VIRNA DE BARROS NUNES FIGUEIREDO

PROTEÇÃO À SAÚDE NO ORDENAMENTO JURÍDICO BRASILEIRO:

UMA ANÁLISE DA DIMENSÃO INFORMATIVA NO CENÁRIO DA LEI GERAL DE PROTEÇÃO DE DADOS

Biblioteca de Referência em Políticas Públicas

CEUB
EDUCAÇÃO SUPERIOR

FIGUEIREDO, Virna De Barros Nunes

Proteção à saúde no ordenamento jurídico brasileiro: uma análise da dimensão informativa no cenário da lei geral de proteção de dados

328 p.

ISBN: 978-85-7267-175-0

Tese apresentada à Banca do Programa Pós-Graduação Stricto Sensu em Direito do Centro Universitário de Brasília – UNICEUB, como requisito parcial para a obtenção do Grau de Doutora em Direito.

Orientador: Professora Doutora Liziane Paixão Silva Oliveira.

Lista de abreviaturas e siglas

ABREVIATURAS	
c/c	Com Cópia
n.	Número
art.	Artigo
§	Parágrafo
sic	desta forma
SIGLAS	
ABRAMED	Associação Brasileira de Medicina Diagnóstica
ANATEL	Agência Nacional de Telecomunicações
ANEEL	Agência Nacional de Energia Elétrica
ANPD	Autoridade Nacional de Proteção de Dados
ANS	Agência Nacional de Saúde Suplementar
CADSUS	Cadastro Nacional de Usuários do SUS
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CE	Conselho Europeu
CEP	Código de Endereçamento Postal
CEPD	Comissão Europeia de Proteção de Dados
CFTV	Circuito Fechado de Televisão
CEM	Código de Ética Médica
CFM	Conselho Federal de Medicina
CGSD	Comitê Gestor de Saúde Digital
CIT	Comissão Intergestores Tripartite do Sistema Único de Saúde
CNES	Cadastro Nacional dos Estabelecimentos de Saúde
CNS	Conselho Nacional de Saúde
CPF	Cadastro de Pessoa Física
DATASUS	Departamento de Informática do SUS
DNA	Ácido Desoxirribonucleico
DOU	Diário Oficial da União
DPO	Data Protection Officer
DUDH	Declaração Universal dos Direitos Humanos
DUDH	Declaração Universal de Direitos Humanos
EDPB	European Data Protection Board
ESD17	Estratégia de Saúde Digital para o Brasil 2017
ESD28	Estratégia de Saúde Digital para o Brasil 2020-2028
EU	União Europeia
HIV	Vírus da Imunodeficiência Humana
IBM	International Business Machines

IMDB	Internet Movies Databases
INTI	Instituto Nacional De Tecnologia Da Informação
IoT	Internet das Coisas (Internet of Things)
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
M&A	Monitoramento e Avaliação
NHS	Sistema Nacional de Saúde no Reino Unido
OMS	Organização Mundial de Saúde
ONU	Organização das Nações Unidas
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PEP	Prontuário Eletrônico do Paciente
PL	Poder Legislativo
PNBL	Plano Nacional de Banda Larga
PNIIS	Política Nacional de Informação e Informática em Saúde
PP	Prontuário de Papel
PRODAPE	Programa de Democratização do Acesso e Permanência de Estudantes das Classes Populares
RES	Registro Eletrônico de Saúde
RGPDE	Regulamento Geral de Proteção de Dados da União Europeia
RIPSA	Rede Interagencial de Informações para Saúde
RNDS	Rede Nacional de Dados em Saúde
RNIS	Rede Nacional de informações de Saúde
ROPA	Registro das Atividades de Tratamento de Dados Pessoais
SAI	Sistema de Informações Ambulatoriais
SciELO	Scientific Electronic Library Online
SIAB	Sistema de Informação de Atenção Básica
SIH	Sistema de Informações Hospitalares
SINAN	Sistema de Informações de Agravos de Notificações
SINASC	Sistema de Informação de Nascidos Vivos
SI-PNI	Sistema de informação do programa Nacional de Imunização
SIS	Sistemas de Informação em Saúde
SISCAN	Sistema de Informação de câncer de Útero e de Mama
SISREG	Sistema Nacional de Regulação
SLTI	Secretaria de Logística e Tecnologia da Informação
SNIS	Sistema Nacional de Informação em Saúde
STF	Supremo Tribunal Federal
STJ	Supremo Tribunal de Justiça
SUS	Sistema Único de Saúde
TCLE	Termo de Consentimento Livre e Esclarecido
TI	Tecnologia de Informação

TIC	Tecnologias da Informação e Comunicação
UNICEUB	Centro de Ensino Unificado de Brasília
UTIs	Unidades de Terapia Intensiva
WHO	World Health Organization

Lista de Figuras

FIGURA 1 - LINHA DO TEMPO DA INFORMATIZAÇÃO DA SAÚDE NO BRASIL ... 69

FIGURA - FASES DO CICLO DE VIDA DO TRATAMENTO DE DADOS PESSOAIS. 101

FIGURA 3 - USOS DAS TECNOLOGIAS DE INFORMAÇÃO NA ÁREA DA SAÚDE .. 106

FIGURA 4 – REPRESENTAÇÃO ESQUEMÁTICA DA RNDS COMO PLATAFORMA NACIONAL DE INOVAÇÃO, INFORMAÇÃO E SERVIÇOS DIGITAIS EM SAÚDE.... 148

FIGURA 5 - SEGURANÇA DA INFORMAÇÃO NO CONECTE SUS..... 158

Lista de Quadros

QUADRO 1 - RISCOS VERIFICADOS A PARTIR DO TRATAMENTO DE DADOS E SEUS ESCOPOS 110

QUADRO 2 – ATOS NORMATIVOS DO CENÁRIO DA INFORMAÇÃO EM SAÚDE NO BRASIL 114

QUADRO 1 – PROCESSO DE CONSTRUÇÃO DA LGPD 165

QUADRO 3 - PANORAMA DA EFETIVAÇÃO DA ANPD 184

QUADRO 4 - DIREITOS SUBJETIVOS DOS TITULARES DE DADOS PESSOAIS 195

QUADRO 5 - DADOS DIRETOS E INDIRETOS NA ESFERA DA SAÚDE 208

QUADRO 6 - COMPARATIVO ENTRE AS ESFERAS DA SAÚDE PÚBICA E PRIVADA QUANTO AO TRATAMENTO DE DADOS 237

QUADRO 7 - PRINCIPAIS INCIDENTES ENVOLVENDO VAZAMENTO DE DADOS DE SAÚDE NO BRASIL 245

Sumário

1 INTRODUÇÃO 10

2 CAPÍTULO I - A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS RELACIONADOS À SAÚDE 19

2.1 Privacidade e dados pessoais: entre o público e o privado 19
2.2 Limites da privacidade individual face ao bem-estar coletivo 24
2.3 Dados pessoais de saúde: hipóteses legais de compartilhamento 28
2.4 Da definição de dados relacionados à saúde e sua condição enquanto dados sensíveis 36
2.4.1 O direito à autodeterminação informativa, dados clínicos de caráter pessoal como objeto de direito fundamental: anonimização e pseudoanonimização 42
2.4.2 Os atores das relações de saúde sob o prisma da LGPD 50

3 CAPÍTULO 2 - O DIREITO À SAÚDE E AS TECNOLOGIAS NA SOCIEDADE DA INFORMAÇÃO 58

3.1 A dimensão informativa do direito à proteção à saúde no ordenamento jurídico brasileiro .. 58
3.2 A tutela da personalidade na era digital: os dados de saúde como dados sensíveis e o problema da sua informatização 63
3.3 Função da informação na área da saúde 71
3.3.1 Do sigilo profissional na área de saúde e a (In)distinção entre sigilo e segredo médico . 76
3.3.2 Relação Médico-Paciente 82
3.3.3 Consentimento Informacional 88
3.4 O ciclo de vida do tratamento dos dados pessoais em saúde 93
3.4.1 Impactos da utilização dos Bancos de Dados em Saúde 102
3.4.2 Segurança da Informação em Saúde 107

4 CAPÍTULO 3 - MARCOS DA PRIVACIDADE DE SAÚDE DIGITAL PARA O BRASIL: UMA RETROSPECTIVA DOCUMENTAL 114

4.1 Política Nacional de Informação e Informática em Saúde (PNIIS) 115
4.2 Estratégias de saúde digital para o BRASIL 2017 124
4.3 Programa Conecte SUS 134
4.4 Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 140
4.5 Estratégia de saúde digital para o Brasil 2020-2028 145
4.6 Avanços e retrocessos verificados na saúde digital de 2020 - 2022 durante o período pandêmico 150

5 CAPÍTULO 4 - DESAFIOS DA SAÚDE DIGITAL NO CONTEXTO BRASILEIRO.... 160

5.1 A proteção de dados pessoais e sensíveis e a sua inserção como política pública conforme a LGPD e Constituição Federal 160
5.2 A amplitude das normas como obstáculos para proteger e administrar os dados pessoais e sensíveis 166
5.3 Vulnerabilidades da utilização de novas tecnologias nos serviços público e privado de saúde face a necessidade da proteção de dados pessoais 170

5.4 Deficiências na gestão de dados no setor de saúde..... 175
5.4.1 Do baixo índice de planejamento, do enfraquecimento da ANPD e da ausência de uma cultura de proteção de dados 179
5.5 Impactos da ausência de uma proteção efetiva dos dados de saúde para os usuários do sistema 188
5.6 O tratamento de dados de saúde como matriz para o surgimento de novas formas de discriminação 198
5.7 Desdobramentos e consequências da utilização indevida de dados sensíveis de saúde na esfera individual de seu titular..... 207

6 CAPÍTULO 5 - A RESPONSABILIDADE CIVIL EM CONSEQUÊNCIA DO VAZAMENTO DE DADOS DE SAÚDE 215
6.1 Responsabilidade mediante o compartilhamento indevido de dados de saúde..... 215
6.2 Da responsabilidade dos envolvidos no processo de tratamento de dados conforme a LGPD 221
6.3 Considerações sobre o sistema de responsabilidade civil adotado pela LGPD..... 227
6.4 Dificuldades inerentes ao arbitramento do valor do dano face ao potencial discriminatório e lesivo das informações de saúde 238
6.5 Análise de decisões envolvendo dados sensíveis de saúde emanadas por tribunais brasileiros246
6.5.1 Inferências acerca das decisões judiciais coletadas 264

7 CONCLUSÃO 268

REFERÊNCIAS 275

ANEXOS 302
Anexo 1 - Política de privacidade..... 302
Anexo 2 - Resumo das ações propostas na estratégia de saúde digital 318

1 Introdução

Os avanços tecnológicos e as recentes crises sanitárias recolocaram em debate os limites da privacidade individual face ao bem-estar coletivo, abrindo uma delicada esfera, sobretudo quando o tema envolve questões saúde. No Brasil, o direito à privacidade dos dados pessoais foi recentemente consolidado pela Lei Geral de Dados Pessoais[1], mas já enfrenta diversos desafios e questionamentos que vão desde as constantes mudanças operadas pela expansão tecnológica apta a coleta de dados, até a necessidade do controle de informações para políticas públicas de controle sanitário.

A cada momento, diversas classes de informações são colhidas e projetadas nas redes, onde se tecem incontáveis bancos de dados, em um movimento tortuoso que demanda uma série de reflexões. Entre os questionamentos mais urgentes, destaca-se a necessidade de mecanismos que assegurem o direito à privacidade e confidencialidade para o indivíduo que utiliza os sistemas de saúde n Brasil, sejam estes públicos ou privados.

As tecnologias não apenas se inserem no cotidiano, mas representam agentes de transformação social, que influenciam e ditam padrões, moldam comportamentos, gerando ainda impactos nos cenários políticos e econômicos. Ao analisar a importância do acesso à Internet, questão que recentemente passou a pleitear a condição de direito humano com base no artigo 19 da Declaração Universal dos Direitos Humanos de 1948[2], por ser considerada ferramenta essencial e um dos principais meios para o exercício da liberdade de expressão, percebe-se que é preciso reavaliar conceitos essenciais como intimidade, privacidade e dignidade da pessoa. A humanidade se encontra sob os reflexos do antagonismo entre as ideias de exposição e compartilhamento de informações *versus* a necessidade de preservação e sigilo.

Nesse contexto apresenta-se o tema da tese: "Proteção à Saúde no Ordenamento Jurídico Brasileiro: Uma Análise da Dimensão Informativa no Cenário da Lei

1 A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília – DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 set. 2022.

2 A Declaração Universal dos Direitos Humanos é um documento que delimita e norteia os direitos fundamentais do ser humano. Foi estabelecida em 10 de dezembro de 1948 pela Organização das Nações Unidas (ONU), à época composta por 58 Estados-membros, entre eles o Brasil. ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos**. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Brasília: Unesco, 1948. Disponível em: http://unesdoc.unesco.org/images/0013/001394/139423por.pdf. Acesso em: 9 mar. 2022.

Geral de Proteção de Dados", matéria que imprime relevância social e jurídica por tratar de assunto relacionado ao direito fundamental à saúde e a proteção da privacidade. O direito à saúde que se encontra elencado como direito fundamental, é, simultaneamente, um instrumento de proteção ao indivíduo e um meio de assegurar o próprio direito à vida, inviolável conforme o artigo 5º da Constituição Federal. Está ainda, diretamente relacionado ao princípio da dignidade da pessoa humana, sendo, este, o princípio fundamental da República Federativa do Brasil, nos termos do artigo 1°. Assim, infere-se que para ser possível uma vida digna, é necessário que todos vivam bem e, por conseguinte, com saúde[3].

O artigo 23 da Carta Magna impõe o cuidado com a saúde e assistência pública, da proteção e garantia das pessoas portadoras de deficiência, incluindo esta como competência comum da União, Estados, Distrito Federal e dos Municípios. Fortalecendo este posicionamento o artigo 196 também da Carta Política, coloca a saúde como direito de todos e dever do Estado, a ser garantido mediante políticas sociais e econômicas que visem à redução dos riscos de doenças e, outros agravos, bem como o acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação[4]. Trata-se de um interesse coletivo que merece a devida análise face às transformações constantes, influenciadas pela ciência e

tecnologia e seus impactos na vida do cidadão brasileiro - usuário dos sistemas de saúde.

O presente estudo desenvolveu-se vinculado à linha de pesquisa: Políticas Públicas, Sociedade Civil e Proteção da Pessoa do Curso de Doutorado e Políticas Públicas do Centro de Ensino Unificado de Brasília - UNICEUB. As questões ora apresentadas fazem parte das indagações da autora, como pesquisadora do Direito e como cidadã, imbuída da consciência da necessidade de implementação de políticas públicas aptas

3 No entendimento atual, tem-se o direito à saúde como parte de um grande grupo que envolve questões de bem-estar físico e mental, assim como os diferentes direitos humanos, interligados e dependentes entre si. Seguindo a amplitude dos direitos humanos fundamentais, as relações de a saúde ultrapassam o potencial de redução da vulnerabilidade, em termos de problemas e fatores de risco e abarca questões de violações de direitos, como a violência nas grandes cidades, casos de tortura, escravidão e violência de gênero, que podem causar danos à saúde. Verifica-se ainda uma conexão direta do desenvolvimento da saúde com outros direitos, tais como a participação social, o acesso à informação, a comunicação, que se tornam instrumentos e potencializam a democracia, o exercício da cidadania e a própria garantia desses direitos considerados fundamentais.

