser disciplinada por lei infraconstitucional, a proteção de dados pessoais também merece especial atenção pelas disposições constitucionais. O Supremo Tribunal Federal (STF), no julgamento da Ação Direta de Inconstitucionalidade nº 6387, confirmou a decisão monocrática proferida pela Ministra Rosa Weber, que suspendeu a eficácia da Medida Provisória (MP) nº 954/2020, que obrigava as empresas de telefonia a disponibilizarem ao IBGE dados como nome, números de telefone e endereços dos usuários, pessoas físicas e jurídicas "com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares"[31].

A decisão, paradigmática em matéria de proteção de dados pessoais no ordenamento jurídico brasileiro, reconheceu de forma inédita a existência de um direito autônomo à proteção de dados pessoais, que não se confunde com o direito fundamental à privacidade. Sobre o tema, discorreu o Ministro Luiz Fux em seu voto:

> A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), todos previstos na Constituição Federal de 1988.

Ainda, a iniciativa de se aproximar o direito à proteção de dados pessoais das normas constitucionais não foi exclusiva do Poder Judiciário. É o que se observa a partir da Proposta de Emenda Constitucional (PEC) nº 17/2019, que resultou na aprovação da Emenda Constitucional (EC) nº 115/2022 e incluiu o direito à proteção de dados pessoais[32] como um dos direitos fundamentais protegidos pelo ordenamento jurídico brasileiro. De acordo com o Senador Eduardo Gomes, autor da PEC, já existe

[31] Art. 1º, §1º da MP nº 954/2020.

[32] Art. 5º, LXXIX da Constituição Federal de 1988.

“uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado”[33].

Diante de todo o exposto, percebe-se que o interesse mundial pela proteção aos dados pessoais, desde a discussão travada pela corte federal alemã até a positivação do tema na carta magna brasileira, representa um importante avanço para a sociedade e uma garantia de que as informações mais importantes da individualidade humana terão a tutela jurídica que merecem.

3.2 ASPECTOS GERAIS DA LGPD

3.2.1 Princípios

Robert Alexy, renomado jurista e filósofo do direito alemão, pensa a sua teoria dos direitos fundamentais com base na existência de normas jurídicas direcionadas a orientar a concretização das regras basilares do ordenamento jurídico, sendo essas normas compostas por duas espécies: regras e princípios. Segundo Alexy, de um lado, regras são normas que devem ser cumpridas de forma exata e integral em todos os casos[34]. Por outro lado, princípios são normas que determinam que algo deve ser realizado na maior medida possível, levando em conta as possibilidades jurídicas e fáticas — nas palavras do autor, seriam “mandados de otimização”[35]. Nesse contexto, infere-se que princípios são diretrizes gerais do ordenamento jurídico, que tem o objetivo de fundamentar e servir como ferramenta interpretativa às demais normas, de modo a levar em consideração os aspectos políticos, econômicos e sociais vivenciados em sociedade, bem como as demais fontes do Direito.

Nesse cenário, a LGPD prevê uma série de princípios, que são direcionados a orientar e a balizar as atividades de tratamento de dados pessoais realizadas em solo brasileiro. É o que se observa abaixo:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

[33] BRASIL. **Proposta de Emenda Constitucional nº 17/2019**. Brasília: Senado Federal, 2019. Disponível em:https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline. Acesso em: 10 out. 2022.
[34] ALEXY, Robert. **Derecho e razón prática**. México: Fontamara, 1993. p. 87.
[35] Ibid.

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas 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 difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

De início, o princípio da finalidade se mostra como um dos mais importantes dentro de toda a dinâmica de tratamento de dados pessoais prevista na LGPD. Possuindo notável relevância prática, o princípio visa garantir que o titular de dados pessoais tenha a informação exata sobre o motivo pelo qual os seus dados serão utilizados, assim como assegurar que seus dados não serão tratados para finalidades diversas das previamente veiculadas.

Na GDPR, o princípio análogo ao da finalidade é da “limitação da finalidade” (*Purpose Limitation*, em inglês), que, assim como ocorre na LGPD, prevê a necessidade de o tratamento de dados pessoais ser realizado para propósitos legítimos, específicos e explícitos. De acordo com a legislação europeia[36], "legítimo" representa um conceito amplo, que deve ser analisado caso a caso, mas deve ser entendido a partir do cruzamento entre as outras normas contidas no ordenamento jurídico brasileiro para que se verifique a adequação da atividade de tratamento. Por

[36] UNIÃO EUROPEIA. **Opinion 03/2013 on purpose limitation**. Bélgica, Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 10 out. 2022.

sua vez, o termo “específico” deve ser entendido como a necessidade de se promover o tratamento apenas para finalidades pontuais e, por isso, não os usar para razões diversas das previamente acordadas com os titulares de dados pessoais. Por fim, “explícito” significa que os agentes de tratamento devem garantir que o titular de dados pessoais tenha ciência inequívoca sobre as finalidades do tratamento.

Não obstante, também vale pontuar que o princípio prevê a necessidade da finalidade do tratamento de dados pessoais ser informada ao titular “de forma clara, adequada e ostensiva”[37]. Nesse aspecto, percebe-se a existência de uma interface concreta entre o princípio da finalidade e o princípio da transparência, que oferece as diretrizes sobre como esse dever informacional por parte dos agentes de tratamento de dados deve ser exercido.

Dessa forma, o princípio da transparência, como o próprio nome já explica, objetiva transparecer ao titular a forma como os seus dados pessoais são tratados (finalidades/propósitos do tratamento, agentes de tratamento envolvidos, compartilhamento com terceiros, etc) por meio de informações claras, precisas e facilmente acessíveis. Assim, o princípio visa permitir com que o titular de dados efetivamente tenha controle sobre os seus dados pessoais ao saber para que eles são utilizados e, por conseguinte, conseguir tomar decisões de acordo com os seus direitos[38].

Outro princípio que guarda estreita relação com princípio da finalidade é o da adequação, uma vez que determina que o tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular. Assim, no caso de um relógio inteligente que coleta os dados sobre os batimentos cardíacos e os compartilha com uma empresa especializada para dar *feedbacks* ao usuário sobre como ter um vida mais saudável, o tratamento de dados pessoais estará em conformidade com o referido princípio, desde que tenha o consentimento específico e destacado do titular para esse propósito específico — considerando que se tratam de dados pessoais sensíveis[39]. Contudo, se essa mesma empresa compartilhar esses dados sobre para outras empresas para que ofereçam produtos e serviços direcionados a pessoas com insuficiência cardíaca, esse tratamento de dados é considerado fora do escopo

[37] VAINZOF, 2020, p. 129.
[38] VAINZOF, 2020, p. 139.
[39] VAINZOF, 2020, p. 133.

previsto inicialmente e, portanto, inadequado de acordo com o princípio da adequação.

Ato contínuo, o princípio da necessidade determina a limitação do tratamento de dados pessoais ao mínimo necessário para atingir as finalidades previstas, tendo em mente quais são as espécies de dados pessoais realmente imprescindíveis para que se atinja a finalidade do tratamento. A temática também é objeto de regulamentação pela GDPR por meio princípio da minimização de dados (*Data Minimisation*), descrito no artigo 5º, alínea "c" da legislação europeia, que prevê que os dados pessoais são "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados"[40]. Nesse contexto, políticas empresariais baseadas na retenção excessiva de dados pessoais podem, provavelmente, representar uma desconformidade com o princípio e tornar a atividade de tratamento ilícita de acordo como a LGPD.

Outrossim, o princípio do livre acesso também figura como um importante elemento para a análise da dinâmica de tratamento de dados prevista na LGPD, visto que foi criado para garantir com que o titular possa controlar a utilização de seus dados pessoais e, dessa forma, concretizar a ideia de autodeterminação informativa, que prevê o indivíduo em uma posição ativa com relação aos seus dados perante entes públicos e privados. Esse princípio tem os seus termos reforçados pelo que é descrito no artigo 9º da LGPD, que prevê o seguinte:

> 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.

[40] UNIÃO EUROPEIA. **Regulamento UE nº 2016/679**. Art. 5º. Disponível em: https://gdpr-info.eu/art-5-gdpr/. Acesso em: 10 out. 2022.

Nesse contexto, o acesso facilitado aos dados pessoais por parte dos titulares funciona como uma forma de permitir com que os mesmos tenham controle sobre o fluxo de informações de sua titularidade, de modo a possibilitar a correção de eventuais inexatidões ou o requerimento do descarte de dados tratados em desconformidade com a LGPD.

Ademais, sobre o princípio da qualidade dos dados, sua importância surge em um contexto em que o tratamento de dados pessoais pode revelar muito mais sobre a pessoa do que apenas o que está escrito. A inexatidão dos dados pessoais de determinada pessoa pode conduzir a análises equivocadas ou precipitadas, que não raro tem o potencial de causar danos ao titular. Como exemplo disso, é possível citar a recusa na concessão de crédito pela imprecisão do histórico de pagamentos de uma pessoa ou o erro no atendimento médico pela ausência da informação sobre a alergia a um determinado medicamento.

Em adição, os princípios da segurança e da prevenção são complementares em razão de seu objetivo comum: prevenir o sofrimento de danos pelos titulares em razão de violações aos seus dados. Segundo Rony Vainzof, violações de dados pessoais "são eventos caracterizados por acessos não autorizados e ocorrências acidentais ou propositais de destruição, perda, alteração, comunicação ou difusão de dados pessoais"[41], que implicam em prováveis danos (i) aos titulares de dados, que terão o seu direito fundamental à privacidade e à proteção de dados violados, e (ii) aos agentes de tratamento, que terão a sua reputação e credibilidade degradadas perante a sociedade.