4 Constituição Federal de 1988, artigo 196: A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação. BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Emendas Constitucionais. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 06 out. 2020.

a proporcionarem uma vida melhor para as pessoas que vivenciam uma realidade na qual a proteção da privacidade encontra-se precária, principalmente no que se refere a dados de saúde. Trata-se de situação, a rigor, exposta nas prestações de serviços realizadas tanto pelo Estado, como por particulares, os quais, na maioria das vezes, não projetam as devidas proteções à privacidade, valor caro aos interesses da coletividade, sobremaneira, quando associados à saúde, oportunidade em que passam a ser classificados como sensíveis.

A LGPD, como ficou popularmente conhecida, entrou em vigor com o objetivo de garantir maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados. A chegada da LGPD responde ao anseio por um resguardo de maneira mais efetiva dos direitos fundamentais de liberdade, privacidade e autonomia informativa, cuja tutela individual e social é vital para a consolidação do regime democrático nas sociedades contemporâneas.

A norma resultou em um delineamento mais nítido no que tange à tutela da privacidade, bem como dos direitos da personalidade, vez que reflete a visão constitucional da cidadania, dignidade humana e proteção do consumidor à luz da ordem econômica. Estes conceitos, previstos na Carta Magna junto à livre-iniciativa, configuram uma dialética normativa positiva pautada no objetivo da promoção da autodeterminação informacional do ser humano.

São configuradas como objeto de aplicação da LGPD, atividades de tratamento que tiverem por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento que se referir a dados de indivíduos localizados no território nacional, bem como situações envolvendo dados pessoais que tenham sido coletados no Brasil. Nesse sentido, resta claro os efeitos extraterritoriais da norma que pode, conforme seu artigo 3º exigir, inclusive, que um o agente de tratamento submeta-se às regras protetivas aos dados pessoais e à privacidade de outros países, em paralelo às suas próprias.

Em seu texto, a LGPD dedicou especial atenção aos dados obtidos em procedimentos associados à saúde, lhes atribuindo a condição de dados sensíveis em razão de seu conteúdo oferecer uma especial vulnerabilidade, e ensejar possibilidade de discriminação de alto potencial, que ultrapassa gerações. Assim, a partir da caracterização do cenário intangível do mundo tecnológico e da visão do Estado brasileiro acerca do direito à saúde, ora ampliado para a esfera digital, justifica-se a necessidade de uma reflexão sobre os desafios a serem enfrentados pelo Poder Judiciário ao buscar estabelecer uma tutela de preservação para os dados sensíveis, em especial aqueles aplicáveis à saúde,

a partir de ponderações realizadas mediante a análise das Estratégias para a Saúde Digital[5]do Governo Federal Brasileiro.

Diante do rigor das políticas propostas para o controle dos dados pessoais, de sua coleta ao descarte, as organizações de saúde assumem uma imensa responsabilidade, vez que seu acervo ultrapassa exames, prontuários e informações biométricas, atingindo ainda registros financeiros, informações de seguros de saúde e inúmeros fornecedores. Surge, então, um relevante questionamento: a proteção de dados sensíveis aplicados a saúde no ordenamento jurídico brasileiro garante o direito à privacidade e à dignidade da pessoa?

A justificativa da tese ocorre porque enquanto bem intangível de todos os seres humanos, a saúde é considerada digna da tutela protetiva estatal, apresentando-se como um dever do Estado a ser observado de forma plena, não apenas por meio de regulação legal, mas também através da efetivação de políticas públicas governamentais. Somente é possível se falar na garantia de uma vida digna mediante a promoção de medidas de bem-estar e vida saudável.

A responsabilidade do Estado pela criação de políticas públicas, que permitam acesso aos serviços necessários à promoção da saúde, é executada via normas infraconstitucionais, tais como a lei 8.080/90, que regulamenta o Sistema Único de Saúde, bem como estabelece princípios e diretrizes para a saúde em nosso país e ora enfrentam o desafio de abarcar os novos paradigmas oriundos da influência da tecnologia no setor.

Na sociedade da informação[6], os dados pessoais configuram verdadeiras extensões do indivíduo demandando proteções eficazes. No caso da saúde, trata-se de informações que, na maioria dos casos, são fornecidas pelo próprio cidadão sobre sua condição física e mental e classificadas como sensíveis pela LGPD, dado seu potencial discriminatório na hipótese de sserem reveladas em determinadas situações e sem o

5 O termo saúde digital, segundo definição do Ministério da Saúde brasileiro, deve ser compreendido enquanto o uso de recursos de Tecnologia de Informação e Comunicação - TIC com a finalidade de produzir e disponibilizar informações confiáveis sobre o estado de saúde para os cidadãos, profissionais de saúde e gestores públicos. O termo Saúde Digital é considerado mais abrangente do que e-Saúde e incorpora os recentes avanços na tecnologia, como novos conceitos, aplicações de redes sociais, internet das coisas, inteligência artificial, entre outros.

6 O conceito de sociedade da informação remonta a década de 80 durante a expansão e reestruturação do capitalismo e a evolução da era industrial. Sua construção foi marcada pela expansão das informações a partir do desenvolvimento da Internet. Deste modo, a visão ofertada pela sociedade da informação se encontra diretamente conectada ao processo de transição da fase industrial para a informacional. Segundo Castells, as tecnologias de informação e comunicação se tornaram fundamentais para a sociedade, tornando-se o elemento central da atividade humana. CASTELLS, M. A sociedade em rede. 2. ed. Tradução: Roneide Venancio Majer. São Paulo: Editora Paz e Terra, 1999.

devido consentimento de seu titular. Nesse contexto, é de suma importância analisar a responsabilidade mediante o compartilhamento indevido de dados clínicos, bem como as especificidades no processo de averiguação e valoração de um possível dano ocasionado pela quebra do sigilo de dados sensíveis.

Daí que o objetivo geral da tese é apontar as principais vulnerabilidades quanto à efetividade das proteções destinadas aos dados de saúde, bem como as consequências de possíveis violações no âmbito da responsabilidade civil, enquanto situações que demandam um olhar diferenciado do Estado para efetivar o almejado direito à privacidade e assegurar a dignidade da pessoa que se utiliza dos serviços de saúde.

Dentre os objetivos específicos, importa investigar como e em que termos se efetiva a proteção do ordenamento jurídico brasileiro quanto aos dados sensíveis aplicados à saúde, no que tange à sua coleta, armazenamento e descarte. Além de empreender uma revisão de literatura em diferentes bases de dados nacionais e internacionais acerca dos mecanismos de proteção de dados sensíveis e sua efetividade face ao direito à privacidade e dignidade da pessoa.

Neste painel, ainda é relevante identificar normas jurídicas brasileiras aptas a viabilizar a implementação das Estratégias para a Saúde Digital do Governo Federal Brasileiro e suas possíveis lacunas, além de verificar as consequências de possíveis violações do direito à privacidade de dados sensíveis aplicados à saúde, no âmbito da responsabilidade civil.

Para alcançar os objetivos propostos, a tese adotará quanto a descrição dos procedimentos que serão utilizados no desenvolvimento da pesquisa científica (objeto de estudo), considerando o objetivo geral e os específicos já delineados, e ainda, a interdisciplinaridade que alcança, a pesquisa de natureza qualitativa e quantitativa. No que se refere ao método do procedimento, adotar-se-á o comparativo e hipotético-dedutivo.

Será realizada ainda uma pesquisa bibliográfica, documental, exploratória e normativa sobre o tema da dimensão da privacidade relacionado a dados médicos, que são dados sensíveis relacionados à saúde, protegidos pela LGPD.

Partindo-se dos referenciais teóricos apresentados, será promovida consulta de obras doutrinárias e artigos científicos publicados em periódicos especializados, veiculados por meio físico ou eletrônico (*internet*), nacionais e estrangeiros, com destaque das plataformas de pesquisa (a exemplo do Catálogo de Teses e Dissertações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES e da

Plataforma *Scientific Electronic Library Online* - SciELO), com posterior seleção de conteúdo por critérios temático e temporal.

Ainda será realizado um levantamento de acórdãos, para no último capítulo da tese, explicar de maneira prática, como ocorrem essas decisões no âmbito dos tribunais, objetivando identificar argumentos utilizados pelas Cortes Estaduais para o enquadramento do tema. A seleção dos acórdãos permitirá a pesquisa exploratória, perquirindo um perfil sobre as decisões no âmbito da privacidade de dados sensíveis.

Pesquisas documentais e normativas serão promovidas pelas plataformas de buscas de pesquisa de legislação e documentos, a exemplo do Ministério da Saúde, somadas a portais de legislação e documentos como Política Nacional de Informação e Informática em Saúde – PNIIS, Estratégias de Saúde Digital para o Brasil - ESD17, ESD28.

Assim, a coleta dos julgados será organizada com base em critérios metodológicos definidos e pré-determinados, por meio da busca de palavras-chaves, com análise e interpretação a partir dos métodos de análise qualitativa de base empírica[7] e análise de conteúdo[8]. Para a construção do desenho metodológico da pesquisa jurisprudencial, pretende-se realizar a formulação de quadros indicativos aptos a condensar resultados apreciáveis e, se possível, comparáveis e que visem avaliação por terceiros.

Anote-se que a metodologia de análise das decisões permitirá identificar um perfil sobre o assunto, a posição dos decisores em relação ao tema e a suas eventuais inclinações em relação às demais possibilidades de solução que porventura não tenham sido adotadas[9]. Ainda, na definição de lacunas encontradas nas espécies legislativas, será utilizada a análise do discurso, para revisar e analisar os critérios que apenas o aspecto normativo-positivo da legislação não seja suficiente para realizar uma interpretação teleológica.

As fontes de pesquisas serão a legislação, doutrina, normas internacionais, jurisprudência e direito comparado para conferir-se a fundamentação teórica e a pesquisa,[10] além de relatórios, e demais documentos que contenham informações sobre proteção de dados de saúde.

---

7 MINAYO, M. C. S. Análise qualitativa: teoria, passos e fidedignidade. Ciência & Saúde Coletiva, Rio de Janeiro, v. 17, n. 3, 2012, p. 621-626. Disponível em: https://www.scielo.br/j/csc/a/39YW8sMQhNzG5N-mpGBtNMFf/?format=pdf&lang= pt. Acesso em: 30 set. 2022.

8 BARDIN, L. Análise de conteúdo. Tradução: Luís Antero Reto; Augusto Pinheiro. 1. ed. São Paulo: Edições 70, 2016.

9 FREITAS FILHO, R,; LIMA, T. M. Metodologia de Análise de Decisões – MAD. Universitas Jus, Brasília, n. 21, p. 1-17, jul./dez. 2010, p. 2-3.

10 GIL, A. C. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 2002, p. 44.

Far-se-á, ainda, uma análise empírica da normativa referente às Políticas Públicas que tratem das Estratégias para a Saúde Digital do Governo Federal Brasileiro, bem como a verificação de sua extensão e aplicação conforme a análise de banco de dados pertinentes.

O processo de verificação dos dados obtidos na pesquisa ocorrerá a partir da análise de conteúdo, a qual se revela mais adequada para a proposta desse projeto. Segundo Bardin[11], a análise de conteúdo consiste num conjunto de técnicas de análise das comunicações, visando obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) dessas mensagens.

O estudo traz à baila, a discussão de um objeto instigante da perspectiva jurídica e de políticas públicas, pois, em uma sociedade democrática, verifica-se a necessidade de meios para proteger os direitos sociais básicos dos cidadãos frente a inoperância estatal de cumprir o texto constitucional. Dessa forma, trabalhar a questão da privacidade em dados de saúde, além de se reputar um tema atual, revela-se necessário na sociedade para que se possa implementar políticas adequadas de proteção de resguardo e sigilo a esses dados.

Entende-se a pesquisa como contínuo diálogo com a realidade, na busca do conhecimento que transcende o senso comum. Destarte ela percorre diversos caminhos, e utiliza-se de instrumentos para captar e promover o confronto de dados, evidências e informações disponíveis.

Essa releitura do direito à privacidade na sociedade da informação faz-se necessária com o intuito de evitar a perda do controle do indivíduo sobre os seus dados pessoais, sobretudo, aqueles que podem ensejar qualquer forma de discriminação. Assim, defende-se uma nova forma de tutela da privacidade que não se limita a proibição à intromissão alheia na vida íntima, isto é, um dever geral de abstenção, mas impõe também deveres de caráter positivo.

A privacidade, ultrapassando a dimensão procedimental, vinculada ao tratamento destinado aos dados pessoais desde sua coleta até o momento de sua eliminação em caráter definitivo, possui uma dimensão substancial, conectada à própria utilização da informação obtida. Todo indivíduo possui o direito de controlar a representação de si mesmo constituída a partir de seus dados e informações pessoais. É direito de toda

11 BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011, p. 12.

pessoa exigir que tal representação reflita a realidade, impedindo que seu uso assuma caráter discriminatório.

Não obstante a urgência de atuação do legislador, com vistas a promover a manutenção do sigilo e a proteção de dados pessoais, somente em 2018 foi editada a Lei Geral sobre a Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018 –, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A lei brasileira dispôs acerca da proteção de dados como um dos paradigmas da dignidade humana, conforme o disposto no Regulamento Geral de Proteção de Dados da União Europeia (RGPD), no qual se considera os direitos da personalidade como projeção da dignidade humana e a proteção de dados como espécie daquele. Logo, elementos como consentimento informado e legítimo interesse, seriam utilizados como parâmetros na busca pela preservação da autonomia da vontade e controle, pelos cidadãos, do uso dos dados e informações pessoais.

Para fins de organização da discussão em torno do tema ora apresentado, estruturou-se esta tese em cinco capítulos. O primeiro deles aborda a proteção jurídica de dados pessoais relacionados à saúde, no qual será reportado todo o tratamento estabelecido pela Lei Geral de Proteção de Dados, além dos conceitos relevantes para a adequada compreensão dos termos da LGPD.

O segundo capítulo se dedica a estudar o direito à saúde e as tecnologias na sociedade da informação. Para tanto será detalhada toda a dimensão informativa e documental do direito à proteção à saúde no direito brasileiro, além do diagnóstico da tutela da personalidade na era digital e os dados de saúde como dados sensíveis e o problema da sua informatização.

No terceiro capítulo será realizada uma retrospectiva documental acerca de estratégias de Saúde Digital para o Brasil entre os anos de 2016 e 2022, com ênfase na análise das versões mais recentes das Estratégias de Saúde digital para o Brasil, além de destacar a Política Nacional de Informação e Informática em Saúde (PNIIS) e o Programa Conecte SUS.

O capítulo seguinte-quarto-foi dedicado aos desafios da saúde digital no contexto brasileiro. O primeiro ponto a ser analisado é justamente a proteção de dados pessoais e sensíveis e a sua inserção como política pública, além de verificar a amplitude das normas como obstáculos para proteger e administrar os dados pessoais e sensíveis. As vulnerabilidades da utilização de novas tecnologias nos serviços públicos serão

delineadas para que se possa detectar as principais deficiências na gestão de dados públicos.

Por fim, o quinto capítulo se reportará a estudar a Responsabilidade Civil em consequência do vazamento de dados de saúde, respaldado, especialmente, na análise de julgados de cortes estaduais. A esta altura serão aprofundados aspectos intrínsecos ao tema como: a indicação do um regime de responsabilidade adotado pela LGPD, caracterização do dano face ao vazamento de dados de saúde, o potencial discriminatório e lesivo das informações de saúde, além das dificuldades inerentes ao arbitramento do *quantum* indenizatório.

As considerações finais retomarão as consequências das lacunas verificadas quanto a proteção de dados sensíveis na LGPD, ao tempo que buscará contribuir para o estudo do tema por meio de questionamentos necessários, ainda não enfrentados diretamente pelos tribunais brasileiros, como os possíveis desdobramentos do dano ocasionado pelo vazamento de dados de saúde.

Após o estudo completo da tese será possível responder até que ponto, e, por quais caminhos, a legislação consegue garantir os direitos à privacidade quanto ao manuseio dos dados de saúde. Também será possível detalhar como os principais documentos e regras, que versam sobre a privacidade na seara de saúde no Brasil, tem sido trabalhados, em via prática, identificando seus principais acertos e pontos de vulnerabilidade.

2 Capítulo I - A proteção jurídica de dados pessoais relacionados à saúde

O Capítulo inaugural da tese cuida da privacidade fazendo uma análise epistemológica e desdobrando a Lei Geral de Proteção de Dados em seus aspectos legislativos. Aqui, estão presentes os conceitos necessários ao entendimento dos limites da privacidade nas searas pública e privada, como também o sopesamento, em face do bem coletivo. Tem-se ainda, o direito à autodeterminação informativa no enfoque dos dados clínicos, sua anonimização e pseudoinformação, além da análise dos procedimentos indicados face ao descumprimento das normas da LGPD, em matéria de saúde.

Neste primeiro momento, serão tecidas considerações quanto aos fundamentos do direito à autodeterminação informativa, partindo do contexto dos dados clínicos de caráter pessoal como objeto de direito fundamental. E como subsídio para as ponderações contidas nos capítulos seguintes, serão apresentados os principais atores envolvidos nas relações de saúde sob o prisma da LGPD.

2.1 Privacidade e dados pessoais: entre o público e o privado

Ao se pensar na ideia de privacidade, amparada pela herança inglesa do conceito de *privacy,* chega-se primeiramente à noção do direito enquanto reserva de informações pessoais, inerentes a fatos próprios da vida e sua exposição. Tal concepção, seria ainda associada ao direito de ser deixado em paz, conforme explicado pelos juristas norte-americanos Louis Brandeis, e Samuel Warren, no artigo *Right to Privacy,*[12] no qual foi apresentada uma construção para a noção de privacidade fundada na obra do filósofo Ralph Waldo Emerson[13], que propunha a solidão como critério e fonte de liberdade[14].

Face a esfera do coletivo, tem-se que a privacidade permeia processos que se refletem diretamente nas relações sociais do indivíduo e pode ser, igualmente, compreendida

12 , "The Right to Privacy" ("O Direito à Privacidade", tradução livre) é um artigo jurídico de autoria de Samuel Warren e Louis Brandeis, que foi publicado pela revista Harvard Law Review no ano de 1890. O texto é considerado um dos ensaios mais influentes na história do direito dos Estados Unidos da América e foi amplamente reconhecido como a primeira publicação do país a defender um direito à privacidade. WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. **Harvard Law Review**, New York, v. 4, n. 5, 1890. Disponível em: http://www.jstor.org/stable/1321160. Acesso em: 06 abr. 2022.

13 Representante da filosofia "transcendentalista", exposta em obras como Natureza, Ensaios e Sociedade e solidão.

14 WARREN; BRANDEIS, op. cit.

como o controle da exposição e da disponibilidade de informações acerca de si mesmo. A imposição de limites ao fluxo de informações e contato com terceiros permitiria o indivíduo existir em sociedade mantendo certos níveis de anonimato e assegurando a não interferência pelo Estado em sua vida particular. No tocante as relações sociais, o conceito também se manifestaria enquanto a possibilidade de reivindicar do Estado a tutela dessa privacidade, gerando uma proteção contra terceiros.

Nas buscas pela origem da privacidade, acredita-se que tal noção surge no viés pessoal entre os séculos XVII e XVIII, com a modificação do padrão das construções que passam a oferecer quartos privados, dando início a práticas individualistas gradativamente inseridas no cotidiano social[15] e, consequentemente, iniciam novos costumes e padrões de comportamento. Desde então, a privacidade atravessa um percurso evolutivo que se inicia em uma inexistência "forçada" pela noção de bem-estar social e segue pelas mais diversas fases das relações humanas, desembocando em um curioso movimento de abolição espontânea com a revolução ocasionada pelas mais recentes tecnologias, em especial a internet.

Por sua importância no desenvolvimento das relações sociais, o direito à privacidade foi reconhecido como um direito fundamental. No âmbito internacional, a Declaração Universal dos Direitos Humanos (DUDH), de 1948, expressa, em seu art. 12, que "ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques"[16].

No ordenamento jurídico brasileiro, as questões sobre a privacidade vêm associadas aos conceitos de vida privada e intimidade, especialmente, na sua configuração como direitos da personalidade. A Constituição da República Federativa do Brasil de 1988 dispõe, em seu art. 5º, inciso X, que "[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"[17]. Já o Código Civil, em seu artigo 21 afirma que "[...] a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do

15 DERLEGA, V. J.; CHAIKIN, A. L. Privacy and Self-Disclosure in Social Relationships. Journal of Social Issues, [*S.l.*], v. 33, n. 3, p. 102–115. Disponível em: https://doi.org/10.1111/j.1540-4560.1977.tb01885.x. Acesso em: 9 mar. 2022.

16 ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Brasília: Unesco, 1948. Disponível em: http://unesdoc.unesco.org/images/0013/001394/139423por.pdf. Acesso em: 9 mar. 2022.

17 BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Emendas Constitucionais. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 5 mar. 2022.

interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma", de modo que acaba por se furtar a obrigação de adentrar nas especificidades da matéria que a cada dia se multiplicam tendo em vista o contexto social, político e econômico dos tempos atuais. Além disso, se faz presente no Código de Defesa do Consumidor, com a regulação de bancos de dados[18].

Nos termos do direito à privacidade, o objeto de proteção é, precipuamente, a integridade moral do indivíduo. Surge assim, no cenário hodierno, o desafio de atualizar a visão do século XIX, a fim de permitir o enfrentamento de novas problemáticas que envolvem as questões de privacidade, com o objetivo de assegurar uma tutela verdadeiramente eficiente. Porém, tal tarefa demanda um vasto esforço, em virtude da velocidade das transformações vivenciadas pela sociedade contemporânea no que se refere as formas de coleta, armazenamento e gestão de informações.

Quando se trata das proteções inerentes à vida privada, não raramente percebe-se uma confusão nas nomenclaturas empregadas no ordenamento jurídico brasileiro, com a mescla dos termos privacidade e intimidade. Alguns autores defendem a diferenciação entre as expressões, enquanto outros as utilizam com caráter similar, não havendo uma uniformização doutrinaria ou legislativa. Em uma visão objetiva, a intimidade poderia ser considerada como um conceito voltado para o âmbito do exclusivo, referente ao que alguém reserva para si, sem qualquer tipo de repercussão social. Já a vida privada, por mais isolada que possa ser, sempre se caracteriza pelo viver entre outros, por exemplo, em família, no trabalho, no lazer em comum.[19]

---

18 O Código de Defesa do Consumidor - Lei nº 8.078 de 11 de setembro d e 1990, dispõe em seu artigo 43 que o consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6o Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. Código de Defesa do. Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990a. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 9 mar. 2023.

19 O raciocínio apresentado na distinção entre intimidade e privacidade pode ser encontrado em diversas obras jurídicas, dentre as quais se utilizou e recomenda a leitura do livro Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, escrita por Tércio Sampaio Ferraz Júnior. FERRAZ JÚNIOR, T. S. A liberdade como autonomia recíproca de acesso à informação. *In*: MARTINS, Ives Gandra da Silva; GRECO, Marco Aurélio. Direito e Internet: relações jurídicas na sociedade informatizada. São Paulo: Revista dos

O direito à intimidade seria conceituado como aquele que visa a resguardar as pessoas dos sentidos alheios, principalmente da vista e dos ouvidos de outrem. Ou seja, é o direito da pessoa de excluir do conhecimento de terceiros tudo aquilo que a ela se relaciona[20]. Seria compreendido, ainda, como o poder correspondente ao dever de todas as outras pessoas de não adentrar na esfera alheia, opondo-se a eventuais descumprimentos desse dever, realizados por meio de investigação e/ou divulgação de informações sobre a vida de outrem[21].

A este ponto, é necessário observar que o direto à intimidade comporta diferentes nuances, dentre as quais se destaca o direito ao segredo ou ao sigilo. O direito ao sigilo, refere-se aos fatos específicos que não convém ser divulgados, seja por razões pessoais, profissionais ou comerciais. Por diversos momentos da vida prática, há para o indivíduo a necessidade de que determinados atos ou questões permaneçam inacessíveis ao conhecimento de terceiros. Em respeito a tal demanda, surgem hipóteses nas quais é ilícito não apenas divulgar tais manifestações, mas também o simples tomar conhecimento delas e o revelá-las, não importa a quantas pessoas[22].

A celeuma das nomenclaturas e seus alcances segue alimentada pela explosão de novos conceitos e vocabulários diariamente criados para representar a sociedade da informação, o que torna mais evidente a defasagem normativa, em situação que abre uma via para a delicada questão das mutações constitucionais, enquanto meio de readequação do direito posto à realidade jurídico-social. É certo que a visão inicial do direito de ser deixado em paz já não reflete o propósito necessário em meio a realidade do indivíduo contemporâneo, que não raramente renuncia a sua privacidade

---

Tribunais, 2001, p. 54.

20 Adriano De Cupis entende que a esfera íntima da pessoa se divide em direito à riservatezza e o direito à segretezza. CUSPIS, A. **I diritti della personalità.** Milano: A. Giuffre, 1982. Descrição Física: xvi, 641 p. Referência: 1982. Disponibilidade: Rede Virtual de Bibliotecas. Localização: STJ.

21 Com este pensamento se posiciona Milton Fernandes. FERNANDES, M. Os direitos da personalidade: estudos jurídicos em homenagem ao Professor Caio Mário da Silva Pereira. Rio de Janeiro: Forense, 1984, p. 17 e ss.

22 No que se refere ao direito ao sigilo, o Código Penal estabelece o crime de violação de correspondência, o qual é uma forma de violação ao direito de segredo. Artigo 151: "Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena – detenção, de 1 a 6 meses, ou multa". Na mesma pena incorre ainda "quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas" São condutas nas quais se verifica grave violação à intimidade da pessoa e por isso tratadas como crime. No mesmo sentido, a Constituição Federal de 1988 estabeleceu "que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei penal estabelecer para fins de investigação criminal ou instrução processual pena". Desta forma a inviolabilidade de correspondência tem entre nós o status de garantia constitucional. BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. 2002. Brasília: Presidência da República, Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 5 mar. 2023.

e individualidade, ao registrar cada uma de suas ações, conduzindo uma vida *on-line* pública e se exaltando sempre que a conexão com a rede se interrompe, mesmo que por breves minutos.

Percebe-se que as noções de público e privado são constantemente fundidas nas práticas cotidianas, em movimentos contraditórios, o que torna necessário uma breve retomada acerca de seus conceitos. Originalmente a noção de privado remetia diretamente à questão da privacidade do indivíduo, enquanto o público deveria corresponder a atuação do Estado e aos espaços nos quais se verificam as relações sociais. Todavia, as transformações das últimas décadas abriram precedentes para uma série de questionamentos, muitos dos quais ainda não foram propriamente respondidos sobre o tema. A realidade é que a fronteira entre as duas esferas é extremamente delicada e diretamente influenciada pelo contexto histórico, o que faz com que se moldem conforme elementos e discursos sociais.

Na antiga Roma[23] havia a distinção entre a visão de público e o privado diretamente associada a separação prática entre o que era de utilidade comum e o que era de utilidade particular, com atenção superior a tudo o que se relacionava com a coletividade, o que enfatizava a ideia da supremacia do público sobre o privado.

Na Grécia, o entendimento sobre o público estava associado aquilo que se encontra visível a todos, em oposição ao secreto, ao segredo, afastando o risco da arbitrariedade nos atos de governo. Enquanto o privado seria aquilo que pertence à ordem do que não se mostra em público, do que não necessita se informar a todos por se relacionar com questões vitais de cada indivíduo. Tal esboço foi amplamente utilizado na construção das democracias modernas.

Mas a distinção entre a esfera pública e a privada, clara na antiguidade, perde nitidez no mundo contemporâneo, perpassada pelos conceitos do social, comuns tanto ao público como ao privado, não sendo viável chamar público tão somente aquilo que afeta a todos, o comum e de interesse coletivo; e de privado o que se relaciona a uma ou a poucas pessoas, conduzindo à uma noção de individualidade.

Ao se pensar em sociedade, encontramos o social público, caracterizado pelas relações políticas, bem como o social privado marcado por questões econômicas de mercado,

23 Desde os primórdios da humanidade se verifica uma preocupação com a preservação da intimidade e da vida privada. Porém, nas sociedades antigas essa necessidade de proteção se apresentava de forma mais branda, visto que a maior parte da vida transcorria em espaços públicos. Em Roma, a vida privada era correspondente as ações que o indivíduo poderia praticar sem confrontar seus deveres públicos. FARIAS, E. P. Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2. ed. Porto Alegre: Sergio Antônio Fabris, 2000, p. 37.

evidenciando as dicotomias entre Estado e sociedade e indivíduo e sociedade. E nesse contexto, retomamos a busca pelas dimensões da privacidade.

O social privado, enquanto mercado permeado por relações econômicas e particulares demanda a garantia de um interesse público, a exemplo da livre concorrência, propriedade privada dos bens de produção, mas não se funde com o Estado na visão política, mesmo que haja sua interferência nas relações. Por outro viés, o mercado frequentemente adentra nas esferas de privacidade do indivíduo.[24] A partir deste exemplo, fica clara a dificuldade de se delinear limites da privacidade individual, especialmente, quando confrontada com situações que refletem diretamente nos interesses do Estado e da sociedade.

2.2 Limites da privacidade individual face ao bem-estar coletivo

A Constituição Federal de 1988 afirma em seu no artigo 5º, inciso X que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas" e em sequência introduz no inciso XII, a inviolabilidade do sigilo de dados como direito fundamental. Trata-se de um dos modos de assegurar o direito à privacidade, contudo a tutela da intimidade apresenta diversas controvérsias quanto a possibilidade de relativização, face a circunstâncias especiais. Um bom exemplo pode ser extraído do confronto entre a privacidade do indivíduo e o direito à informação de interesse público, verificado no cenário da crise sanitária decorrente do vírus COVID-19[25] nos últimos anos.