Nesse contexto, o princípio da segurança define que as violações de dados pessoais devem ser evitadas a todo o custo, sendo imperioso que os agentes de tratamento efetivem medidas técnicas e administrativas para efetivar essa proteção, o que deve ocorrer desde a fase de concepção do produtos ou serviço até a sua execução. Por sua vez, o princípio da prevenção determina que as atividades de tratamento de dados pessoais devem ser pautadas em medidas destinadas a evitar com que ocorram violações de dados. Essa prevenção deve ser pautada no conceito de *Privacy by Design*, que delimita que o processamento de dados pessoais deve ser

[41] VAINZOF, Rony. Capítulo I: disposições preliminares. In: MALDONADO, Viviane Nóbrega *et al* (org.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 142.

exercido com base em três pilares indispensáveis, descritos por Rony Vainzof como "(i) sistemas de tecnologia da informação (*IT systems*); (ii) práticas negociais responsáveis (*accountable business practices*); e (iii) design físico e infraestrutura de rede (*physical and network infrastructure*)".

Outrossim, o princípio da responsabilização e da prestação de contas demonstra a preocupação da LGPD em demonstrar que os agentes de tratamento (controladores, operadores e encarregados) são responsáveis pela realização do tratamento de dados em conformidade com o diploma legal. Muito embora a sistemática de responsabilização civil e administrativa por violações de dados pessoais esteja implícita em nosso ordenamento jurídico, o princípio visa reforçar efetivo compromisso dos agentes com a subsunção do tratamento de dados a todos os demais princípios previstos na LGPD.

Por fim, é importante tratar sobre o princípio da não discriminação, que possui estreita relação com a temática tratada no presente estudo — a implementação de um sistema de *Open Health* no Brasil. O referido princípio tem especial relevância na LGPD, tendo em vista que existe como uma ferramenta para coibir a realização de práticas discriminatórias envolvendo o tratamento de dados pessoais e, dessa forma, salvaguardar os direitos dos titulares de dados. Nas palavras de Rony Vainzof, o princípio da não discriminação tem o objetivo de "impor limites e permissões no processamento de dados, de modo a mitigar o risco do determinismo tecnológico"[42]. Dentre as práticas discriminatórias e segregatórias possivelmente tomadas em razão do processamento de dados, é possível citar a negação de uma vaga de emprego em razão de opção sexual ou o aumento no valor mensal de um plano de saúde por causa de predisposição a certa doença — esse último, inclusive, vedado expressamente pelo artigo 11, §5º da LGPD.

3.2.2 Dados pessoais e dados pessoais sensíveis

Inicialmente, antes de se adentrar no estudo sobre dados pessoais conforme a LGPD, faz-se necessário pontuar o que são dados, sendo eles pessoais ou não. Segundo Gomes, Pimenta e Schneider, dado é o "registro do atributo de um ente,

[42] VAINZOF, 2020, p. 149.

objeto ou fenômeno", sendo que "registro" é a impressão de caracteres que sejam imbuídos de significado e "atributo" representa uma propriedade desses entes, objetos ou fenômenos[43].

De acordo com Danilo Doneda, existe uma diferença marcante entre os termos "dado" e "informação", comumente despercebida pela lei e pela doutrina no Direito brasileiro, que tratam os conceitos de forma indistinta[44]. Esses termos possuem vários pontos de contato, o que pode justificar a confusão existente, sendo possível entender o seu elemento comum como o fato de ambos simbolizarem um aspecto particular da realidade. O trecho abaixo demonstra as diferenças:

> Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza[45].

Na mesma linha, Ingo Sarlet entende que dados são elementos, como sinais ou símbolos, que ainda não foram interpretados e processados, sendo esse o motivo pelo qual eles dependem de um meio técnico para sua existência, não podendo existir apenas no plano semântico[46]. Por outro lado, informações são elementos obtidos por meio do processo de interpretação dos dados, que leva em conta fatores externos para a atribuição de sentido, como o contexto social em que estão inseridos[47].

Apesar da clara diferença entre terminológica existente, o presente trabalho abordará ambos os conceitos como sinônimos, o que ocorre por dois motivos. Em primeiro lugar, enquanto lei de regência do tratamento de dados pessoais em solo brasileiro, a própria LGPD mescla os termos ao conceituar dado pessoal como

---

[43] GOMES, Josir Cardoso; PIMENTA, Ricardo Medeiros; SCHNEIDER, Marco André Feldman. Mineração de dados na pesquisa em ciência da informação: desafios e oportunidades. In: XX ENANCIB, 2019, Florianópolis. **Conference paper.** [S.L.]: Zenodo, 2019. p. 4-5. Disponível em: https://zenodo.org/record/3521038#.Y32eGnbMLIU. Acesso em: 10 out. 2022.

[44] DONEDA, 2020, p. 139.

[45] Ibid.

[46] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 82.

[47] Ibid.

"informação relacionada à pessoa natural identificada ou identificável"[48]. Ao fazer isso, é evidente que a legislação insere ambas as expressões dentro do regime de proteção de dados no ordenamento jurídico pátrio e, portanto, torna desnecessária a realização de uma análise própria para "dados" e "informações". Ademais, em segundo lugar, a análise do tratamento de dados pessoais no âmbito da implementação de um sistema de *Open Health* não requer a diferenciação entre os termos. É que se a diferença entre dados e informações está na interpretação e no sentido atribuído aos mesmos, torna-se nítido que ambos serão utilizados pelos integrantes do sistema de saúde suplementar para concretizar os objetivos do *Open Health* — mesmo que em diferentes momentos e para diferentes finalidades. Feitos estes breves esclarecimentos, passa-se à análise dos dispositivos de lei que tratam sobre os dados pessoais e dados pessoais sensíveis.

Em seu artigo 5º, a LGPD traz os conceitos de uma série de termos utilizados ao longo do texto legal, que servem como subsídio para permitir a correta compreensão dos dispositivos de lei e evitar interpretações equivocadas. Dentre os termos conceituados estão "banco de dados", "titular", "tratamento" e, por certo, "dados pessoais" e "dados pessoais sensíveis". Nesse contexto, a LGPD os conceitua da seguinte forma:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal 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;

De início, sobre o conceito de dado pessoal, é interessante pontuar que o legislador adota o viés expansionista como uma forma de caracterizar os tipos de informações que compõem o termo "dado pessoal"[49]. Isso significa dizer que o dado pessoal não é apenas toda a informação diretamente ligada à pessoa natural, mas também aquela informação que possa ser relacionada ao titular de dados pessoais — mesmo que indiretamente[50].

---

[48] Art. 5º, I da LGPD.
[49] VAINZOF, 2020, p. 82.
[50] Ibid.

De forma complementar, Danilo Doneda leciona que é necessário ter em mente a diferença entre dados “comuns” e dados pessoais, tendo em vista que, enquanto o primeiro representa uma categoria geral, o segundo mantém um vínculo direto e indissolúvel com a pessoa humana[51]. No mesmo sentido, Rony Vainzof entende que a característica indissociável ao dado pessoal é o seu componente de identidade em relação à pessoa natural. Essa identidade, por sua vez, representa o pressuposto de existência do dado pessoal, que extrapola o que “a pessoa realmente é, envolvendo também atributos, fatos, comportamentos e padrões”[52]

Alguns exemplos de dados pessoais com os quais lidamos diariamente são: nome, sobrenome, RG, CPF, título de eleitor, passaporte, data de nascimento, endereço residencial, conta de *e-mail*, informação de localização pelo GPS, renda, histórico de transações financeiras, entre tantos outros que fazem parte da vida cotidiana.

Dessa forma, percebe-se que dados corporativos, de pessoas jurídicas, não são classificados como dados pessoais por conta da ausência de relação de identidade com a pessoa física e, portanto, não estão sob proteção da LGPD. Assim, dados como balanços financeiros, planejamentos estratégicos, fórmulas e segredos de negócio são somente protegidos por diplomas legais como a Lei de Propriedade Industrial[53] e o Código Civil[54], mas não pela legislação de proteção de dados brasileira.

Além dos dados pessoais, a LGPD inclui em uma categoria especial aqueles que necessitam de tutela específica: os dados pessoais sensíveis. Em suma, dados pessoais sensíveis são as informações relacionadas à pessoa natural, identificada ou identificável, com o potencial de causar danos mais graves e críticos aos direitos fundamentais de seus titulares por meio da discriminação[55] — notadamente, os direitos à intimidade/vida privada[56] e à proteção de dados pessoais[57].

Diante das características particulares dos dados pessoais sensíveis, a LGPD impõe obrigações diferenciadas para o seu tratamento, como a existência de bases

---

[51] DONEDA, 2020, p. 146.
[52] VAINZOF, 2020, p. 83.
[53] Lei nº 9.279, de 14 de maio de 1996.
[54] Lei nº 10.406, de 10 de janeiro de 2002.
[55] VAINZOF, 2020, p. 85.
[56] Art. 5º, X da Constituição Federal de 1988.
[57] Art. 5º, LXXIX da Constituição Federal de 1988.

legais específicas[58], o seu compartilhamento entre controladores para se obter benefícios econômicos[59] e a necessidade de se elaborar relatório de impacto à proteção de dados pessoais[60]. Essas particularidades, previstas na LGPD como pressupostos para o tratamento de dados pessoais sensíveis, representam o nível mais elevado de rigor que a legislação confere a essa categoria de dado pessoal, tendo em vista o seu maior potencial lesivo aos titulares de dados pessoais em razão de uma especial vulnerabilidade: a discriminação[61].

Previstos de forma taxativa no artigo 5º, II da LGPD, os dados pessoais sensíveis são 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". Muito embora a LGPD não dê explicações detalhadas sobre o que seriam cada um desses tipos de dados pessoais sensíveis, a GDPR traz a definição de dados de saúde, genéticos e biométricos[62] — todos esses, inclusive, muito importantes para a análise do compartilhamento de dados no sistema de *Open Health*. De acordo com a legislação da União Europeia, dados de saúde são relacionados à condição física ou psicológica da pessoa natural, incluindo as informações obtidas em atendimentos médicos, que refletem a condição de saúde do titular de dados. Dados genéticos, por sua vez, representam dados relativos à herança genética de uma pessoa, que fornecem informações únicas sobre a sua fisiologia a partir da análise de sua amostra biológica. Por fim, dados biométricos correspondem aos dados que provêm uma identificação única da pessoa, como imagens faciais, padrão da íris ou impressões digitais.

Importante mencionar, contudo, que a caracterização de um dado pessoal como sensível pode não ser tão direta como parece. Muito embora o conceito de dados pessoais sensíveis trazido pela LGPD preveja um rol taxativo de opções, existe a possibilidade do tratamento de dados pessoais em grande volume resultar na obtenção de dados pessoais sensíveis sobre o titular pela via indireta. Sobre o

---

[58] Art. 11 da LGPD.

[59] Art. 11, §4º da LGPD.

[60] Art. 38, caput da LGPD.

[61] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021, p. 118.

[62] UNIÃO EUROPEIA. **Regulamento UE nº 2016/679**. Art. 4º, itens 13 à 15. Disponível em: https://gdpr-info.eu/art-4-gdpr/. Acesso em: 10 out. 2022.

assunto, Mario Viola e Chiara Teffé resumem a obtenção indireta de dados pessoais da seguinte forma:

> Dados que pareçam não relevantes em um momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela, conforme já observou o Bundesverfassungsgericht (Tribunal Constitucional Federal Alemão) no emblemático julgamento sobre a lei do censo de 1983[63].

Um exemplo desse cruzamento de dados é o que aconteceu em 2012 com a empresa Target, uma das maiores varejistas dos Estados Unidos da América, que descobriu a gravidez de uma cliente antes mesmo de sua família[64]. Isso ocorreu porque a empresa percebeu um padrão de consumo comumente praticado por mulheres em fase de gestação (loções sem essência, suplementos alimentares, sabonetes sem cheiro, etc) e começou a enviar promoções e ofertas para a casa da mulher, que eram direcionadas a "mamães" durante o seu período de gravidez. Isso chegou ao conhecimento do pai da cliente (agora avô da criança sendo gestada), que descobriu sobre a gravidez da filha antes mesmo de um anúncio oficial. No caso em tela, percebe-se que os dados pessoais não eram sensíveis, como o histórico de compra da cliente, mas o seu tratamento ocasionou o descobrimento de um dado relacionado à saúde, previsto na LGPD como um dado pessoal sensível e inserido em um regime legal diferenciado.

No mesmo sentido, outro exemplo da obtenção indireta de dados pessoais sensíveis por meio do tratamento de dados pessoais, é a verificação da opção religiosa de determinada pessoa através da análise de sua rotina. Na hipótese, poderiam ser cruzados (i) os dados de localização por GPS, determinando a quantidade de dias na semana e o tempo passado em uma sinagoga; (ii) os dados sobre aumentos da utilização do *smartphone* nas sextas-feiras em que deixa o trabalho para o *shabat*, período da semana sagrado para os judeus; e (iii) os dados

---

[63] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais da LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 194-195.

[64] TERRAÇO ECONÔMICO. **Big Data: Como a Target descobriu uma gravidez antes da família? O Guia Financeiro.** [S.L]. 18 fev. 2019. Disponível em: https://www.oguiafinanceiro.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/. Acesso em: 10 out. 2022.

de transações financeiras que demonstram a compra de produtos *kosher*, alimentos que obedecem a tradição judaica em sua forma de preparação. Todas essas informações, portanto, conduziriam à constatação de que a pessoa é adepta da religião judaica, de modo a revelar um dado pessoal sensível, a orientação religiosa, através de dados pessoais sem correlação direta a essa informação.

3.2.3 Hipóteses de tratamento de dados pessoais: as bases legais

Além do cumprimento aos princípios descritos no artigo 6º da LGPD, o tratamento de dados pessoais realizado em conformidade com o diploma de proteção de dados brasileiro também deve ser baseado em alguma das hipóteses legais, descritas nos artigos 7º e 11 da LGPD, que determinam os casos específicos em que um dado pessoal poderá ser objeto de atividades de tratamento.

Em matéria de dados pessoais, o artigo 7º da LGPD prevê que o seu tratamento somente poderá ser realizado se for enquadrado em alguma das dez hipóteses descritas. São elas:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

De início, cabe destacar que as hipóteses aqui previstas — assim como no artigo 11 — são taxativas, isto é, não permitem o tratamento de dados pessoais fundamentado em quaisquer outras possíveis bases legais, presentes ou não na LGPD. Mesmo que algumas bases legais sejam dotadas de maior grau de subjetividade, como o legítimo interesse[65], é fato que as atividades de tratamento de dados devem ser restritas a elas. Contudo, há quem entenda que a LGPD comportaria mais uma base legal, prevista no artigo 23, que possibilitaria o tratamento de dados pessoais para o cumprimento de atribuições legais pela Administração Pública. Apesar disso, Mario Viola e Chiara Teffé entendem que essa atividade de tratamento já estaria abarcada pelas hipóteses descritas nos artigos 7º, III e 11, II, "b" da LGPD, que autorizam o tratamento de dados pessoais para cumprimento de obrigação legal ou regulatória, motivo pelo qual criação de nova hipótese de tratamento seria desnecessária[66].

Apesar de não existir, ao menos com relação aos dados pessoais, hierarquia entre as hipóteses para tratamento de dados, uma base legal merece destaque pela sua relevância e aplicabilidade: o consentimento.

O consentimento é descrito pela LGPD como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[67]. A partir disso, o consentimento pode ser tido como um "instrumento de manifestação individual no campo dos direitos da personalidade", sendo a base legal que mais se relaciona com o conceito de autodeterminação informacional ao inserir o titular de dados no fluxo de tratamento de dados com o poder direto de escolha. De modo a apontar o consentimento como ferramenta essencial para a proteção de dados na sociedade da informação, Danilo Doneda leciona:

> O consentimento, nas matérias que envolvem diretamente a personalidade, assume hoje um caráter bastante específico. A evolução tecnológica é responsável por um crescimento das possibilidades de escolha que podem ter reflexos diretos para a personalidade, visto que várias configurações possíveis, referentes tanto à privacidade como à imagem, identidade pessoal, disposições sobre o próprio corpo e outras, dependem em alguma medida de uma manifestação da autonomia privada. O consentimento, ao sintetizar essa atuação da autonomia privada em um determinado momento, há de ser

[65] VIOLA; TEFFÉ, 2021, p. 195.
[66] Ibid.
[67] Art. 5º, XII da LGPD.

> interpretado de forma que seja o instrumento por excelência da manifestação da escolha individual, ao mesmo tempo em que faça referência direta aos valores fundamentais em questão.

Em consonância com as demais legislações de proteção de dados ao redor do mundo, a referida base legal dialoga com o conceito previsto na GDPR, que caracteriza o consentimento como a “manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”. Isso demonstra a importância da hipótese legal para tratamento de dados não apenas em nível nacional, mas também internacional.

Ademais, conforme já exposto anteriormente, a LGPD determina um padrão ainda mais rigoroso de proteção para que seja realizado o tratamento de dados pessoais sensíveis, que requer um cuidado mais intenso por parte dos agentes de tratamento em razão do seu maior potencial lesivo aos titulares de dados por conta do possível viés discriminatório. Nesse sentido, a LGPD prevê que o tratamento dessa espécie de dados pessoais poderá ser realizado de forma exclusiva nas seguintes hipóteses:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Dessa forma, percebe-se que o tratamento de dados sensíveis é possível e, em muitas circunstâncias, é necessário — é o exemplo do tratamento de dados de saúde em procedimentos realizados por médicos ou hospitais. Entretanto, é imprescindível que as atividades de tratamento sejam pautadas nos ditames legais previsto na LGPD, tendo em vista a sensibilidade dessa espécie de dados pessoais sob a ótica dos direitos e liberdades fundamentais, e que não sejam utilizadas para fins discriminatórios ou abusivos, o que é reforçado pelo princípio da não discriminação[68].

[68] Art. 6º, IX da LGPD.

4 A IMPLEMENTAÇÃO DE UM SISTEMA DE *OPEN HEALTH* NO BRASIL: LIMITES LEGAIS E DESAFIOS

De acordo com o banco de dados e indicadores da Agência Nacional de Saúde Suplementar (ANS)[69], o número de beneficiários dos planos privados de saúde era de 50.199.241 brasileiros e brasileiras em setembro de 2022. O número, que representa aproximadamente 25% da população brasileira, demonstra a extrema relevância do sistema de saúde suplementar para que milhões de cidadãos brasileiros tenham acesso a serviços médicos e odontológicos sem sobrecarregar a estrutura da saúde pública, de modo a concretizar o direito fundamental à saúde, de ordem social, previsto no artigo 6º e detalhado no artigo 196 da Constituição Federal de 1988.