Em um contexto no qual se tem risco de danos em grande escala para a população em geral, questiona-se para qual lado penderia a balança da equidade. Mas antes de qualquer resposta, é preciso retomar a ideia do princípio da supremacia do interesse público[26], base da Administração Pública e norteador da atuação estatal. É este, um

24 FERRAZ JUNIOR, T. S. **Introdução ao estudo do direito**: técnica, decisão, dominação. São Paulo: Atlas, 2003, p. 36.

25 A cidade de Wuhan, na província de Hubei, na China, detectou os primeiros casos de uma estranha pneumonia em dezembro de 2019. Um novo tipo de coronavírus eclodiu, mais tarde batizado de Sars-Cov-2 e popularizado sob a nomenclatura de COVID-19. A Organização Mundial da Saúde (OMS) declarou a infecção humana pelo vírus Emergência de Saúde Pública em 30 de janeiro de 2020. Quatro dias depois, em 3 de fevereiro, o Ministério da Saúde brasileiro seguiu os passos da OMS e decretou Emergência em Saúde Pública de Importância Nacional. O COVID-19 fez milhares de vítimas ao redor do mundo e mesmo após dois anos, com boa parte da população vacinada, segue como grande ameaça em virtude de mutações e variantes que surgem constantemente.

26 O princípio da supremacia do interesse público sobre o particular tem surgimento no século XIX, pois o direito deixa de ser apenas um instrumento de garantia dos direitos dos indivíduos e passa a objetivar a consecução da justiça social e do bem comum. Os interesses representados pela Administração Pública, está previsto no Art. 37 da Constituição Federal Brasileira, e se aplica na atuação do princípio da supremacia do interesse público. Por tal princípio entende-se, que sempre que houver conflito entre um particular e um interesse público

princípio geral do direito inerente a qualquer sociedade, também considerado essencial para sua existência, enquanto norteador da conduta administrativa. Por tal princípio, cabe ao Estado uma série de prerrogativas com a finalidade de assegurar um objetivo específico: a busca pelo interesse público.

A primeira dificuldade decorre do próprio conceito de interesse público, considerando de certo modo indeterminado, vindo a depender da análise de cada caso concreto. O interesse público surge associado a duas vertentes distintas, sendo chamado primário quando apresenta relação direta com os interesses da coletividade, e secundário quando se refere ao interesse do Estado como ente individual. Desta forma, quando o Estado age visando aos interesses da coletividade, atua sob o manto do princípio da supremacia do interesse público sobre o privado, com a possibilidade de se sobrepor ao interesse individual em caso de confronto direto. Tal situação alerta para a problemática acerca dos limites entre o princípio da supremacia do interesse público sobre o privado e os direitos fundamentais dispostos na Carta Magna.

Para registro, o princípio da supremacia do interesse público está expresso na Lei n. 9.784/99, que tem por objetivo regular o processo administrativo no âmbito da Administração Pública Federal, e traz em seu artigo 2º a afirmação que a Administração Pública obedecerá: "[...] dentre outros, aos princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência"[27].

Tal princípio, considerado inerente à concepção de sociedade e convívio social encontra-se, implícito na Constituição Federal de 1988, fortalecendo o pensamento de que o Estado necessita de prerrogativas frente aos interesses individuais para atingir, satisfatoriamente, a finalidade pública[28]. Seria então, um pressuposto para uma sociedade bem-organizada.

Vale recordar que a ideia da primazia do interesse público sobre o privado é inerente à atuação estatal e acaba por se sobressair em virtude da existência do Estado se justificar na busca do interesse da coletividade. Tal interesse público prevalente é extraído da ordem jurídica, conforme cada caso concreto, sendo, portanto, indeterminado, o que

coletivo, deve prevalecer o interesse público. MELLO, C. A. B. Conteúdo jurídico do princípio da igualdade. 3. ed. São Paulo: Malheiros, 2017, p.53.

27 BRASIL. Lei nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 30 maio 2022.

28 MELLO, C. A. B. Vazamento de dados na saúde coloca pacientes na mira de golpes. Medicina S/A, São Paulo, 2022. Disponível em: https://medicinasa.com.br/vazamento-dados-saude/. Acesso em: 30 ago. 2022.. Curso de direito administrativo. 35. ed. São Paulo: Malheiros, 2021, p. 96.

dificulta a unificação de uma definição,[29] e provoca confusão quando do confronto com direitos fundamentais. Uma vez estabelecida a celeuma, a solução só poderia ser alcançada com a aplicação do princípio da razoabilidade, em uma ponderação de interesses[30].

Há quem defenda que tal relativização não deveria existir, vez que baseada em uma interpretação equivocada. Porém, a referida visão não se sustenta, pois embora não haja dúvidas que o ordenamento jurídico oferta garantias aos particulares, em determinadas relações jurídicas em face do Estado, é igualmente certa a obrigação de respeitar o interesse coletivo quando em conflito com o interesse particular, ainda que se trate de direitos fundamentais.

No que se refere, especificamente, ao direito à privacidade, a vida em sociedade e as múltiplas formas de interação entre indivíduos, impede uma interpretação em linhas absolutas. Frequentemente o judiciário se depara com a necessidade de ponderação frente aos dilemas envolvendo a matéria e, geralmente, responde com o amparo do texto contido no artigo 93, inciso IX, da Constituição Federal, que afirma que todos os julgamentos nos órgãos do Poder Judiciário serão públicos. O texto insere a ressalva que a lei poderá restringi-los em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação.

Torna-se clara a possibilidade de restrições e limitações a privacidade enquanto direito fundamental, sempre que confrontada com interesses sociais que permeiam a coletividade, como a segurança, saúde e a própria Ordem Pública. Conforme as circunstâncias verificadas, o interesse não apenas pode, como irá se sobrepor à pretensão de ser deixado só.

Em tempos de violência e insegurança, a tensão entre a vida privada e o interesse público resta mais evidente, exigindo especial cuidado para que não se ultrapassem os limites, tornando incipiente o direito à vida privada. Nesse sentido, o exemplo da justiça americana, a qual aprovou uma série de normas, no calor dos ataques de 11 de setembro de 2021, cujo objetivo era facilitar a captura de terroristas. Assim, concedeu-se permissão aos órgãos de segurança e inteligência para vasculhar os elementos claramente restritos à esfera privada dos cidadãos.[31]

---

29 , MEIRELLES, H. L. Direito Administrativo Brasileiro. 42. ed. São Paulo: Malheiros, 2016, p. 113.

30 DI PIETRO, Maria Sylvia Zanella. Direito administrativo. 35. ed. São Paulo: Forense, 2022, p. 48-49.

31 Recomenda-se a leitura do documento intitulado Patriotic Act - Provide Appropriate Tools Required to Intercept and Obstruct Terrorism. GPO – GOVERNMENT PUBLISHING OFFICE. Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (usa patriot act) act of 2001. Congressional Record, Whashington, v. 147, 2001. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf. Acesso em: 14 fev. 2023.

O Tribunal Constitucional Português, analisando a matéria, se posicionou em uma linha de relativização, concluindo que o direito fundamental a reserva da intimidade da vida privada pode, em certos casos, conflitar com outros interesses previstos no corpo da Constituição, dentre eles, o interesse público. O posicionamento da Corte Portuguesa é coerente com a jurisprudência de outros tribunais constitucionais e supranacionais, que igualmente reconhecem a necessidade de equilibrar direitos fundamentais em casos de colisão. A Convenção Europeia dos Direitos Humanos, por exemplo, prevê que os direitos podem ser restringidos quando necessários em uma sociedade democrática, desde que respeitem os princípios da proporcionalidade e da legalidade.

Na visão do ordenamento Brasileiro, o Supremo Tribunal Federal enfrentou a problemática da tensão entre o direito à intimidade em face ao princípio da ampla defesa e contraditório c/c o interesse público de persecução criminal e moralidade administrativa na Rcl-QO 2040/DF[32]. A Reclamação envolvia denúncias de agentes públicos em delitos contra a liberdade sexual de um detento, e entendeu pela relativização da privacidade, autorizando a realização do exame de DNA do filho da reclamante, com a utilização da placenta recolhida, preservando os direitos da criança recém-nascida.

32 - Reclamação. Reclamante submetida ao processo de Extradição n.º 783, à disposição do STF. 2. Coleta de material biológico da placenta, com propósito de se fazer exame de DNA, para averigüação de paternidade do nascituro, embora a oposição da extraditanda. 3. Invocação dos incisos X e XLIX do art. 5º, da CF/88. 4. Ofício do Secretário de Saúde do DF sobre comunicação do Juiz Federal da 10ª Vara da Seção Judiciária do DF ao Diretor do Hospital Regional da Asa Norte - HRAN, autorizando a coleta e entrega de placenta para fins de exame de DNA e fornecimento de cópia do prontuário médico da parturiente. 5. Extraditanda à disposição desta Corte, nos termos da Lei n.º 6.815/80. Competência do STF, para processar e julgar eventual pedido de autorização de coleta e exame de material genético, para os fins pretendidos pela Polícia Federal. 6. Decisão do Juiz Federal da 10ª Vara do Distrito Federal, no ponto em que autoriza a entrega da placenta, para fins de realização de exame de DNA, suspensa, em parte, na liminar concedida na Reclamação. Mantida a determinação ao Diretor do Hospital Regional da Asa Norte, quanto à realização da coleta da placenta do filho da extraditanda. Suspenso também o despacho do Juiz Federal da 10ª Vara, na parte relativa ao fornecimento de cópia integral do prontuário médico da parturiente. 7. Bens jurídicos constitucionais como "moralidade administrativa", "persecução penal pública" e "segurança pública" que se acrescem, - como bens da comunidade, na expressão de Canotilho, - ao direito fundamental à honra (CF, art. 5º, X), bem assim direito à honra e à imagem de policiais federais acusados de estupro da extraditanda, nas dependências da Polícia Federal, e direito à imagem da própria instituição, em confronto com o alegado direito da reclamante à intimidade e a preservar a identidade do pai de seu filho. 8. Pedido conhecido como reclamação e julgado procedente para avocar o julgamento do pleito do Ministério Público Federal, feito perante o Juízo Federal da 10ª Vara do Distrito Federal. 9. Mérito do pedido do Ministério Público Federal julgado, desde logo, e deferido, em parte, para autorizar a realização do exame de DNA do filho da reclamante, com a utilização da placenta recolhida, sendo, entretanto, indeferida a súplica de entrega à Polícia Federal do "prontuário médico" da reclamante. BRASIL. Supremo Tribunal Federal – STF. Reclamação 2040 QO / DF - Distrito Federal questão de ordem na reclamação. Reclamação. Reclamante submetida ao processo de Extradição n.º 783, à disposição do STF. Relator: Ministro Néri da Silveira. Diário do Judiciário – DJ, v. 2116, p. 129, 2003.

Por estes exemplos resta clara a possibilidade de se admitir, mediante a constatação de um interesse com respaldo constitucional e após a devida ponderação dos elementos extraídos do caso concreto, que o direito fundamental à privacidade venha a limitado. Contudo, é preciso atentar ao fato de que esta possibilidade não autoriza restrições aos direitos individuais e a intimidade privada do indivíduo pela mera invocação da garantia ao interesse público.

Em casos de tal complexidade é necessário ponderar a importância e relevância das normas colididas em face ao caso concreto, recorrendo a algumas técnicas fornecidas pela hermenêutica com base nas mais recentes interpretações constitucionais, em especial a ponderação. Esta deve tomar por base o princípio da proporcionalidade, assegurando que quando da necessidade do sacrifício de um direito para a solução do problema, o ônus imposto à parte sacrificada seja inferior ao benefício geral que se pretende obter com a solução.

Uma vez configurado o conflito entre o direito à privacidade e o interesse público, o caminho mais seguro a ser percorrido inicia com a verificação se de fato existe o conflito entre os referidos valores. Em caso afirmativo, deverá se seguir o exercício da ponderação com a averiguação de todas as circunstâncias que compõem o caso concreto, a atribuição de valores e pesos para, ao final, chegar ao entendimento sobre qual grupo de normas deverá, efetivamente, prevalecer.

Essa análise é essencial para garantir a proteção dos direitos individuais, ao mesmo tempo em que reconhece a importância dos interesses coletivos e do bem comum, e demanda maior cuidado quando envolve dados e informações associadas à saúde do indivíduo.

2.3 Dados pessoais de saúde: hipóteses legais de compartilhamento

Em seu processo de contínua evolução, a humanidade atingiu uma elevada esfera de inovações científicas, biológicas e tecnológicas, que expande seu raio a cada dia, ao tempo em que promove significativas alterações da forma como se vive e interage em sociedade. Diante de olhos, nem sempre atentos, se desenvolve uma importante mudança de paradigma que ultrapassa a condição de mera etapa no desenvolvimento tecnológico e atinge o status de revolução.

Mudanças que chegam com grande alarde e mesmo as que se apresentam de forma silenciosa são rapidamente absorvidas e incorporadas à rotina, influenciando condutas,

criando vocabulários e até padrões comportamentais. Trata-se de uma revolução marcada pelo processo tecnológigio, na qual se vivencia uma transição constante em direção a novos sistemas e objetos construídos sobre a infraestrutura digital.[33]

Nesse contexto tecnológico, também é possível afirmar o curso de uma revolução informacional. Os dados se tornaram parte essencial de processos rotineiros nas mais diversas áreas, influenciando ostensivamente tanto a vida privada do indivíduo, como suas relações sociais. O homem vive cercado de dados pessoais e não pessoais sob os quais se assenta a base para o crescimento tecnológico e econômico em linhas globais, de modo que a necessidade de uma regulamentação para a matéria se torna urgente.

Ao entrar em vigor, a Lei Geral de Proteção de Dados atingiu amplitude quanto a sua dimensão conceitual e efeitos jurídicos expressivos a ponto de ser comparada ao Código de Defesa do Consumidor[34], pois suas normas geram movimentação e reflexo nas mais diversas searas do âmbito público e privado. Trata-se de norma aplicável a todas as empresas e organizações que realizam tratamento de dados pessoais no Brasil, independentemente do tamanho ou segmento de atuação.

A proteção de dados foi ainda consagrada na emenda constitucional nº 115[35], em vigor desde fevereiro de 2022, sendo formalmente alçada ao rol de direitos fundamentais contidos na Constituição Federal de 1988. Deste modo, resta atribuído ao Estado, o dever de assegurar as proteções pertinentes aos usuários de sistemas eletrônicos.

---

33 A quarta revolução industrial, ou Indústria 4.0, é um conceito desenvolvido pelo alemão Klaus Schwab, diretor e fundador do Fórum Econômico Mundial. Hoje, é uma realidade defendida por diversos teóricos da área. Segundo ele, a industrialização atingiu uma quarta fase, que novamente "transformará fundamentalmente a forma como vivemos, trabalhamos e nos relacionamos. PORTES, R. Indústria 4.0: entenda o que é a quarta revolução industrial. Startse, 2021. Disponível em: https://www.startse.com/artigos/industria-40-entenda-o-que-e-a-quarta-revolucao-industrial/. Acesso em: 30 ago. 2022.

34 A Lei n°. 8.078/1990, popularmente conhecida como Código de Defesa do Consumidor - CDC, foi um marco na legislação nacional. Trata-se de um conjunto de normas com função social, cujo objetivo central é definir e garantir o cumprimento dos direitos dos consumidores, parte considerada como mais vulnerável em uma relação de consumo (BRASIL, op. cit., 1990a). O Código de Defesa do Consumidor é um instrumento extraordinário na concretização da cidadania e da justiça social, que pretende realizar uma tutela efetiva e integral do consumidor, através da disciplina das mais diversas faces da relação de consumo, abrangendo desde à produção e circulação dos bens e serviços, até o crédito e o *marketing*. A tutela protetiva do consumidor vem como um dos direitos e garantias fundamentais na Carta Constitucional de 1988.