Nesse contexto, percebe-se que a implementação de um sistema de *Open Health* simboliza um medida de indiscutível relevância aos direitos dos atores envolvidos no sistema de saúde suplementar (beneficiários, OPS, médicos, hospitais, etc), sendo que o seu impacto não pode passar despercebido, em especial aos direitos fundamentais à proteção de dados pessoais e à privacidade. A respeito disso, entendem Gabrielle Sarlet, Márcia Fernandes e Regina Ruaro[70]:

> São essenciais à área da saúde a preservação e a proteção de dados pessoais de indivíduos, grupos e populações, por isso os sistemas de informação e tecnologias que coletem, armazenem e utilizem dados e informações na área da saúde devem ser organizados para assegurar direitos e deveres dos cidadãos. O registro, o armazenamento, o tratamento e a preservação de dados e informações pessoais impõem cuidados e sistematização, apesar da necessidade do uso de dados pessoais de indivíduos ou de grupos para o aprimoramento na assistência à saúde, assim como à pesquisa.

Dessa forma, o presente capítulo buscará resgatar e conectar os assuntos tratados nos capítulos anteriores para que se promova a análise da implementação de um sistema de *Open Health* na saúde suplementar sob a ótica da Lei Geral de

---

[69] BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. **Dados e indicadores do setor**. Disponível em: <https://www.gov.br/ans/pt-br/acesso-a-informacao/perfil-do-setor/dados-e-indicadores-do-setor>. Acesso em: 10 out. 2022.

[70] RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales; FERNANDES, Márcia Santana. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 752.

Proteção de Dados (LGPD), vista como a norma jurídica mais relevante para a doutrina da proteção de dados brasileira.

Nesse sentido, em uma primeira análise, serão feitas considerações sobre as limitações legais ao tratamento de dados pessoais no âmbito de um sistema de *Open Health*, tendo especial enfoque nos dados de saúde. Ato seguinte, em uma segunda análise, serão abordados os principais desafios vislumbrados na construção de um sistema de dados abertos na saúde suplementar, assim como possíveis soluções para a resolução desses impasses.

4.1 LIMITES LEGAIS E CONSIDERAÇÕES SOBRE O COMPARTILHAMENTO DE DADOS PESSOAIS COM OS ATORES DA SAÚDE SUPLEMENTAR

Conforme exposto anteriormente, o tratamento de dados pessoais realizado em conformidade com a LGPD deve observar requisitos específicos, mais rigorosos, quando versar sobre dados pessoais sensíveis, que correspondem às informações relacionadas à origem racial ou étnica, convicção religiosa, opinião política, saúde ou vida sexual, entre outras. De acordo com Márcio Cots e Ricardo Oliveira, essa espécie de dado pessoal recebe o adjetivo “sensível” porque diz respeito a informações que “mergulham ainda mais na privacidade do ser humano, alcançando sua intimidade”[71], o que justifica a maior proteção do ordenamento jurídico brasileiro às atividades de tratamento que os envolvem.

Nesse sentido, diante de peculiaridade dos dados pessoais sensíveis, serão analisados, abaixo, os principais contornos jurídicos relacionados à implementação de um sistema de *Open Health* sob a ótica da LGPD, tendo enfoque nas hipóteses legais que justificam, ou não, o tratamento desses dados e na vedação à prática de seleção de riscos nos planos de saúde.

4.1.1 Bases legais aplicáveis

De acordo com o apresentado no capítulo anterior, o tratamento de dados pessoais só pode ocorrer se for enquadrado em alguma das hipóteses previstas nos

[71] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados comentada**. São Paulo: Thomson Reuters, 2018.

artigos 7º ou 11 da LGPD, que se referem aos dados pessoais e dados pessoais sensíveis, respectivamente. Apesar de existirem semelhanças entre as bases legais previstas nos dispositivos de lei, é notório que as hipóteses de tratamento direcionadas aos dados pessoais sensíveis são muito mais restritivas, tendo em vista o seu potencial de causar danos mais críticos à intimidade humana.

Uma demonstração desse maior grau de rigor é a impossibilidade de utilização do interesse legítimo do controlador ou de terceiro, previsto no artigo 7º, IX da LGPD, como base legal para autorizar o tratamento de dados pessoais sensíveis. Segundo Viola e Teffé, o legítimo interesse é a base legal com o maior grau de flexibilidade e discricionariedade na sua utilização[72], que pode ser aplicada a qualquer operação de tratamento de dados, desde que seja realizada em conformidade com a Lei e não implique em restrição aos direitos e garantias fundamentais do titular de dados pessoais. Nesse sentido, a hipótese de tratamento pode ser conceituada da seguinte forma:

> O legítimo interesse é a hipótese legal que visa a possibilitar tratamentos de dados importantes, vinculados ao escopo de atividades praticadas pelo controlador, e que encontrem justificativa legítima. Diante da flexibilidade dessa base legal, as expectativas do titular dos dados têm peso especialmente relevante para sua aplicação, devendo ser consideradas também a finalidade, a necessidade e a proporcionalidade da utilização dos dados. Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse[73].

Sendo assim, no lugar do legítimo interesse, a LGPD incluiu a base legal do artigo 11, II, “g”, que possibilita o tratamento de dados pessoais sensíveis para a “prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos”. Esse seria o caso de uma empresa que trata os dados biométricos de seus colaboradores, considerados dados pessoais sensíveis, sem o consentimento prévio dos titulares de dados, com o intuito de controlar e permitir o acesso a áreas restritas[74]. Ainda, pode-se citar o caso de uma operadora de planos de saúde que exige do segurado que coloque o seu dedo polegar

[72] VIOLA; TEFFÉ, 2021, p. 201.
[73] Ibid.
[74] VIOLA; TEFFÉ, 2021, p. 215.

em um leitor biométrico para evitar com que terceiros, não cobertos pelo seguro de saúde, utilizem o benefício em seu lugar[75].

Nessa circunstância, nota-se que a sistemática de proteção aos dados pessoais no ordenamento jurídico brasileiro confere mais atenção aos dados pessoais sensíveis, o que se justifica pela característica delicada das informações envolvidas. Feitos esses breves esclarecimentos sobre as particularidades das bases legais para tratamento de dados sensíveis, passa-se à análise daquelas possivelmente aplicáveis ao tratamento de dados pessoais sensíveis relacionados à saúde no contexto da implementação de um sistema de *Open Health* na saúde suplementar.

Ao analisarem as bases legais possivelmente cabíveis ao compartilhamento de dados pessoais sensíveis entre OPS, Juliano Maranhão e Ricardo Campos citam duas em específico: (i) o cumprimento de obrigação legal ou regulatória pelo controlador e (ii) o consentimento específico e destacado do titular de dados, conferido para finalidades específicas[76].

Inicialmente, o compartilhamento de dados de saúde entre OPS para o cumprimento de obrigação legal ou regulatória pelo controlador é limitado. A sua utilização se restringe ao estritamente necessário para: a verificação de elegibilidade, a autorização de procedimentos, a comunicação de internação ou alta do beneficiário, a cobrança de serviços de saúde, os demonstrativos de retorno, o envio e recebimento de documentos necessários para solicitação, a autorização e cobrança, o recurso de glosa e o comprovante de comparecimento[77]. Isso demonstra que essa hipótese de tratamento de dados pessoais é aplicável apenas em casos específicos e, portanto, não serviria ao propósito de um compartilhamento em larga escala previsto em um sistema de *Open Health*.

Diante do exposto, Maranhão e Campos entendem que a única base legal possivelmente aplicável ao compartilhamento de dados pessoais entre seguradoras de saúde, conforme a proposta de *Open Health* veiculada pelo Ministério da Saúde, seria a obtenção do consentimento dos titulares de dados.

---

[75] Ibid.

[76] CAMPOS, Ricardo; MARANHÃO, Juliano. **Estudo: compartilhamento de dados de saúde**. São Paulo: Instituto Legal Grounds, 2022b. p. 104-105.

[77] CAMPOS; MARANHÃO, 2022b. p. 96.

> Se a noção de Open Health no programa anunciado na imprensa estiver baseada na troca direta de informações entre seguradoras de saúde, independentemente de consentimento dos titulares, então eventual legislação que introduza tal permissão certamente será questionável frente ao direito fundamental constitucional de proteção aos dados pessoais, cf. LXXIX do art. 5o da CF88 (introduzido pela EC 115/2022). O Open Health somente seria admissível, em termos de portabilidade dos dados por manifestação de vontade do titular dos dados[78].

O consentimento, conforme o artigo 5º, XII da LGPD, é uma manifestação de vontade "livre, informada e inequívoca" por meio da qual o titular concorda com o tratamento de seus dados pessoais para finalidades específicas e determinadas. "Livre" significa que o titular de dados pode escolher entre aceitar ou recusar a realização de determinada atividade de tratamento[79], sendo que esse poder de "barganha" deve ser exercido sem interferência, sob pena do tratamento de dados ser considerado ilegal em razão de vício de consentimento[80]. Por sua vez, "informado" quer dizer que o titular tem ao seu dispor as "informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados"[81], o que dialoga com o princípio do livre acesso e da transparência para que o direito à autodeterminação informacional seja concretizado. Por fim, "inequívoca" diz respeito à necessidade de que o consentimento seja prestado de forma objetiva, clara e não ambígua[82].

Ademais, cabe destacar que o consentimento, enquanto manifestação de vontade, deve constar em "cláusula destacada das demais cláusulas contratuais"[83], no caso de ser coletado por escrito, e que seja o ônus do controlador[84] a comprovação de que o consentimento foi obtido em conformidade com a LGPD. Ainda, é facultado ao titular de dados a revogação do seu consentimento, conforme a disposição do artigo 8º, §5º da LGPD, de modo a potencializar a ideia de autonomia informacional a que devem estar submetidas todas as pessoas naturais que têm os seus dados pessoais parte de alguma atividade de tratamento.

---

78 Ibid.
79 VIOLA; TEFFÉ, 2021. p. 197-198
80 Art. 8º, §3º da LGPD.
81 VIOLA; TEFFÉ, 2021. p. 198.
82 VIOLA; TEFFÉ, 2021. p. 199.
83 Art. 8º, §1º da LGPD.
84 Art. 8º, §2º da LGPD.

Vale pontuar que essas várias qualificadoras atribuídas ao consentimento demonstram a importância conferida pelo legislador a essa base legal, mas também geram a chamada “hipertrofia do consentimento” a partir da extrema dificuldade em se obter o consentimento válido. É o que leciona Bruno Bioni[85]:

> Essa espécie de “hipertrofia do consentimento” gera implicações normativas das mais importantes. Ao mesmo tempo que se procura programar um consentimento extremamente qualificado, corre-se o risco de, paradoxalmente, limitar o terreno por ele ocupado. Isso porque a barra pode vir a ser tão elevada a ponto de ser exponencial o risco de o consentimento ser considerado inválido [...].

Essa robustez normativa conferida ao consentimento, é claro, não retira a importância do consentimento como hipótese legal de altíssima relevância para o cenário de proteção de dados brasileiro.

Ante o exposto, entende-se que a implementação de um sistema de *Open Health*, de acordo com a proposta do Ministério da Saúde, possui o consentimento — descrito no artigo 11, I da LGPD — como a única base legal autorizadora do tratamento dos dados pessoais sensíveis relacionados à saúde. Nesse contexto, a formatação de um sistema de dados abertos de saúde, necessariamente, implicará em um pensamento centrado no consentimento do titular.

4.1.2 Vedação à prática da seleção de riscos

Além de prever bases legais específicas para o tratamento de dados pessoais sensíveis, a Lei Geral de Proteção de Dados (LGPD) também possui diversos mecanismos legais para evitar com que o tratamento de dados pessoais sensíveis referentes à saúde seja realizado de forma discriminatória, segregatória ou desrespeitosa aos direitos e garantias fundamentais positivados no ordenamento jurídico brasileiro.

De acordo com a proposta de instituição do *Open Health* na saúde suplementar, veiculada pelo Ministério da Saúde, é dito que o sistema corresponderia à centralização dos dados de saúde em um banco de informações mantido pelo

[85] BIONI, Bruno. O consentimento como processo: em busca do consentimento válido. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 245.

governo, que seriam compartilhados entre os atores do sistema de saúde suplementar para (i) aumentar a concorrência, (ii) facilitar a portabilidade e (iii) reduzir custos. Apesar disso, é necessário observar que o tratamento de dados pessoais no contexto do *Open Health* deve seguir uma série de requisitos previstos na LGPD, específicos aos dados de saúde, para que esteja em conformidade com a sistemática de proteção de dados brasileira.

De início, o compartilhamento de dados em um sistema *Open Health* deve observar o princípio da não discriminação, que prevê a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Em síntese, o princípio serve como norteador ao tratamento de dados pessoais em geral, não apenas aos dados pessoais sensíveis de saúde, visando impor limites e permissões no processamento de dados para evitar com que essas informações sejam utilizadas contra os titulares.

Ademais, o artigo 11, §5º da LGPD determina que as operadoras de planos privados de saúde não podem realizar o "tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários". No mesmo sentido, o artigo 11, §4º da Lei também veda o compartilhamento de dados pessoais de saúde para se obter vantagem econômica, exceto para (i) viabilizar a prestação de serviços na área da saúde, como assistência médica/odontológica/farmacêutica, (ii) permitir a portabilidade de dados quando requisitado pelo titular e (iii) realizar transações financeiras e administrativas resultantes da prestação de serviços na área da saúde.

Essas determinações legais estão em consonância com o entendimento da ANS, manifestado por meio da Súmula Normativa nº 27/2015, que estabelece a vedação à "prática de seleção de riscos pelas operadoras de planos de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde". A normativa se refere, de forma específica, à restrição à prática de seleção de riscos ao ingresso de beneficiários em razão da idade ou de serem portadores de deficiência.

Todos esses dispositivos legais funcionam como salvaguardas aos direitos fundamentais dos titulares em um contexto em que os dados pessoais sensíveis referentes à saúde revelam muito sobre a pessoa natural e podem ser, facilmente, utilizados para práticas discriminatórias ilícitas e/ou abusivas. Um exemplo prático do motivo pelo qual esses dispositivos existem é para evitar casos como o de uma

operadora de planos de saúde que exige que um homem homossexual pague um valor de mensalidade maior porque o "grupo" a que pertence, em razão de sua orientação sexual, teria, estatisticamente, maior probabilidade de contrair o vírus do HIV[86] e, dessa forma, poderia gerar mais despesas à seguradora. Outro exemplo foi dado pela própria ANS, por meio da Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES:

> Por outro lado, também é possível que essas informações sejam utilizadas de forma abusiva na gestão dos recursos humanos, seja pela negativa da contratação de mulheres grávidas e de candidatos cujo histórico médico aponte risco de absenteísmo, seja pela demissão de funcionários de maior risco de morbidade. Também há doenças estigmatizantes que submetem seus portadores à repulsa da sociedade como a AIDS, a tuberculose e a hanseníase. Os casos citados por Anne Wells Branscomb ilustram como as vidas de pessoas infectadas pelo HIV podem ser devastadas pela revelação pública de suas condições[87].

Assim sendo, entende-se que o tratamento de dados pessoais no âmbito de um sistema de *Open Health* na saúde suplementar deve respeitar integralmente as disposições da LGPD e, por utilizar dados de saúde, em especial as regras de não discriminação e vedação à seleção de riscos em planos de saúde. Nesse contexto, uma das possíveis soluções para evitar a ocorrência dessas práticas é fazer com que os órgãos com competência regulatória sobre a temática proponham diretrizes e normativas direcionadas a mitigar a existência de práticas discriminatórias no sistema de saúde suplementar diante da implementação do *Open Health* — tarefa, essa, que poderá ser compartilhada entre a ANS e a ANPD, tendo em vista as regras de competência concorrente previstas no artigo 55-J, XXIII da LGPD.

Por outro lado, contudo, pensa-se que a melhor alternativa seria a centralização da proposta de *Open Health* no paciente, de modo com que o vetor do compartilhamento de dados pessoais esteja focado nos pontos de atenção e cuidado com o beneficiário, e não na redução de custos ao consumidor, o que facilitaria muito

---

[86] MENDES, Laura Schertel; MATTIUZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 664

[87] BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. **Processo nº 33910.029786/2019-51, Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES**. Brasília, 2019. p. 5. Disponível em: https://www.sbac.org.br/wp-content/uploads/2019/12/Nota-Te%CC%81cnica-sobre-LGPD.pdf. Acesso em: 10 out. 2022.

as práticas discriminatórias. É o que entendem Maranhão e Campos[88] ao dizerem que essa solução possuiria duas vantagens ao (i) fazer com que o sistema de dados abertos na saúde suplementar seja focado no bem-estar do paciente, o que, por consequência, diminuiria os custos com a promoção de soluções contínuas de tratamento e (ii) assegurar os direitos fundamentais à privacidade e à proteção de dados por meio da restrição ao acesso desses dados pessoais de saúde àqueles que efetivamente necessitarem.

4.2 DESAFIOS

Além dos limites legais impostos pela LGPD, que devem ser observados de forma compulsória pelos agentes de tratamento de dados e levados em conta no momento da formatação de um sistema de dados abertos de saúde, a proposta de implementação de um sistema de *Open Health* na saúde suplementar também demonstra a existência de desafios a serem superados.

4.2.1 Guarda de dados pelo governo

Um dos desafios observados, que merece especial destaque no presente estudo, é a forma de armazenamento de dados pessoais prevista na proposta de implementação do *Open Health*. Na declaração do Ministério da Saúde, é dito que os dados de saúde dos brasileiros farão parte de um banco chamado de “Rede Nacional de Dados em Saúde (RNDS)”, que representaria uma espécie de prontuário eletrônico com as informações médicas do usuário. Ainda, esse repositório de dados seria acessado pelas OPS, que veriam, de forma anônima, o perfil dos usuários e informações como o histórico de inadimplência, as características do seu contrato e o quanto pagam, o que auxiliaria na migração entre planos do ponto de vista da portabilidade de dados. De acordo com Marcelo Queiroga, a proteção dos dados e a privacidade dos consumidores seria garantida, visto que estariam “preservados e sob a guarda do Estado — não do médico ou dos planos de saúde”[89].

[88] CAMPOS; MARANHÃO, 2022b, p. 94.
[89] QUEIROGA, 2022.

Apesar disso, a guarda de dados pessoais, de forma centralizada, nas mãos do Estado, preocupa. Segundo Maranhão e Campos, o risco de vazamento de dados, já presente em qualquer operação de tratamento, seria muito mais acentuado no caso da centralização dos dados pessoais de saúde em uma base específica[90]. Essa concentração de informações, inclusive, vai na contramão da ideia de interoperabilidade, que diversos países vêm desenvolvendo como estratégia para garantir o compartilhamento de dados de forma mais segura[91]. É que, com a aplicação do conceito de interoperabilidade e a retirada do Estado enquanto intermediador na relação de compartilhamento de dados pessoais, a tendência é que os riscos de possíveis vazamentos de dados e incidentes de segurança sejam minimizados. Nas palavras de Maranhão e Campos, a unidade informacional nas mãos do Estado "não se justifica sob o prisma de necessidade, uma vez que os objetivos podem ser alcançados com a interoperabilidade no acesso padronizado aos dados descentralizados por estabelecimentos e profissionais de saúde"[92].