35 Emenda Constitucional nº 115, de 10 de fevereiro de 2022: Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Acrescentou o inciso LXXIX, segundo o qual é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais, ao artigo 5º da Constituição Federal. BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Presidência da República, 2022.

Assim, qualquer operação de tratamento de dados pessoais realizada em território nacional atrairá a aplicação da LGPD, independente da possibilidade de incidir sobre essa mesma operação, outras regras, tais como, a RGPD europeia, sendo objeto de aplicação da LGPD, atividades de tratamento que tiverem por objetivo a oferta ou o fornecimento de bens ou serviços, ou o tratamento que se referir a dados de indivíduos localizados no território nacional, bem como situações envolvendo dados pessoais coletados no Brasil.

Ficam, portanto, evidentes os efeitos extraterritoriais da norma que pode, conforme exigência do seu artigo 3º, determinar, inclusive, que um agente de tratamento submeta-se às regras protetivas aos dados pessoais e à privacidade de outros países, em paralelo às suas próprias.

Importante destacar que a LGPD, fundamentada na proteção dos "direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural", também é aplicada a dados pessoais armazenados em meios físicos, que não passaram por processos de digitalização. São considerados dados pessoais fatos, ações e comunicações que tratam de circunstâncias inerentes a um indivíduo identificado ou minimamente identificável, bem como seus meios de processamento, sobre os quais deve recair a tutela jurídica proposta pela LGPD.

Conforme a visão apresentada no artigo 2º da Diretiva Europeia 95/46/CE, dado pessoal é qualquer informação relativa a uma pessoa singular identificada ou identificável, considerando nesta última acepção todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.[36]

Nesse mesmo sentido encontra-se a definição de dados pessoais contida no artigo 5º, inciso I, da LGPD[37], segundo a qual seria a informação, relacionada à pessoa natural identificada ou identificável. A norma também apresenta a divisão do conceito

36 EUROPA. Diretiva Europeia 95/46/CE do Parlamento Europeu e do Conselho. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Luxemburgo: Parlamento Europeu Pelo Conselho, 24 de outubro de 1995. Disponível em: https://www.conjur.com.br/dl/diretiva-europeia.pdf. Acesso em: 27 ago. 2021.

37 Artigo 5º, inciso II e III, da LGPD: 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 (BRASIL, op. cit., 2018).

de dados pessoais conforme a origem, efeitos e potencial de identificação do indivíduo, formalizando a classificação de dados pessoais sensíveis e dos anonimizados.

Os dados pessoais sensíveis são apresentados como aqueles referentes à "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", bem como os "dados genéticos ou biométricos, quando vinculados a uma pessoa natural". Tal visão, é similar a apresentada no RGPD que os indica como dados cujo processamento pode representar um risco maior para os direitos e liberdades individuais.

Outra definição relevante trazida pela LGPD é a que se refere aos dados anonimizados[38], definidos como aqueles relativos à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

A diferenciação proposta pela norma pode ser resumida com a afirmação de que dado pessoal é aquele que identifica ou torna identificável o indivíduo, enquanto o dado anonimizado é aquele que não identifica o indivíduo. Quanto ao segundo grupo, o conceito apresentado deve ser tomado com cautela, uma vez que não se pode descartar a possibilidade de obtenção de novos elementos informativos por meio da combinação de informações brutas[39] em clara afronta ao direito à privacidade. Tanto os dados pessoais sensíveis, como os dados anonimizados, serão objeto de um maior aprofundamento nos próximos tópicos deste estudo.

A este ponto é preciso destacar que a privacidade é pressuposto basilar das normas expressas na LGPD, que direciona suas proteções à figura do titular, compreendido como a pessoa natural a quem se referem os dados pessoais. Nos artigos da lei, é possível perceber a intenção de ampliar sua efetividade por meio do incentivo aos controladores e operadores de dados a formularem regras de boas práticas e governança,

---

38 A saber, O artigo 4º, parágrafo 5 do RGPD fornece a definição de anonimização: "A anonimização é o processo de transformação de dados pessoais de forma a que estes já não possam ser identificados ou não sejam visíveis, utilizando meios razoáveis ao seu alcance. Os meios direitos utilizados devem ser considerados para determinar se o responsável pelo tratamento ou terceiro a quem seja revelado os dados pode ou não identificar um indivíduo." Quando os dados são capturados anonimizados, eles deixam de ser considerados dados pessoais sob a perspectiva do RGPD, desde que não seja possível reverter o processo de anonimização. Essa abordagem permite que as organizações utilizem dados de forma mais segura, preservando a privacidade das pessoas envolvidas. RGPD - REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Acesso em: 19 maio 2023.

39 Técnicas, como o "*profiling*", "*data mining*", "*data warehousing*", "*scoring-system*", entre outros.

em privacidade, com base em pressupostos mínimos descritos no texto mencionado, especialmente nos incisos do § 2º do art. 50. Exemplo disso é a demonstração do comprometimento do controlador em adotar processos e políticas internas a fim de assegurar a proteção dos dados pessoais, estabelecimento de políticas de salvaguarda, plano de ação para casos de incidente, avaliações periódicas, entre outros.[40]

Tais práticas tem a possibilidade de reconhecimento e publicação pela Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados. A Autoridade Nacional de Proteção de Dados será ainda responsável pela promoção e elaboração das diretrizes, estudos, práticas de proteção de dados pessoais e privacidade, bem como edição de regulamentos e procedimentos e relatórios de impacto sobre o tema.

Vinculado a ANPD, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade deverá propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD, bem como elaborar relatórios anuais, estudos, debates, audiências e disseminar conhecimento à população sobre tema.

É perceptível o desafio abraçado pela LGPD no sentido de resguardar o direito à privacidade individual de cada cidadão que faz uso, consciente ou inconscientemente, de instrumentos retentores de dados pessoais. Ao longo de seus artigos foram propostos diversos caminhos para o devido tratamento de dados, fiscalizações necessárias e organização do âmbito de aplicação; contudo a natureza da matéria dificulta a possibilidade de uma orientação precisa. Ainda assim, a LGPD representa

40 LGPD, artigo 50, § 2º: Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
II - Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

um considerável avanço, com significativa relevância em âmbito social, despontando como instrumento imprescindível para a preservação do direito à privacidade.

A partir deste contexto, abre-se via para a reflexão da aplicação da LGPD a questões associadas à saúde. O fluxo gigantesco de dados pessoais diariamente verificado na área da saúde, faz com que o setor desponte como um dos mais impactados pelas normas da LGPD, afetando diretamente a rotina de pacientes, profissionais, planos de saúde, clínicas, laboratórios e hospitais públicos e privados.

Para dimensionar tal impacto é importante destacar que conforme a Agência Nacional de Saúde Suplementar – ANS, até junho de 2022 se contabilizava, mais de 49 milhões de usuários de planos de saúde privados no Brasil[41], sem mencionar o Sistema Único de Saúde – SUS, responsável pelo atendimento maciço da população brasileira. Mediante números tão expressivos, resta claro o desenho de um cenário desafiador no que tange ao tratamento e proteção destes dados de forma adequada.

Conforme o texto da LGPD, cabe a todo estabelecimento comercial atender aos critérios básicos de suas diretrizes, comprometendo-se a seguir seus princípios a fim de assegurar a segurança dos dados pessoais, e proteger o direito e a dignidade de seus titulares. No entanto, no caso de hospitais, clínicas, profissionais de saúde, laboratórios e planos de saúde, é preciso um olhar ainda mais aguçado para efetivar, na prática, a proteção prevista em lei.

Assegurar a privacidade de informações sobre a saúde significa, acima de tudo, neutralizar seu potencial discriminatório[42] sobre o indivíduo, respeitando a restrição ao acesso de informações que poderão prejudicar o desenvolvimento das atividades de sua vida cotidiana e, consequentemente, evitando uma situação de vulnerabilidade civil para aqueles que já convivem com a fragilidade da saúde.

A atenção à saúde, quando mediada por tecnologias da informação e comunicação, as conhecidas TICs, é denominada pela Organização Mundial da Saúde - OMS como e-Saúde[43], englobando todos os processos de assistência ao paciente, pesquisa científica,

41 Dados coletados no sítio eletrônico da ANS: ANS - AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. ANS registra recorde de consumidores em planos de assistência médica. ANS: Ministério da Saúde, 2023. Disponível em: https://www.gov.br/ans/pt-br/assuntos/noticias/numeros-do-setor/ans-registra-recorde-de-consumidores-em-planos-de-assistencia-medica. Acesso em: 11 jul. 2022.

42 SARLET, I. W.; KEINERT, T. M. M. O direito fundamental à privacidade e as informações em saúde: alguns desafios. *In*: KEINERT, T. M. M.; et al. (Orgs.). Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015, p. 87.

43 Em 2005, a Organização Mundial da Saúde (OMS) editou uma resolução recomendando aos seus 192 estados membros o uso da tele-Saúde como estratégia para a melhoria dos sistemas de saúde, em especial os públicos de acesso universal, como o Sistema Único de Saúde (SUS).

educação e capacitação da força de trabalho, monitoração e avaliação em saúde. Em caráter similar, é empregada a nomenclatura Saúde Digital.

Dentre os pontos mais delicados verificados no manuseio dos massivos bancos de dados gerados a partir dos usuários do setor de saúde, seja a base pública ou privada, tem-se as questões envolvendo compartilhamento de dados e as próprias medidas de segurança. Sobre o primeiro ponto, a LGPD expressa claramente em seu artigo 11, que o tratamento de dados pessoais sensíveis somente poderá ocorrer quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas, salvo exceções elencadas na própria lei. Tal regra deve ser considerada tanto para prontuários que serão criados a partir de agora, quanto para dados que já foram coletados e inseridos no sistema, o que demanda a adequação, com a coleta retroativa do termo de consentimento.

Excepcionalmente, será permitido o tratamento dos dados de saúde, bem como de outros dados considerados sensíveis quando esta prática for indispensável ao cumprimento de obrigação legal ou regulatória pelo controlador; Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; 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); Proteção da vida ou da incolumidade física do titular ou de terceiro; Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou 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.[44]

O artigo 11 da LGPD, em seu § 4º, enfatiza ainda a proibição quanto ao compartilhamento de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, à exceção das seguintes hipóteses: casos relativos à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde; para a portabilidade de dados quando solicitada pelo titular; ou ainda em casos de transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde

44 LGPD, Artigo 11, II. (BRASIL, op. cit., 2018).

[45]. Outro ponto que, certamente, merece destaque no posicionamento da LGPD é a proibição imposta aos planos privados de saúde quanto ao 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"[46].

Em que pesem tais proibições, verifica-se a dificuldade de efetivação de proteção face às constantes falhas de segurança de informação, que acabam por permitir a divulgação indiscriminada dos dados de saúde, comprometendo os direitos e causando prejuízos diretos aos usuários. Infelizmente, há registro de centenas de ataque de *hackers* que sequestram e criptografam dados para venda ou com a intenção de obter um "resgate", sob a chantagem de descarte definitivo ou exposição aberta[47].

Por estas e outras ameaças, a LGPD adota como princípios a segurança, ou seja, a 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; E a prevenção enquanto adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.[48]

Espera-se que nos próximos tempos, com as ações de adequação tomando forma mais robusta, se perceba não apenas o reforço as medidas de segurança dos sistemas, mas também um considerável investimento na capacitação de equipes e operadores de dados de saúde, gerando protocolos a serem aplicados em todas as etapas do tratamento de dados na organização, incluindo, desde o agendamento de consultas, acesso e

45 LGPD, Artigo 11, § 4º: É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. Idem.

46 LGPD, Artigo II, § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. Ibid.

47 Como exemplo da situação narrada tem-se a notícia veiculada nas mais diversas mídias em dezembro de 2020: Uma nova falha do Ministério da Saúde expôs dados de cerca de 243 milhões de brasileiros na internet, de acordo com informações do jornal "O Estado de S. Paulo" desta quarta-feira. A TV Globo confirmou os dados revelados pelo jornal, e o Ministério disse em nota que houve exposição de base cadastral, mas que não houve acesso às informações. De acordo com "O Estado de S. Paulo", o vazamento foi causado pela exposição indevida de login e senha de acesso ao sistema do Ministério da Saúde, mesma falha que expôs 16 milhões de pacientes que tiveram COVID-19 na semana passada.

48 LGPD, Artigo 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: 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 (BRASIL, op. cit., 2018).

manuseio à prontuários impressos ou eletrônicos, bem como diagnósticos, exames e receitas.

Com a alteração do formato de atendimentos, popularizados durante o período crítico da pandemia COVID-19, se faz necessária ainda, a reflexão sobre a efetividade das medidas de segurança da informação indicadas, originalmente na LGPD, e em outros documentos no que se refere à prática da telemedicina, na qual não raramente conversas e informações entre paciente e profissionais de saúde são realizadas por aplicativos de mensagem.

É urgente a compreensão de que a concentração de dados de saúde, seja por meio do Cartão Nacional de Saúde implantado no Sistema Único de Saúde (SUS), ou nos prontuários dos planos de saúde e clínicas privadas, configura uma extensão do indivíduo, gerando uma espécie de "avatar" ou "corpo eletrônico", cuja divulgação de forma indevida pode ocasionar uma série de prejuízos e constrangimentos que podem inclusive, ultrapassar a figura de seu titular, atingindo seus descendentes.

2.4 Da definição de dados relacionados à saúde e sua condição enquanto dados sensíveis

Sob o prisma dos profissionais e organizações de saúde, o que se anseia é especialmente por práticas eficazes de adequação e conformidade, o que demanda esforços materiais e intelectuais na implementação de registros, procedimentos, protocolos, sistemas e rotinas capazes de assegurar o devido cumprimento da Lei. Seria este o caminho para assegurar o processamento de dados, garantindo a proteção dos direitos fundamentais das indivíduos.

A reflexão quanto ao manejo dos dados, ganha novas nuances quando se trata de matéria de saúde. A Organização Mundial de Saúde (OMS) afirma que a ideia de saúde deve ser compreendida em sentido amplo, como um estado de completo bem-estar físico, mental e social e, não somente enquanto a ausência de afecções e enfermidades. Logo, trata-se de um processo em constante evolução.

Retomando a noção de dado pessoal, enquanto atributos que são próprios da personalidade de cada um, como por exemplo nome, endereço, telefone e outros que ao serem colhidos, tratados ou transmitidos, tem o potencial de individualizar e identificar seu titular. Dentre estes dados pessoais, verificam-se categorias que

demandam atenção especial, com regras próprias para seu tratamento e manuseio, recebendo a nomenclatura de "sensíveis".

Para solidificar este estudo, é necessário aprofundar o conceito anteriormente apresentado de dados sensíveis, como sendo todos os dados à "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", são considerados sensíveis conforme o artigo da LGPD no artigo 5º, inciso II da LGPD.

A natureza de dado sensível[49] dos dados de saúde, foi reconhecida pela LGPD com o objetivo de indicar situações de repercussão mais severa no âmbito da personalidade, em virtude de um maior potencial discriminatório[50], em situação de publicização inadequada. Dentre as acepções do vocábulo sensibilidade, encontram-se a indicação daquele que recebe facilmente as impressões ou sensações externas e ainda daquilo que se percebe facilmente, por este motivo a nomenclatura dado sensível adotada pela lei se faz oportuna e aparentemente encontra fácil encaixe nas situações que envolvem a saúde.