Ademais, o histórico de vulnerabilidades dos sistemas informacionais do governo brasileiro não passa credibilidade. Um exemplo disso foi o ataque *hacker* à plataforma "ConecteSUS", que fez com que o sistema ficasse indisponível por 13 dias e mantivesse os dados pessoais sensíveis relacionados aos certificados de vacinação contra a Covid-19 inacessíveis durante todo o período[93]. Outro caso emblemático foi o vazamento de dados pessoais de mais de 200 milhões de brasileiros, o que ocorreu por conta da exposição indevida de informações de acesso aos sistemas do Ministério da Saúde, que armazenam dados cadastrais como nome completo, número de CPF e endereço dos cidadãos[94].

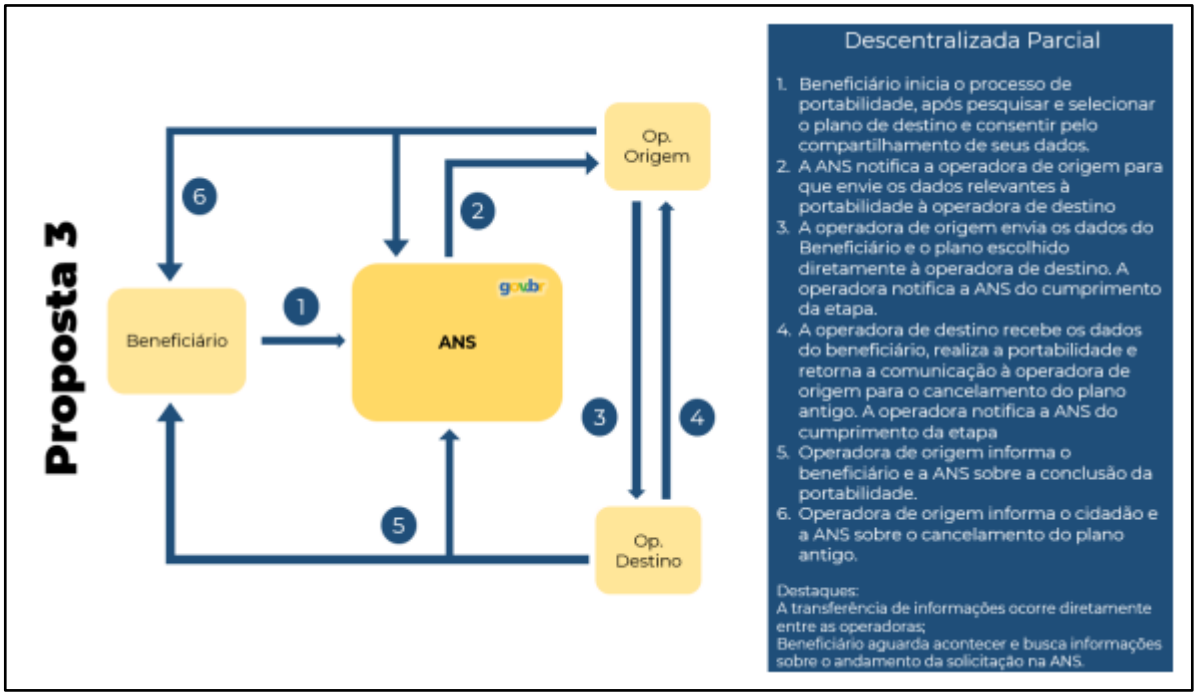
Nesse sentido, um possível recurso para evitar a centralização no contexto do *Open Health* é, justamente, alterar a dinâmica de compartilhamento de dados pessoais prevista na proposta do Ministério da Saúde, de modo a fazer com que o governo deixe de ter responsabilidade direta sobre a guarda dessas informações e as

[90] CAMPOS; MARANHÃO, 2022a.
[91] Ibid.
[92] CAMPOS; MARANHÃO, 2022b, p. 96.
[93] ROSA, Ana Beatriz Rezende; MACIEL, Caroline Stéphanie; NUNES, Oto Barbosa. O apagão do ConecteSUS e a vulnerabilidade do tratamento de dados no Brasil. **Jota**. São Paulo, 12 jan. 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/conectesus-apagao-vulnerabilidade-tratamento-de-dados-12012022/. Acesso em: 10 out. 2022.
[94] Ibid.

OPS passem a ter mais autonomia sobre a gestão desses dados pessoais. É o que se verifica no caso do *Open Finance* e do *Open Insurance*, em que as empresas promovem o compartilhamento de dados pessoais entre si por meio de APIs, sem necessitar da interferência de um terceiro elemento — no caso, o Estado — para viabilizá-lo.

De forma complementar, o Ministério da Saúde criou um grupo de trabalho por meio da Portaria GM/MS nº 392, de 23 de fevereiro de 2022, tendo o objetivo de elaborar uma "proposta de aprimoramento do setor de saúde suplementar, mediante compartilhamento de dados de usuários e provedores de serviços de saúde". No relatório final do grupo[95], foram apresentadas três possíveis estruturas de compartilhamento de dados pessoais, sendo que a figura a seguir demonstra a que mais se aproxima da ideia de descentralização apresentada no presente trabalho.

Figura 3 - Proposta de compartilhamento de dados de forma descentralizada



Fonte: Relatório final do grupo de trabalho instituído pelo Ministério da Saúde

[95] BRASIL. MINISTÉRIO DA SAÚDE. **Relatório Final do Grupo de Trabalho**: aprimoramento do setor de saúde suplementar - mediante compartilhamento de dados de usuários e provedores de serviços de saúde. 2022. Disponível em: https://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/relatorios/2022/relatorio-final-do-grupo-de-trabalho/view. Acesso em: 10 out. 2022.

Em conclusão, o grupo de trabalho entendeu que a proposta representaria um aumento de custos para as OPS e para a ANS, além de demandar um maior prazo para implementação. Por esse motivo, em apertada decisão (354 a 356), o grupo de trabalho optou por uma proposta com o compartilhamento de dados pessoais em regime de centralização parcial, tendo a ANS como intermediária na comunicação entre beneficiários e planos de saúde em todas as hipóteses.

Figura 4 - Resultado da análise multicritério entre as três alternativas

Resumo AIR Intermediário

CRITÉRIOS PARA A ANÁLISE INTERMEDIÁRIA	PONTUAÇÃO GERAL			DEM PARA SELEÇÃO POR VALORES (CRESCEN			CRITÉRIOS PARA A ANÁLISE INTERMEDIÁRIA
	Proposta 1	Proposta 2	Proposta 3	Proposta 1	Proposta 2	Proposta 3	
1. EFICIÊNCIA	55	50	45	1	2	3	1. EFICIÊNCIA
2. EFETIVIDADE	90	90	90	1	1	1	2. EFETIVIDADE
3. EQUIDADE	83	83	83	1	1	1	3. EQUIDADE
4. TRANSPARÊNCIA	84	73	79	1	3	2	4. TRANSPARÊNCIA
5. RAZOABILIDADE	43	30	57	2	3	1	5. RAZOABILIDADE
TOTAL GERAL	356	326	354				
MÉDIA GERAL	71	65	71				
% DA PONTUAÇÃO MÁXIMA	79,10%	72,49%	78,57%				
ORDEM PARA SELEÇÃO GERAL DAS ALTERNATIVAS (CRESCENTE)	1	3	2				

Fonte: Relatório final do grupo de trabalho instituído pelo Ministério da Saúde

Sendo assim, pensa-se que o compartilhamento de dados pessoais, pilar de um sistema de dados abertos de saúde, deve ser visto sob a lente da proteção de dados pessoais em quaisquer hipóteses. A descentralização de bases de dados, nesse sentido, pode servir como uma ferramenta para diminuir os riscos existentes nas atividades de tratamento de dados, limitar o compartilhamento de dados entre apenas os atores necessários e aproximar a proposta de *Open Health* aos princípios descritos na LGPD, tendo especial enfoque nos princípios da segurança e da prevenção.

4.2.2 Segurança e digitalização do sistema de saúde

Outro desafio observado a partir da implementação de um sistema de *Open Health* no país é a ausência de mecanismos de segurança para a proteção de dados pessoais e da prática de digitalização no sistema de saúde brasileiro. De acordo com

a “Pesquisa TIC Saúde 2021”[96], promovida pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), houve um crescimento expressivo no uso de tecnologias e sistemas informacionais por parte dos estabelecimentos de saúde desde a pandemia de Covid-19 — 94% deles possuem ao menos um computador e acesso à internet[97].

Apesar do amplo acesso à rede global de computadores, a falta de digitalização ainda representa um desafio a ser superado. De acordo com o estudo, 88% dos estabelecimentos possuem sistemas eletrônicos para registro de dados dos pacientes, mas apenas 49% afirmam realizar a manutenção de informações nos prontuários eletrônicos[98]. Esses dados demonstram que ainda há um longo caminho a ser trilhado para que a implementação de um sistema de *Open Health* possa beneficiar a todos as pessoas incluídas no sistema de saúde suplementar.