O RGPD reconhece a natureza especial dos dados pessoais sensíveis de saúde e apresenta disposições específicas para sua proteção, destacando tratar-se de dados particularmente sensíveis, uma vez que fornecem informações íntimas e privadas sobre a saúde de uma pessoa. O conceito de dados pessoais sensíveis de saúde é definido no artigo 4º, parágrafo 15, do diploma europeu, indicando informações relacionadas ao estado físico ou mental de uma pessoa, incluindo o fornecimento de serviços de saúde, bem como dados genéticos e biométricos relacionados à saúde.

Porém, ao tratar dos dados pessoais relativos à saúde, o legislador brasileiro, no texto da LGPD, limitou-se a estabelecer que tais dados são sensíveis, mas sem definilos ou conceituá-los de forma clara, gerando uma tensão em torno da matéria. Tal lacuna reflete o silêncio de legislações antecedentes acerca do tema, a exemplo da Lei nº 12.965/2014, definidora do Marco Civil da Internet; a Lei nº 9.656/1998, que dispõe sobre os planos de saúde; e a Lei nº 13.787/2018, responsável por tratar da

49 Para fins de comparação, no texto da RGPD consta que "os seguintes dados pessoais são considerados «sensíveis» e estão sujeitos a condições de tratamento específicas: dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou orientação sexual da pessoa.

50 FERREIRA, K. P.; RODRIGUES, Y.G. S. A Privacidade no Ambiente Virtual: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil. Revista do Direito do Consumidor, São Paulo, v. 28, n. 122, p. 181-202, 2019. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/131407. Acesso em: 30 mai de 2022.

digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Diante disso, recorre-se ao rol de princípios aplicáveis ao tratamento de dados pessoais, elencados no artigo 6º da LGPD, para aclarar a visão sobre os dados sensíveis relativos à saúde. Dentre os mencionados princípios dispostos na lei encontram-se: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.[51] Na seara dos dados sensíveis de saúde, dois destes ganham especial relevância demandando maior atenção: o princípio da finalidade e o da não discriminação.

Primeiramente, se faz oportuno observar o princípio da finalidade, segundo o qual os dados devem ser tratados para fins determinados, devem ser de conhecimento prévio de seu titular, de maneira explícita e sem que seja possível a sua utilização posterior para outra aplicação. Deve, portanto, haver uma clareza de propósito desde o momento da coleta até o descarte do dado.

Conforme a doutrina, esta regra apresenta extrema relevância prática, vez que fundamenta a restrição da transferência de dados pessoais a terceiros e possibilita a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade, evitando condutas abusivas[52].

O tratamento de dados sensíveis, especialmente sua coleta necessita, de motivação objetiva e bem delimitada a partir de uma finalidade legítima. Neste quadro, também se exige a comunicação ao titular ou responsável acerca de como serão utilizadas as informações coletadas. Quanto aos dados de saúde, destaca-se que tal comunicação

---

51 LGPD, Artigo 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: 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. BRASIL, op. cit., 2018.

52 DONEDA, D. Da privacidade à proteção de dados: Fundamentos da Lei Geral de Proteção de Dados. 3 ed. Rio de Janeiro: Editora Revista dos Tribunais, 2021, p. 216.

deve ser realizada de forma prévia, dando ciência dos manejos antes da entrega de qualquer dado e ainda sob validação prática, por meio da assinatura do termo de consentimento.

O segundo princípio merece um maior destaque em relação a condição dos dados de saúde, enquanto dados sensíveis: o da não discriminação. Por este princípio, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. Entretanto, a LGPD nitidamente reconhece a possibilidade de tratamento distintivo, desde que este seja considerado lícito e não abusivo. Esclarecendo, tem-se pela interpretação da norma que em certos casos seria legítimo ao operador de dados realizar tratamentos diferenciados, desde que tal prática não gere consequências excludentes que poderiam ser consideradas ilícitas.

Em um exemplo prático, seria possível e legítimo que um operador de dados da área de seguros apresente precificação diferenciada para um serviço de seguros de automóveis, considerando características como sexo, idade, condição familiar, entre outros, ofertando valores que reflitam os riscos de danos usualmente ocasionados ou sofridos.

A este ponto surge um importante questionamento sobre a possibilidade desde tratamento segregado, caracterizado como não ilícito e abusivo vir a ser estendido para dados pessoais sensíveis. Porém esta tese, quando aplicada a dados sensíveis, especialmente em matéria de saúde, não se sustenta pelo fato de que esses dados possuem características personalíssimas, tuteladas de forma diferenciada face a seu potencial lesivo, decorrente de uma alta capacidade discriminatória.

Não há dúvidas que o sujeito pode ser amplamente prejudicado em sua vida prática quando incluído em um grupo do qual tenha sido traçado um perfil com conotações negativas[53]. É evidente que o conhecimento referente a pessoas em tratamento contra efeitos do vírus HIV, ou que apresentem outro tipo de comprometimento de saúde, ainda que por questões genéticas, pode gerar discriminações, especialmente, perante seguradoras e relativas ao mercado de trabalho.

Na doutrina, frequentemente se encontram as expressões dados de saúde e dados em saúde sendo utilizadas como sinônimas e sem que seus conceitos sejam propriamente definidos. O RGPD europeu, por outro lado, abraçou a questão e define os dados relativos à saúde como todos aqueles que revelem informações sobre o estado de saúde

53 RODOTÀ, S. A vida na sociedade de vigilância: privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 56.

do titular, tanto físico quanto mental[54]. Uma definição nos mesmos moldes pode ser encontrada na Lei portuguesa nº 12/2005, que estabeleceu informação de saúde como todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar[55].

Embora os conceitos europeus pareçam satisfatórios em um primeiro olhar, a matéria enseja controvérsias. Existem dados de saúde para além da descrição dos dados de saúde. Ocorre que certos dados pessoais, embora não apresentem relação direta com os dados de saúde, conforme o contexto de seu uso, poderiam ser classificados como tal, alçando inclusive a categoria de dados sensíveis.

Tome-se o exemplo de dados obtidos a partir de um aplicativo *Fitness Tracker*[56] sobre a rotina de exercícios e planejamento de ações voltadas para bem-estar e saúde de um certo indivíduo, que podem vir a ser considerados dados pessoais relativos à saúde. A realidade é que conforme o contexto e interseção com outros dados não sensíveis, poderiam estes dados assumir a posição de dados pessoais relativos à saúde, revelando, por exemplo, peso, histórico de doenças, comorbidades, dentre outros.[57]

---

54 O artigo 35 do RGPD afirma que deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho (9), a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro. RGPD, op. cit.

55 O artigo segundo da Lei Portuguesa Lei n.º 12/2005, de 26 de janeiro afirma que "para os efeitos desta lei, a informação de saúde abrange todo o tipo de informação directa ou indirectamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar". PORTUGAL. Lei n.º 12/2005, de 26 de janeiro. Informação genética pessoal e informação de saúde. Lisboa: Assembleia da República; Procuradoria Geral de Lisboa, 2005. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1660&tabela=leis. Acesso em: 30 ago. 2022.

56 Aplicativos pagos ou gratuitos, que oferecem um conjunto de recursos para acompanhar a saúde de seu usuário.

57 Sugere-se a leitura do Parecer ECLI:EU:C:2017:592 emitido pelo Tribunal de Justiça (Grande Seção) da União em 26 julho de 2017, que ao analisar a compatibilidade de um tratado internacional firmado entre o Canadá e a União Europeia em 2014, acabou por se posicionar no sentido de que os dados provenientes do Registro de Nome de Passageiro contém informações sobre a vida privada dos passageiros, dentre elas, situação financeira, relações pessoais, dieta, dados de saúde e outros dados considerados sensíveis, declarando assim, o Acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros é incompatível com os artigos 7.°, 8.°, 21.° e 52.°, n. o 1, da Carta dos Direitos Fundamentais da União Europeia, na medida em que não exclui a transferência de dados sensíveis da União Europeia para o Canadá nem a utilização e a conservação desses dados. UNIÃO EUROPEIA. Tribunal de Justiça (Grande Seção). Parecer ECLI:EU:C:2017:592. 26 jul. 2017. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2017%3A592. Acesso em: 15 jun. 2022.

Seguindo a tendência da União Europeia, o legislador brasileiro tomou o cuidado de estabelecer para os dados pessoais relativos à saúde, um regime jurídico diferenciado visando uma maior efetividade da proposta protetiva. Porém, pela interpretação da norma pátria é possível perceber que o RGPD europeu, mais uma vez, toma um caminho mais acertado, ao atribuir um caráter mais rígido quanto a matéria. Aquele diploma legal estabelece a proibição expressa do tratamento de dados sensíveis, que só poderá ser verificada em situações pontuais, devidamente elucidadas no próprio Regulamento. Essas hipóteses poderão, inclusive, ser revogadas em casos determinados.

Em contrapartida, o ordenamento brasileiro se reveste de maior flexibilidade nas hipóteses em que tal tratamento poderá ser executado, que vão desde a proteção de interesses vitais do indivíduo, até razões de substancial interesse público[58], sem, contudo, especificar claramente quais seriam essas hipóteses, abrindo uma perigosa via para discussões.

Conforme a LGPD, os dados de saúde são propriedade de seu titular, o paciente, afastando o antigo entendimento, segundo o qual a titularidade da informação de saúde seria do profissional ou da organização de saúde. O titular é, portanto, a pessoa natural a quem se referem os dados pessoais sensíveis que são objeto de tratamento[59] e conforme indicado anteriormente, deve consentir a utilização destes desde sua obtenção, tratamento, transmissão, até o momento do descarte.[60]

Para tanto, o Termo de Consentimento Informacional ofertado ao usuário dos serviços de saúde deve ser claro quanto a finalidade a qual se presta, e contar com assinatura do titular ou de seu responsável legal. A ausência do documento válido acarretará a vedação do tratamento de dados pessoais, como forma de coibir erros e vícios da manifestação de vontade[61].

---

58 MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei nº 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, p 159-160, 2018. Disponível em:
https://sisbib.emnuvens.com.br/direitosegarantias/article/download/1603/pdf/. Acesso em:24 maio 2022.

59 LGPD, Artigo 17: Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. BRASIL, op. cit, 2018.

60 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; Idem.

61 LGPD, Artigo 8º: Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. Ibid.

A exigência seria o meio de materialização do princípio da autodeterminação informativa[62], segundo o qual o titular manifesta sua vontade, decidindo onde, quando, por quem e com qual finalidade suas informações serão utilizadas. Nesse sentido, tem-se a indicação de que, sempre que possível, o titular receba ciência sobre quais dados são necessários à coleta, meios de armazenamento, tratamentos realizados, finalidades, e se haverá repasse dos dados à outra pessoa.

2.4.1 O direito à autodeterminação informativa, dados clínicos de caráter pessoal como objeto de direito fundamental: anonimização e pseudoanonimização

A autodeterminação informativa está consagrada como um dos fundamentos da disciplina de proteção de dados pessoais, de acordo com o art. 2º, inciso II, da LGPD, contudo, mais uma vez a norma brasileira se omite quanto a uma definição conceitual. O direito à autodeterminação informativa não é uma construção recente e, observando suas origens, é possível encontrar o sentido proposto na seara da proteção de dados, enquanto o poder concedido ao indivíduo para que ele próprio decida sobre divulgação e utilização de seus dados pessoais.

Em fato, a autodeterminação informativa pode ser encontrada em diversas situações e procedimentos nos sistemas de saúde. Houve Constituições mundo à fora, que embora de modo implícito, abraçaram a causa da democracia e do desenvolvimento social. Dentre estas, merece especial consideração a Lei Fundamental da República Federal da Alemanha (Lei de Bonn), de 1949. Embora não trouxesse, em seu bojo, a expressa previsão à autodeterminação informativa, serviu por base para impedir que o Tribunal Constitucional Federal da Alemanha viesse a reconhecer a existência desse direito, ao enfrentar julgamento sobre a constitucionalidade da Lei do Censo de 1983.

A controvérsia principal se estabelecia à luz do questionário aplicado no recenseamento da população, o qual, não apenas permitia o tratamento dos dados pessoais, mas também assegurava seu compartilhamento entre órgãos públicos.[63]

Na decisão mencionada prevaleceu o entendimento de repudio ao tratamento não transparente de dados pessoais, tomando por base o princípio da dignidade da pessoa

62 Conceito oriundo da terceira geração de leis de proteção de dados pessoais, a autodeterminação informativa, teve origem em decisão do Tribunal Constitucional Alemão a respeito da Lei do Recenseamento de População, Profissão, Moradia e Trabalho de 1982 e se encontra no art. 2º, II, da Lei Geral de Proteção de Dados Pessoais – LGPD, com o objetivo de a garantir ao indivíduo proteção, a partir da necessidade de prévio consentimento do titular para a coleta, armazenamento e tratamento de informações pessoais. Ibid.

63 Recomenda-se a leitura do caso BVerfGE 65, 1, "Recenseamento" (Volkszählung). MARTINS, L. (org.) **Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244-245.

humana e do livre desenvolvimento da personalidade. Na ocasião destacou-se que a quantidade de informações coletadas, em razão do recenseamento, poderia possibilitar a criação de perfis completos da personalidade dos cidadãos, comprometendo a autonomia das pessoas. Além disso, a Corte alemã enfatizou que o tratamento de dados deveria ocorrer somente diante de uma justificativa legal, considerando igualmente a finalidade do processamento.[64]

No Brasil, a autodeterminação informativa é considerada um direito fundamental autônomo, ainda que não venha expresso no texto da Constituição Federal de 1988. Na realidade, trata-se de um direito extraído a partir da interpretação integrada do princípio da dignidade da pessoa humana, do direito à privacidade, e da garantia processual do habeas data[65], visão corroborada pelo recente debate nas Ações Diretas de Inconstitucionalidade nº 6387[66], 6388, 6389, 6393, 6390.

Na ocasião, o Supremo Tribunal Federal definiu que a privacidade só poderá ser mitigada frente à justificativa legítima de que não existam dados insignificantes no contexto atual de automatização de processos[67]. Tal decisão não apenas referendou a proteção constitucional autônoma aos dados pessoais, mas reconheceu que a Magna Carta de 1988 assegura o direito à autodeterminação informativa, devendo o uso dos dados e informações pessoais ser controlado pelo próprio indivíduo, salvo quando a legislação, estritamente determinar.

Ao contrário do que se vivenciou no passado, a base sobre a qual se assentam poder e riqueza já não é necessariamente material. Longe da posse de terras e meios de produção e ainda do próprio acúmulo de capitais, o verdadeiro poder de nossos tempos se encontra na informação, sendo os dados considerados como principal ativo do século 21. Logo, urge a adaptação do Estado no sentido de efetivar a proteção

64 MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. Revista de Ciências Jurídicas Pensar, Fortaleza, v. 25, n. 4, 2020. Disponível em: https://periodicos.unifor.br/rpen/article/view/10828/pdf. Acesso em 22 mai. 2023, p. 7.