Dessa forma, um possível recurso para evitar o desabastecimento das bases de dados seria a implementação de políticas públicas que prevejam a utilização de sistemas eletrônicos como mandatária aos atores do sistema de saúde suplementar. Assim, a iniciativa teria o fito de promover a concentração dos dados pessoais de saúde no ambiente virtual, de modo que a instituição de um sistema de *Open Health* seja, efetivamente, possível em um cenário no qual a interoperabilidade entre sistemas pode ser viabilizada. Inclusive, entende-se que uma forma inteligente de fomentar a adoção dos sistemas informacionais seria o conferimento de incentivos fiscais às entidades que cumprirem metas de digitalização estabelecidas por lei ou outro ato de caráter normativo.

Não obstante, outro aspecto importante sobre o estudo realizado pelo Cetic.br é a quantidade de estabelecimentos de saúde que realizam alguma medida para buscar a adequação à LGPD. Conforme a pesquisa, apenas 38% disponibilizam canais de atendimento e interação com os titulares dos dados e 32% realizam campanhas internas de conscientização sobre o tema[99], o que demonstra a baixíssima

[96] NASCIMENTO, Ana. Uso de tecnologias digitais avança nos estabelecimentos de saúde brasileiros, mas a segurança da informação segue sendo desafio, aponta pesquisa TIC Saúde 2021. **Cetic.Br.** Brasil, 24 nov. 2021. Disponível em: https://cetic.br/pt/noticia/uso-de-tecnologias-digitais-avanca-nos-estabelecimentos-de-saude-brasileiros-mas-a-seguranca-da-informacao-segue-sendo-desafio-aponta-pesquisa-tic-saude-2021/. Acesso em: 10 out. 2022.

[97] Ibid.

[98] Ibid.

[99] Ibid.

adesão do sistema de saúde às diretrizes previstas na lei de proteção de dados brasileira e outra importante barreira a ser ultrapassada para que seja possível a implementação de um sistema de dados abertos na saúde suplementar que assegure a proteção aos dados pessoais — em específico, os considerados sensíveis por serem relacionados à saúde.

4.2.3 Forma de instituição

Por fim, outro ponto importante sobre a proposta de implementação do *Open Health* diz respeito à sua forma de instituição. De acordo com o pronunciamento do ministro da Saúde, o sistema de dados abertos de saúde seria instituído por uma medida provisória que descreveria as regras e medidas a serem adotadas pelos atores públicos e privados inseridos no sistema de saúde suplementar, como as OPS, a ANS e o próprio Ministério da Saúde.

Prevista no ordenamento jurídico brasileiro por meio do artigo 62 da Constituição Federal de 1988, a medida provisória consiste em um instrumento utilizado pelo Presidente da República para editar normas com força de lei em situações de urgência e relevância, que produzem efeitos imediatos, mas precisam passar pela aprovação do Congresso Nacional para serem efetivadas como leis ordinárias. De acordo com Pedro Lenza, a medida provisória consiste em "ato monocrático, unipessoal, sem a participação do Legislativo, chamado a discuti-la somente em momento posterior, quando já adotada pelo Executivo, com força de lei e produzindo os seus efeitos jurídicos"[100].

A intenção de se instituir o *Open Health* por meio de medida provisória, contudo, causa estranheza, porque o instituto pressupõe a existência de situação urgente, que não possa aguardar o período de tramitação de um projeto de lei para ser positivada no ordenamento jurídico — o que não parece ser o caso em tela. Como exemplo recente de correta aplicação do instituto, é possível citar a MP 1.026/2021, que instituiu o Plano Nacional de Vacinação contra a Covid-19 e previu a adoção de regras mais flexíveis nas contratações públicas envolvendo insumos para o combate ao vírus em um contexto de urgência e relevância social.

[100] LENZA, Pedro. **Direito constitucional esquematizado**. 23. ed. São Paulo: Saraiva Educação, 2019. p. 1078.

Ademais, a ausência de participação da sociedade e diálogo com os sujeitos envolvidos[101] também não faria jus à complexidade e à sensibilidade do tema, que afetaria milhões de cidadãos brasileiros inseridos no sistema de saúde suplementar. Conforme exposto anteriormente, todos os outros sistemas *Open* implementados no Brasil foram acompanhados de amplo debate com os setores da sociedade diretamente afetados, tendo em vista a multiplicidade de implicações possivelmente causadas aos atores envolvidos, o que chama ainda mais a atenção para a forma de instituição do *Open Health* ventilada pelo ministro de Saúde.

Inclusive, a falta de escuta e inclusão da sociedade civil no debate sobre o compartilhamento de dados repercutiu dentre os próprios órgãos governamentais envolvidos no ecossistema de saúde. Por meio da Recomendação nº 002, de 04 de fevereiro de 2022, o Conselho Nacional de Saúde (CNS) sugeriu que a implementação do *Open Health* seja precedida de ampla discussão e debate público, com a participação da sociedade civil e de entidades representativas dos planos de saúde.

De acordo com o CNS, apesar das semelhanças superficiais com o *Open Finance* e o *Open Insurance*, os dados de saúde estão distribuídos por diversos sistemas de informação, públicos e privados, o que implicaria na necessidade de um estudo aprofundado sobre a logística de interoperabilidade entre esses bancos de dados. Ademais, também chamou a atenção para a sensibilidade dos dados pessoais de saúde, incluídos pelo artigo 5º, II da LGPD como dados sensíveis, e para os graves incidentes de segurança vivenciados pelo Ministério da Saúde durante a pandemia de coronavírus — como ocorreu com a plataforma "ConecteSUS"[102]. Todos esses argumentos, levantados pelo CNS em sua Recomendação nº 002/2022, convergem para a necessidade do amadurecimento da proposta antes de sua edição, sendo que "medida desse calibre não deve, em hipótese alguma, tramitar por meio de Medida Provisória".

A rejeição de diversos setores da sociedade à instituição do *Open Health* sem um prévio debate e discussão sobre os seus moldes, contudo, alertou o Ministério da Saúde, que criou um grupo de trabalho para discutir a melhor forma de se implementar

[101] SADAMI, Arthur; HADDAD, Frederico; PONCE, Paula Pedigoni. Open Health: vícios da proposta e riscos regulatórios. **Jota.** São Paulo, 18 fev. 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/open-health-vicios-proposta-riscos-regulatorios-18022022>. Acesso em: 10 out. 2022.
[102] ROSA; MACIEL; NUNES, 2022.

um sistema de compartilhamento de dados pessoais no setor de saúde em consonância com o atual cenário regulatório brasileiro. Apesar disso, o grupo de trabalho resolve apenas parte do problema, tendo em vista que é composto por integrantes do Ministério da Saúde, da Agência Nacional de Saúde Suplementar, da Secretaria de Governo Digital do Ministério da Economia e do Banco Central, sem, portanto, contar com a participação mais ampla de outros atores do sistema de saúde, como entidades representativas da sociedade civil e das OPS.

Nessa perspectiva, entende-se que a criação de um sistema de *Open Health* deve ser antecedida por um amplo debate entre os envolvidos no sistema de saúde suplementar (beneficiários, OPS, médicos, hospitais, entre outros), sendo que, apesar da intenção ventilada pelo ministro Marcelo Queiroga, não se entende que a temática tenha a urgência e relevância necessárias para que seja instituída por medida provisória. Assim, uma possível solução seria que o Ministério da Saúde proponha a instituição do sistema de dados abertos na saúde suplementar por meio de um projeto de lei, que será submetido ao processo legislativo e todas as suas etapas, como a tramitação em comissões temáticas e a aprovação pelas duas câmaras do Congresso Nacional.

Na mesma linha, outra forma de democratizar o debate seria fazer com que o *Open Health* seja regulamentado de forma setorial pela ANS, o que tenderia a aproximar o debate sobre a instituição de um sistema de dados abertos na saúde suplementar aos efetivamente envolvidos. Em comparação direta, é o que ocorreu com o *Open Finance*, que foi instituído pela Resolução nº 01/2020, editada conjuntamente entre o Banco Central e o Conselho Monetário Nacional, mas não pelo Ministério da Economia.

Apesar disso, parece imperioso que, independentemente da sua forma de instituição, o *Open Health* seja objeto de consulta pública amplamente veiculada nos meios de comunicação (televisão, rádio e redes sociais), de modo que os beneficiários dos planos de saúde, que também são titulares de dados pessoais sensíveis no contexto analisado, possam opinar, debater e construir um sistema de dados abertos de saúde feito que respeite o interesse da maioria.

5 CONSIDERAÇÕES FINAIS

O presente trabalho propôs-se a analisar a proposta de instituição de um sistema de *Open Health* no setor de saúde suplementar brasileiro, ventilada pelo Ministério da Saúde, com base nas diretrizes previstas na Lei Geral de Proteção de Dados Pessoais (LGPD). Dessa forma, como objetivo final, se pretendeu indicar os limites jurídicos e as possibilidades normativas envolvendo a implementação do sistema de dados abertos na saúde suplementar, assim como potenciais desafios enfrentados e suas possíveis soluções.

No que diz respeito às bases legais para o tratamento de dados pessoais sensíveis, percebeu-se que o consentimento é a única hipótese prevista em lei capaz de autorizar o compartilhamento de informações entre as OPS no contexto do *Open Health* — não sendo aplicáveis nem a base legal do cumprimento de obrigação legal ou regulatória pelo controlador, nem a da tutela da saúde. Por sua vez, o consentimento deve ser qualificado, de modo que a manifestação de vontade do titular acerca do tratamento de dados pessoais deve ser livre, informada, inequívoca e direcionada a finalidades específicas para que esteja em conformidade com a LGPD.