65 Artigos 1º, III, e 5º, X e LXXII da Constituição Federal de 1988. BRASIL, op. cit., 1988.

66 ADI 6387, proposta pela Conselho Federal da Ordem dos Advogados do Brasil contra a Medida Provisória nº 954/2020 tratava da relação entre as empresas de telecomunicações que compartilhavam diversos dados pessoais de seus consumidores com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), que utilizaria os dados "exclusivamente" para realizar pesquisas domiciliares por telefone. BRASIL. Supremo Tribunal Federal – STF. Ação Direta de Inconstitucionalidade – ADI 6387. Medida cautelar na ação direta de inconstitucionalidade 6.387 Distrito Federal. Relatora Ministra Rosa Weber. Brasília: STF, 2020. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 30 maio 2022.

67 Em seu voto o Ministro Luiz Fux entendeu "que a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada".

quanto à privacidade e da autodeterminação em relação aos dados pessoais de seus cidadãos.

Tem-se no direito à autodeterminação informativa, o meio de assegurar o controle do cidadão relativo às suas próprias informações, possibilitando o domínio sobre os seus dados pessoais, ainda que o tratamento dessas informações seja legítimo[68]. Deste modo, se enfatiza a proteção para os dados pessoais, ultrapassando o conceito de intimidade, conduzindo a privacidade para o âmbito procedimental, visão cuja materialização ficou a cargo da LGPD.

Como ferramenta prática para assegurar a proteção dos dados sensíveis de saúde, a norma brasileira propõe anonimização de dados, a qual pode ser entendida como uma técnica de processamento de dados que remove ou modifica informações capazes de identificar uma pessoa. Essa técnica resulta em dados anonimizados, que não podem ser associados a nenhum indivíduo específico, além de ser também um componente importante do compromisso das Empresas públicas e privadas.

Com a análise de dados anonimizados, é possível criar produtos e recursos seguros e valiosos, como o preenchimento automático de uma consulta de pesquisa inserida, e detectar com mais precisão as ameaças à segurança, como *sites* de *phishing e malware*[69], além de proteger a identidade dos usuários. Ainda permite compartilhar, também, externamente e com segurança os dados anonimizados, tornando-os úteis para outras pessoas sem colocar a privacidade dos usuários em risco.

Conforme a leitura do artigo 5º, inciso III, da LGPD, são dados anonimizados aqueles que relativos a um "titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Em complemento, o inciso XI do mesmo artigo, afirma que anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos

68 LEONARDI, M. Tutela e privacidade na internet. São Paulo: Editora Saraiva, 2011, p. 67-68.

69 São chamados "*Malware"* todo tipo de software malicioso usado para causar prejuízo, que pode ser até financeiro, danificar sistemas, interceptar dados, afetando tanto computadores como celulares e até redes inteiras. O termo que vem da fusão da palavra inglesa "*malicious*", aqui traduzida como malicioso, com a palavra "software" e atualmente é utilizada para definir qualquer tipo de aplicação cujo objetivo é causar danos ou qualquer tipo de prejuízo ao usuário. Já o "*phishing*" seria qualquer tipo de fraude por meios de telecomunicação, que usa truques de engenharia social para obter dados privados das vítimas. A expressão é a associada a ideia de que cibercriminoso vai "pescar", no inglês, se usa a palavra "*fishing*". Nesta prática ilícita, se utiliza algum tipo de isca para fisgar as vítimas que navegam nas redes. O ph em "phishing" vem de "phreaking de telefone", termo que surgiu em meados de 1900, no qual os "phreaks", ou seja, entusiastas, faziam experimentos com as redes de telecomunicações para descobrir como elas funcionavam. Phreaking + fishing = phishing. BELCIC, I. Avast Academy: Segurança. Publ. 5 de fevereiro de 2020. Disponível em: https://www.avast.com/pt-br/cphishing#:~:text=Phishing%20nos%20sites%3A%20Os%20sites,login%20nas%20suas%20contas%20reais. Acesso em 15 jun. 2021, p. 2.

quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". A anonimização surge de forma recorrente em outros tópicos da LGPD, sempre com o objetivo de prover segurança no sentido de que os dados pessoais envolvidos percam a possibilidade de associação e identificação, direta ou indireta, a um indivíduo.[70]

É exatamente o que se prevê no caso da autorização do paciente para o tratamento de dados pessoais que permitam a realização de estudos por órgão de pesquisa, "garantida, sempre que possível, a anonimização dos dados pessoais", prevista pelo artigo 7º, IV da LGPD, bem como na hipótese de utilização de dados pessoais para realização de estudos em saúde pública, indicada no artigo 13 da referida lei. Em ambas as situações, os dados sensíveis, por serem considerados indispensáveis e de interesse social, os são coletados sem o consentimento expresso do titular, nestes casos, protegido pela prática da anonimização. Outros casos de anonimização também encontram amparo na LGPD, como por exemplo a conservação de dados após o término do seu tratamento para finalidades de estudo por órgão de pesquisa e para uso exclusivo do controlador.[71]

Por estas situações, resta clara a intenção do legislador em utilizar a anonimização como forma de legitimação, seja para autorizar um tratamento, seja para autorizar armazenamento mesmo após o término de um tratamento, descaracterizando os dados pessoais. Neste sentido, o artigo 12 da LGPD afirma que os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

E em sequência procura elucidar em seu parágrafo primeiro o que seria considerado razoável para este fim, indicando observar fatores como custo e tempo necessários para

70 Anonimização, anonimizar, anonimizado são expressões recorrentes no texto da LGPD, vejamos: no art. 7º, inciso IV, definindo uma hipótese de tratamento de dados pessoais para fins de realização de estudo por órgão de pesquisa, "garantida, sempre que possível, a anonimização dos dados pessoais"; no art. 11, que trata de dados pessoais sensíveis; no art. 12, que trata especificamente de dados anonimizados, são 4 ocorrências; no art. 13, que trata da realização de estudos em saúde pública; no art. 16, sobre a eliminação dos dados após o tratamento, inciso II, que autoriza a conservação dos dados após o seu tratamento, para fins de estudo por órgão de pesquisa, com anonimização sempre que possível, e no inciso IV, para uso exclusivo do controlador, desde que anonimizados; no art. 18, inciso IV, que garante como direito do titular a possibilidade de saber sobre "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade" com o disposto na LGPD e também nos parágrafos 6º e 7º. BRASIL, op. cit., 2018.

71 LGPD, Artigo 16: Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I -cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Idem.

reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.[72]

Avançando nestes critérios, tem-se o custo, com a necessidade de avaliar o gasto de recursos financeiros e humanos para realizar a reversão de um processo de anonimização, considerando a tecnologia disponível no momento e o tempo, que se refere a extensão da tarefa. Outro critério apresentado se pauta na figura do agente de tratamento de dados e seus recursos para concretizar a reversão, o que será indicado certamente por uma avaliação subjetiva. E por fim, há de se considerar como se comportam os dados externamente, considerando a viabilidade de terceiros reverterem a anonimização por meios próprios. Assim, a possibilidade de identificação deve ser avaliada em duas perspectivas distintas: a do agente de tratamento e a de qualquer terceiro.[73]

Para realizar um processo de anonimização, deve-se primeiramente, definir quais conjuntos de dados deverão ser anonimizados, bem como qual será a técnica aplicada a cada um destes atributos.[74] Ao configurar uma propriedade ou característica de um objeto, os atributos podem ser classificados a partir da sensibilidade da informação que contém como atributos identificadores, aptos a designar o indivíduo, a exemplo de documentos pessoais tais como o cadastro de pessoas físicas – CPF; atributos semi-identificadores, passíveis de combinações com informações externas que poderiam vir a identificar ou expor o indivíduo, como por exemplo, data de nascimento ou o código de endereçamento postal – CEP. E por fim, atributos sensíveis, que revelam as condições específicas dos indivíduos a exemplo dos dados de saúde.[75]

---

72 Tal raciocínio segue a indicação do item 26 da exposição de motivos do RGPD. RGPD, op. cit.

73 Conforme a doutrina recente, existem abordagens relativistas e absolutistas quanto à questão. Para a linha absolutista a perspectiva, enquanto controlador ou terceiro, é irrelevante desde que os dados se qualifiquem como dados pessoais, uma vez que qualquer sujeito deve proteger os direitos do titular dos dados. Para a segunda corrente, a abordagem absoluta elimina a necessidade de qualquer gerenciamento de riscos por parte dos agentes de tratamento. A adoção de uma abordagem absoluta poderia levar ao descarte da existência de dados anônimos, já que sempre haverá alguém com o interesse de identificar um conjunto de dados que foi anonimizado. Mediante o antagonismo das visões, surge ainda, uma abordagem intermediária, baseada na figura do "intruso motivado", que seria um terceiro "razoavelmente competente" e com acesso a recursos como Internet, bibliotecas, documentos públicos. Contudo, não é necessário que este tenha conhecimento especializado, habilidades hackers ou acesso a equipamentos especiais. FINCK, M.; PALLAS, F. They who must not be identified: distinguishing personal from non-personal data under the GDPR. International Data Privacy Law, Oxford, v. 10, n. 1, p. 11-36, 2020. Disponível em: https://doi.org/10.1093/idpl/ipz026. Acesso em: 30 maio 2022, p. 25.

74 Nas ciências da computação, são considerados atributos os elementos de dado que contém informação que descreve uma relação. Seriam ainda, uma propriedade ou característica de um objeto. Uma relação deve ter um atributo ou combinação de atributos que identificam cada ocorrência. Estes atributos formam a chave primária da relação.

75 SILVA, H. O. Uma abordagem baseada em anonimização para privacidade de dados em plataformas analíticas. 2019. 117 f. Dissertação (Mestrado em Tecnologia)– Universidade Estadual de Campinas, Limeira, 2019, p.28.

Em que pese as diferentes técnicas para tornar dados anônimos, as abordagens mais comuns são a aleatorização e a generalização. A primeira, tem por objetivo tornar os dados imprecisos. Em seu processo, ocorre a alteração da veracidade dos dados a fim de eliminar a estreita ligação entre os dados e o indivíduo. A segunda abordagem mencionada, denominada generalização, promove a diluição dos atributos dos titulares dos dados através da alteração da escala ou ordem de grandeza.[76] Cada abordagem comporta diversas técnicas, mas até o momento, nenhuma foi considerada completamente segura, corroborando a ideia de que os dados podem ser úteis ou perfeitamente anônimos, mas nunca os dois[77].

Na realidade a anonimização não consegue cumprir fielmente seu papel enquanto meio de assegurar a proteção dos dados pessoais, sendo prejudicada pelos processos de reidentificação. Sempre que dados anonimizados são novamente associados a seus titulares de maneira bem-sucedida, mesmo que se revelem aparentemente sem sentido, há a ampliação do potencial de risco para a privacidade, visto a facilitação para uma reidentificação futura de maior precisão.

Todo processo de anonimização de dados é passível de riscos para a privacidade do indivíduo, sendo os principais a possibilidades de identificação, ligação e inferência. A saber, mesmo após a anonimização existe a possibilidade de isolar alguns ou todos os registros que identifiquem uma pessoa. Também pode se verificar a conexão de pelo menos dois registros sobre a mesma pessoa; e por fim, não se descarta a possibilidade de deduzir, com uma probabilidade significativa, o valor de um atributo a partir dos valores de um conjunto de outros atributos.

O termo "anonimização" é criticado neste cenário, sob a acusação de apresentar de uma ideia ilusória, visto que não há garantia quanto a permanência na condição de dados não pessoais. Porém, em que pesem os riscos, a anonimização continua sendo a ferramenta utilizada nas mais diversas iniciativas associadas à coleta de dados, especialmente na área de saúde, a exemplo do que se verificou durante o auge das ações de combate à pandemia de COVID-19.

Entende-se que a anonimização é um mecanismo que busca garantir proteção à personalidade humana por meio do desfazimento de qualquer tipo de vínculo capaz de associar, direta ou indiretamente, um dado ao seu respectivo titular, valendo-se,

76 A título de exemplo, seria indicar uma região em vez de uma cidade, um mês em vez de uma semana.

77 OHM, P. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review, Rochester, v. 57, p. 1701-1777, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em: 20 jun. 2023, p. 1701.

para isso, da utilização de meios técnicos razoáveis e disponíveis no momento do tratamento dos dados pessoais.

Não é por outro motivo que tal mecanismo, além de ser um direito do titular de dados pessoais quanto aqueles considerados desnecessários, excessivos ou tratados em desconformidade com a lei (art. 18, IV, da LGPD), deverá também ter, sempre que possível, sua aplicação garantida no tratamento de dados pessoais sensíveis para a realização de estudos por órgãos de pesquisa (artigos 7º, inciso IV e 11, ambos da LGPD).

A anonimização dá origem ao chamado dado anonimizado que, por sua vez, é considerado o oposto do dado pessoal. Pelo seu significado semântico, seria aquele incapaz de revelar a identidade de uma pessoa e, por isso, não apresentaria necessidade de proteção legal.

A discussão acerca da anonimização de dados ainda encontra outro importante desdobramento com o conceito de pseudoanonimização[78], que apresentado pela LGPD como alternativa específica à anonimização, na hipótese de tratamento de dados para a realização de estudos em saúde pública por órgãos de pesquisa.[79] A pseudoanonimização é uma forma de tratamento na qual se verifica a substituição das informações contidas num conjunto de dados que identifica um indivíduo por um identificador artificial, um pseudônimo.[80] Desta forma, serão criadas duas bases de dados, sendo a primeiro com a utilização do pseudônimo e a segundo conteria a referência relativa aos pseudônimos, de modo que o processo de reidentificação só seria possível mediante a junção das duas bases de dados.

Para fins de pseudoanonimização, são utilizadas duas técnicas com a finalidade omitir os dados de uma pessoa natural. Conforme as chaves utilizadas, tem-se a pseudoanonimização simétrica e a assimétrica. Na primeira, uma mesma chave é usada para criptografar os dados e, posteriormente, torná-los legíveis novamente, todavia, há

78 O prefixo "pseudo" é utilizado na língua portuguesa para indicar algo que superficialmente parece ser uma coisa, mas é outra coisa. Sujeito ao contexto, pseudo pode conotar coincidência, imitação, engano intencional ou uma combinação dos mesmos. Aplicado na composição do termo "pseudoanonimização", indica um procedimento alternativo, sem o mesmo grau de eficácia da anonimização quanto a proteção de dados pessoais.

79 LGPD, Artigo 13: Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoaninimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. BRASIL, op. cit., 2018.

80 LGPD, Artigo 13, § 4º Para os efeitos deste artigo, a pseudoaninimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Idem.

o problema de como compartilhar a chave sem que ela se torne vulnerável. Na segunda existem duas chaves diferentes: a primeira utilizada para criptografar os dados- visível para qualquer pessoa- e a segunda para decifrá-los, cujo acesso pertencerá somente ao destinatário, de modo a evitar o compartilhamento.

A pseudoanonimização é adotada pelo RGPD, que a aponta como uma técnica apta a minorar riscos para os titulares de auxiliar os responsáveis pelo tratamento e os seus subcontratantes a cumprir suas obrigações estabelecidas pelo regulamento. Aponta ainda que os dados pseudoanonimizados deverão ser considerados como informações sobre uma pessoa natural identificável. Contudo o legislador europeu não deixou de registrar os riscos envolvidos nestes processos, enfatizando em suas motivações que se as medidas não são adotadas de forma adequada e, no caso da pseudoanonimização, venha a ocorrer uma inversão não autorizada, essa violação pode vir a causar danos aos titulares, devendo ser notificada à autoridade.[81]

No que diz respeito à segurança do tratamento de dados pessoais, a pseudoanonimização surge como medida técnica apta a assegurar um nível de segurança adequado ao risco (Art. 32, Item 1, c). O RGPD também sugere que esta técnica esteja presente em códigos de conduta elaborados pelos responsáveis pelo tratamento ou por subcontratantes (Art. 40º, Item 2, d).