Ademais, acerca das possíveis práticas discriminatórias e segregatórias envolvendo o tratamento de dados pessoais de saúde, verificou-se que a LGPD possui dispositivos legais direcionados a coibir as referidas atividades de tratamento, como o princípio da não discriminação e a vedação à seleção de riscos em planos de saúde. Apesar disso, chegou-se à conclusão de que uma forma de mitigar essas práticas seria promover a instituição de um *Open Health* focado na melhoria direta do atendimento ao paciente, e não na redução de custos ou no aumento da concorrência. Isso ocorreria por meio da redução dos atores da saúde suplementar, de modo com que apenas os estritamente necessários para atingir as finalidade do *Open Health* façam parte da dinâmica de tratamento de dados pessoais sensíveis relacionados à saúde.

Depreende-se, portanto, que a implementação de um sistema de *Open Health* no setor de saúde suplementar é possível e pode ser conciliada com as regras e diretrizes previstas na LGPD, mas não da forma como foi proposta pelo Ministério da Saúde. A proposta ainda carece de amadurecimento por meio do debate com a sociedade civil, além de precisar ser formatada com um olhar mais direcionado aos

direitos e garantias fundamentais, como o direito à privacidade e à proteção de dados, ambos assegurados pela Constituição Federal de 1988. No mesmo sentido, percebe-se que a carência de mecanismos de segurança capazes de salvaguardar os dados pessoais também deve ser observada ao se formatar um sistema *Open Health*, diante dos evidentes desafios de segurança da informação presentes na proposta.

Assim, espera-se que o bem-estar dos indivíduos inseridos no sistema de saúde suplementar e os benefícios econômicos inerentes ao sistema de dados abertos de saúde consiga ser conciliado e equilibrado para que o progresso seja atingido, mas de uma forma responsável e sustentável.

REFERÊNCIAS

ALEXY, Robert. **Derecho e razón prática**. México: Fontamara, 1993.

BANCO CENTRAL. **Open Finance Brasil**. Disponível em: https://openfinancebrasil.org.br/. Acesso em: 10 out. 2022.

BANQ. **Open Banking Directory and PSD2 API Tracker**. Disponível em: https://openbankingtracker.com/. Acesso em: 10 out. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. **Dados e indicadores do setor**. Disponível em: <https://www.gov.br/ans/pt-br/acesso-a-informacao/perfil-do-setor/dados-e-indicadores-do-setor>. Acesso em: 10 out. 2022.

BRASIL. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. **Processo nº 33910.029786/2019-51, Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES**. Brasília, 2019. p. 5. Disponível em: https://www.sbac.org.br/wp-content/uploads/2019/12/Nota-Te%CC%81cnica-sobre-LGPD.pdf. Acesso em: 10 out. 2022.

BRASIL. **Constituição da República Federativa do Brasil (1988)**. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 out. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9656.htm. Acesso em: 10 out. 2022.

BRASIL. **Lei nº 9.656, de 3 de junho de 1998**. Dispõe sobre os planos e seguros privados de assistência à saúde. Brasília: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9656.htm. Acesso em: 10 out. 2022.

BRASIL. **Medida Provisória nº 954/2020**. 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). Brasília: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 10 out. 2022.

BRASIL. MINISTÉRIO DA SAÚDE. **Relatório Final do Grupo de Trabalho**: aprimoramento do setor de saúde suplementar - mediante compartilhamento de dados de usuários e provedores de serviços de saúde. 2022. Disponível em: https://www.gov.br/saude/pt-br/centrais-de-

conteudo/publicacoes/relatorios/2022/relatorio-final-do-grupo-de-trabalho/view. Acesso em: 10 out. 2022.

BRASIL. **Proposta de Emenda Constitucional nº 17/2019**. Brasília: Senado Federal, 2019. Disponível em:https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline. Acesso em: 10 out. 2022.

CAMPOS, Ricardo; MARANHÃO, Juliano. Considerações sobre a construção de um open health no Brasil. **Jota**. São Paulo, 2 de setembro de 2022a. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/consideracoes-sobre-a-construcao-de-um-open-health-no-brasil-02092022>. Acesso em: 10 out. 2022.

CAMPOS, Ricardo; MARANHÃO, Juliano. **Estudo: compartilhamento de dados de saúde**. São Paulo: Instituto Legal Grounds, 2022b.

CARVALHO, Sérgio. Das 119 seguradoras autorizadas a operar no Brasil, apenas 10 detém 80% de todo o mercado. **Jornal Nacional dos Seguros.** São Paulo. out. 2019. Disponível em: https://genteseguradora.com.br/das-119-seguradoras-autorizadas-a-operar-no-brasil-apenas-10-detem-80-de-todo-o-mercado/. Acesso em: 10 out. 2022.

CAVALCANTE, Eric. O novo paradigma tecnológico do setor financeiro nacional: a implantação do *Open Banking* no Brasil. **Radar: tecnologia, produção e comércio exterior**, Brasília, vol. 66, p. 20, ago. 2021. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/10726/1/radar_n66.pdf. Acesso em: 10 out. 2022.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados comentada**. São Paulo: Thomson Reuters, 2018.

COUNTRYECONOMY.COM. **Dados econômicos e demográficos da União Europeia**. Disponível em: https://pt.countryeconomy.com/paises/grupos/uniao-europeia. Acesso em: 10 out. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed.São Paulo: Revista dos Tribunais, 2020.

EUR-LEX: ACCESS TO EUROPEAN UNION LAW. **Revised rules for payment services in the EU**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366. Acesso em: 10 out. 2022.

GOMES, Josir Cardoso; PIMENTA, Ricardo Medeiros; SCHNEIDER, Marco André Feldman. Mineração de dados na pesquisa em ciência da informação: desafios e oportunidades. In: XX ENANCIB, 2019, Florianópolis. **Conference paper.** [S.L.]: Zenodo, 2019. p. 4-5. Disponível em: https://zenodo.org/record/3521038#.Y32eGnbMLIU. Acesso em: 10 out. 2022.

GUIMARÃES, Olavo. Concorrência bancária e o *Open Banking* no Brasil. **Revista de defesa da concorrência**, Brasília, vol. 9, pg. 129, jun. 2021. Disponível em:

https://www.bnb.gov.br/s482-dspace/bitstream/123456789/880/1/2020_INET_01.pdf. Acesso em: 10 out. 2022.

IS DATA REALLY THE NEW OIL? **Kenway Consulting.** [S.L]. 10 ago. 2022. Disponível em: <https://www.kenwayconsulting.com/blog/data-is-the-new-oil/>. Acesso em: 10 out. 2022.

LENZA, Pedro. **Direito constitucional esquematizado**. 23. ed. São Paulo: Saraiva Educação, 2019.

MALDONADO, Viviane Nóbrega *et al* (org.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MENDES, Laura Schertel; MATTIUZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

NASCIMENTO, Ana. Uso de tecnologias digitais avança nos estabelecimentos de saúde brasileiros, mas a segurança da informação segue sendo desafio, aponta pesquisa TIC Saúde 2021. **Cetic.Br.** Brasil, 24 nov. 2021. Disponível em: https://cetic.br/pt/noticia/uso-de-tecnologias-digitais-avanca-nos-estabelecimentos-de-saude-brasileiros-mas-a-seguranca-da-informacao-segue-sendo-desafio-aponta-pesquisa-tic-saude-2021/. Acesso em: 10 out. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. **Onu News**. [S.L], 16 set. 2022. Disponível em: https://news.un.org/pt/story/2022/09/. Acesso em: 10 out. 2022.

QUEIROGA, Marcelo. “Open Health” é uma questão de tempo, coragem e decisão. **Folha de São Paulo**. São Paulo, 5 de março de 2022. Disponível em: https://www1.folha.uol.com.br/opiniao/2022/03/open-health-e-questao-de-tempo-coragem-e-decisao.shtml. Acesso em: 10 out. 2022.

ROSA, Ana Beatriz Rezende; MACIEL, Caroline Stéphanie; NUNES, Oto Barbosa. O apagão do ConecteSUS e a vulnerabilidade do tratamento de dados no Brasil. **Jota**. São Paulo, 12 jan. 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/conectesus-apagao-vulnerabilidade-tratamento-de-dados-12012022/. Acesso em: 10 out. 2022.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados - Lei 13.709/2018. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 305.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales; FERNANDES, Márcia Santana. A proteção de dados no setor de saúde em face do sistema normativo

brasileiro atual. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SADAMI, Arthur; HADDAD, Frederico; PONCE, Paula Pedigoni. Open Health: vícios da proposta e riscos regulatórios. **Jota.** São Paulo, 18 fev. 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/open-health-vicios-proposta-riscos-regulatorios-18022022>. Acesso em: 10 out. 2022.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. In: BIONI, Bruno *et al* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SILVA, Vitor Hugo. 81% da população brasileira acessou a internet em 2021, diz pesquisa. **G1**. São Paulo, 21 jun. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/06/21/81percent-da-populacao-brasileira-acessou-a-internet-em-2021-diz-pesquisa.ghtml. Acesso em: 10 out.2022.

TAVARES, Letícia Becker. O papel do Banco Central na implementação do *Open Finance* no Brasil. In: CRAVO, Daniela Copetti; JOBIM, Eduardo; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Direito público e tecnologia**. São Paulo: Editora Foco, 2022.

UNIÃO EUROPEIA. **Opinion 03/2013 on purpose limitation**. Bélgica, Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 10 out. 2022.

UNIÃO EUROPEIA. **Regulamento UE nº 2016/679**. Disponível em: https://gdpr-info.eu/. Acesso em: 10 out. 2022.

VAINZOF, Rony. Capítulo I: disposições preliminares. In: MALDONADO, Viviane Nóbrega *et al* (org.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.