O artigo 4º, item 5 do RGPD define a pseudoanonimização como uma forma de tratamento na qual os dados pessoais deixam de poder ser atribuídos a uma pessoa natural específica sem recorrer a informações suplementares, desde que estas sejam mantidas separadamente, e sujeitas a medidas técnicas e organizativas que impeçam a identificação.

O critério a ser adotado para determinar qual técnica deverá ser utilizada deve ser a da maior efetividade, ou seja, deve-se optar por aquela que traga mais segurança ao processo. Assim, mediante o caso concreto, caberá uma avaliação quanto aos métodos, definindo a possibilidade da pseudoaninimização ser ou não suficiente para garantir a

81 RGPD, Exposição de Motivos, Razão 85: Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares. Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá notificá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada. RGPD, op. cit.

segurança do tratamento dos dados, com a diminuição do risco de revelação indevida desses dados. Em uma avaliação negativa, a escolha deve ser pela anonimização.

Apesar da falibilidade técnica e do potencial de reversibilidade, tanto a anonimização, como a pseudoanonimização são consideradas medidas mitigadoras de riscos no tratamento de dados pessoais. Todavia, é preciso ter em vista que sua utilização deve vir materializada por procedimentos transparentes, nos quais os interessados tenham ciência dos riscos, a partir da perspectiva de que a esta altura, ainda não se verificam modelos livres de falhas, no que se refere à preservação da privacidade.

Como se pode depreender, o processo de pseudonimização contribui com o cumprimento da obrigação de proteção de dados pelos responsáveis por seu tratamento e, por consequência, reduz os riscos para os titulares de dados. Porém, por não garantir de maneira absoluta o afastamento de qualquer risco de identificabilidade, os dados pseudoanonimizados permanecem adstritos aos ditames da Lei Geral de Proteção de Dados Pessoais.

Assim, para um dado para ser considerado anônimo ou anonimizado e, portanto, livre da incidência da Lei Geral de Proteção de Dados Pessoais, precisa ser desprovido de qualquer tipo de informação identificável.[82] As questões envolvendo segurança de dados sensíveis, exigem ainda, diretrizes claras de tratamento e condução a ser observadas por profissionais e usuários do sistema de saúde. Desta forma, o próximo item se dispõe a analisar o posicionamento da LGPD em relação aos indivíduos considerados como principais atores nas relações envolvendo saúde no Brasil.

2.4.2 Os atores das relações de saúde sob o prisma da LGPD

Ao reconhecer o caráter sensível dos dados pessoais de saúde, a LGPD determina uma série de medidas de segurança, tanto de caráter técnico quanto administrativo, a serem adotadas por seus agentes como forma de assegurar a proteção dos dados pessoais de tratamento inadequado por situações acidentais ou ilícitas. Embora as

82 O Caso Netflix Prize. Como exemplo cita-se o caso Netflix Prize em que os pesquisadores Arvind Narayanan e Vitaly Schmatikov reidentificaram a base de dados que havia sido anonimizada por meio da técnica de randomização. Em resumo, a provedora de *streaming* de filmes criou um concurso visando a melhoria do desempenho de seu algoritmo de sugestões aos seus clientes. Para isso, disponibilizou sua base de dados, referente ao período de 1998 a 2005, com apenas data e nota de avaliação, suprimindo os nomes dos usuários avaliadores. Os pesquisadores mencionados, então, desenvolveram um algoritmo apto a calcular quantos *bits* de informação seriam necessários para reverter o processo e identificada a quantidade, recorreram às informações publicamente disponíveis e acessíveis no Internet Movies Databases/ IMDB. Correlacionaram tais informações com as existentes na base de dados disponibilizada e encontraram a identidade dos usuários avaliadores. O exemplo demonstra, portanto, que uma base de dados embora anonimizada, pode ser reidentificada com base no cruzamento de dados presentes em outras bases disponíveis.

profissões da área da saúde apresentem regulação própria para o sigilo profissional relativo às informações do paciente, a realidade da rápida expansão dos gigantescos bancos de dados gerados dentro dos procedimentos de saúde digital, requer, sem dúvidas, medidas mais sólidas.

Coube à LGPD estabelecer obrigações adicionais e novos parâmetros a serem adotados como padrões de conduta para o tratamento dos dados pessoais pelas instituições de saúde, incluindo neste meio, os dados pessoais dos próprios profissionais, colaboradores e parceiros.

No que se refere à extensão quanto a matéria de saúde, o disposto na alínea f do inciso II do artigo 11 da LGPD, abrange profissionais de saúde, os serviços de saúde[83] e ainda, a autoridade sanitária. Esclarecendo melhor, entende-se por profissionais de saúde pessoas naturais formadas em algum ramo da ciência que seja relacionado com a vida, saúde ou doença humana[84].

Já os serviços de saúde são aqueles prestados em estabelecimentos voltados para à promoção da saúde do indivíduo, com o objetivo de protegê-lo de toda a sorte de doenças e agravos, além de prevenirem e limitarem eventuais danos que possam ser causados à pessoa, objetivando a reabilitação de sua capacidade física, psíquica e social quando afetada.[85]

E por fim, as entidades sanitárias que são definidas como órgão ou agente público competente da área da saúde, com atribuição legal no âmbito da vigilância e da atenção à saúde, nos termos da pelo artigo 4º, inciso III da Portaria nº 1.139/2013, do Ministro da Saúde[86]. Podem ser consideradas como autoridades sanitárias, qualquer

83 A redação original da LGPD mencionava expressamente os serviços de saúde, o que acarretava a consequente exclusão da permissão de tratamento de dados pessoais sensíveis ligadas à saúde pelas entidades privadas. Porém, este equívoco foi corrigido pela Lei n.13.853/2019, que alterou a redação do inciso VIII do artigo 7º e à alínea f do inciso II do artigo 11 da LGPD, para incluir os serviços de saúde e em consonância com o texto constitucional que permite a atuação privada na saúde. BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 12 jul. 2022.

84 COTS, M.; OLIVEIRA, R. **Lei Geral de Proteção de Dados Pessoais comentada.** 2. ed. São Paulo: Editora Revista dos Tribunais, 2019, p. 85.

85 Conceito extraído do sítio eletrônico da Agência Nacional De Vigilância Sanitária – ANVISA, 2022. ANVISA – AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. Página Inicial. Brasília, Ministério da Saúde, 2022. Disponível em: https://www.gov.br/anvisa/pt-br. Acesso em: 22 jul. 2022.

86 BRASIL. Portaria n. 1.139, de 10 de junho de 2013. Define, no âmbito do Sistema único de Saúde (SUS), as responsabilidades das esferas de gestão e estabelece as Diretrizes Nacionais para Planejamento, Execução e Avaliação das Ações de Vigilância e Assistência à Saúde em Eventos de Massa. Brasília: Ministério da Saúde, 2013. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2013/prt1139_10_06_2013.html. Acesso em: 24 mai. 2022.

ente de direito público que tenha por objetivo garantir a preservação da saúde pública, seja este integrante da administração direta ou indireta.

Mesmo diante de tais definições, mais uma vez percebe-se que as proteções pretendidas são prejudicadas pelo silêncio do legislador quanto a delimitação do alcance das expressões utilizadas. Note-se que a expressão "procedimento" empregada pela lei é extremamente ampla, carecendo de uma elucidação, que provavelmente ficará a cargo da ANPD no futuro, como forma de precisar o alcance dessa base legal. Apesar da falha, prevalece a interpretação de que a tutela ofertada pela LGPD deve ser estendida a todo a procedimento realizado que tenha por objetivo a proteção à saúde.

A LGPD também se posiciona quanto ao tratamento de dados pessoais para fins de estudos em saúde pública, assegurando o acesso dos órgãos de pesquisa às bases de dados pessoais para fins de estudos em saúde pública, conforme o disposto em seu artigo 13[87]. No caput do mencionado artigo, o legislador estabelece que o acesso às bases de dados pessoais deverá obedecer a procedimento estrito, com o tratamento realizado exclusivamente dentro do órgão e mediante a comprovação da finalidade de estudos e pesquisas.

Além disso, exige-se a manutenção de ambiente controlado e seguro, conforme práticas de segurança determinadas por regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoanonimização dos dados, e ainda a consideração de padrões éticos. Há, portanto, o requisito técnico da finalidade de estudos em saúde pública, limitando o acesso dos órgãos de pesquisa.

Os referidos órgãos de pesquisa encontram definição no artigo 5º, inciso XVIII da norma, sendo considerados como todo órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão

87 LGPD, ARTIGO 13: Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências. § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. BRASIL, op. cit., 2018.

institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Importante destacar que ao afirmar que o tratamento de dados pelo órgão de pesquisa deverá ocorrer exclusivamente dentro do órgão, o legislador impôs uma restrição, que abre margem à interpretação de que tal tratamento só poderá ser realizado dentro da estrutura organizacional do órgão e consequentemente sob sua supervisão. No entanto, tal interpretação perde força face aos fundamentos da proteção de dados, a saber, o desenvolvimento econômico e tecnológico e a inovação, que contrariam a imposição de restrição para uma pesquisa científica com finalidade comprovada.[88]

Outro ponto relevante é a consideração de padrões éticos[89] nos estudos e pesquisas mencionados. Percebe-se que a LGPD impôs padrões éticos, exigindo que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em hipótese alguma, revele dados pessoais. Ou seja, na prática para que haja a divulgação dos resultados ou mesmo de excertos do estudo, deverá ser realizada pelo menos a pseudoanonimização dos dados.

Aprofundando o tema, propõe-se a análise dos conceitos e delimitações da atuação dos agentes de tratamento de dados. Em sede de saúde, os agentes de tratamento de dados receberam a responsabilidade de implementar medidas de proteção e segurança dos dados na esfera interna. A este ponto, é de suma importância revisitar o texto da LGPD para também compreender as designações utilizadas quanto às pessoas ou entidades responsáveis pelo manuseio e tratamento de dados. Conforme a lei, são denominados agentes de tratamento, os indivíduos que irão manipular os dados pessoais de outrem, sendo classificados nas figuras do controlador e do operador de dados.[90]

---

88 LGPD, Artigo, 2º: A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. BRASIL, op. cit., 2018.

89 A título de exemplos pode ser citada a Resolução n. 466/201246, do Conselho Nacional de Saúde que disciplina as pesquisas realizadas envolvendo seres humanos. BRASIL. Resolução nº 466, de 12 de dezembro de 2012. A presente Resolução incorpora, sob a ótica do indivíduo e das coletividades, referenciais da bioética, tais como, autonomia, não maleficência, beneficência, justiça e equidade, dentre outros, e visa a assegurar os direitos e deveres que dizem respeito aos participantes da pesquisa, à comunidade científica e ao Estado. Projetos de pesquisa envolvendo seres humanos deverão atender a esta Resolução. Brasília: Presidência da República, 2012. Disponível em: https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf. Acesso em: 30 maio 2022.

90 LGPD, Artigo, 5º. IX: agentes de tratamento: o controlador e o operador. BRASIL, op. cit., 2018.

O controlador de dados, enquanto agente de tratamento poderá ser uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Seria, portanto, o principal agente de tratamento responsável, uma vez que deverá definir a finalidade e os motivos para o tratamento de dados pessoais.[91]

A LGPD, atribui ao controlador responsabilidades específicas como comunicar incidentes à ANPD, elaborar o Registro das Atividades de Tratamento de Dados Pessoais – ROPA e ainda, o dever de apresentar, quando requerido, um relatório de impacto à proteção de dados, contendo a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.[92]

Quanto a figura do operador, enquanto agente de tratamento de dados, este poderá ser uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Sua atuação se dá a partir das orientações e instruções lícitas do controlador, conforme explica o artigo 5º, inciso VII, da LGPD[93]. Controlador e operador responderão por seus atos relativos ao tratamento de dados, matéria que será discutida nos capítulos finais desse estudo.

Conforme os conceitos apresentados, infere-se que a LGPD distingue as duas figuras especialmente pelo poder de decisão, atribuindo ao controlador o papel de comando, enquanto o operador atuaria de forma subordinada a este. Como recurso para aclarar a questão no que se refere à esfera de saúde, seguem dois exemplos extraídos do Guia Orientativo da Autoridade Nacional de Proteção de Dados para definições dos agentes de tratamento da própria ANPD. Como primeiro exemplo, tem-se a figura de uma médica, profissional liberal, que armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório.

---

91 LGPD, Artigo, 5º, VI: controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; Idem.

92 LGPD, Artigo, 38: A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Ibid.

93 LGPD, Artigo 5º, VII: operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; Ibid.

A médica, enquanto pessoa natural, é a controladora dos dados pessoais, não estando subordinada a outrem. Em uma segunda hipótese, a médica é empregada de um hospital, constituído sob a forma de associação civil sem fins lucrativos, e atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes. O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador neste caso e tem a médica atuando sob seu poder diretivo.[94]

Por fim, há que se mencionar a figura do encarregado de proteção de dados[95], descrita no artigo 5º, inciso VIII, como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD[96]. Tal função exige confiança e transparência, visto que implica no acesso aos dados pessoais e às operações de tratamento das instituições. Segundo a LGPD, a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador[97], o que facilitará o acesso dos titulares de dados ao empreendimento em caso da necessidade de realizar alguma solicitação.

As atividades do encarregado, também se encontram elencadas na lei e estão divididas entre a comunicação e a manutenção do programa de compliance[98]. No primeiro caso, o encarregado atua como elo de comunicação entre as partes do processo de tratamento de dados, sejam internas ou externas, interagindo com colaboradores, titulares, ANPD, prestadores de serviços, entre outros.

A título de exemplo, sempre que houver alguma reclamação ou solicitação por parte do titular de um dado pessoal (um cliente, por exemplo), é o encarregado que a recebe e toma as devidas providências. Também caberá ao encarregado receber os

94 ANPD - Autoridade Nacional de Proteção de Dados. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 20 jul. 2022.

95 Também denominado DPO (*Data Protection Officer*).

96 A figura do encarregado passou por importantes mudanças no texto da LGPD. Conforme o texto originalmente aprovado do diploma, restava explícita a necessidade de o encarregado ser uma pessoa natural. Porém, a Medida Provisória nº 869 e depois pela Lei nº 13.853 de 2019, alteraram o texto original, de modo que já não existe a forma, atualmente há a possibilidade de que a função de encarregado, seja exercida por pessoa jurídica, o que abre espaço para o surgimento de empresas especializadas.

97 LGPD, Artigo 41, § 1º. BRASIL, op. cit, 2018.

98 Com origem vem no verbo em inglês "*to comply*", a ideia de compliance indica o dever de agir de acordo com uma ordem, um conjunto de regras ou um pedido. No mundo das corporações, compliance diz respeito à conformidade ou até mesmo à integridade corporativa. Em outras palavras, significa estar alinhado às regras da empresa, assegurando que sejam observadas e cumpridas atentamente.

comunicados da ANPD e adotar as devidas providências. Essa amplitude de conexões e seus desdobramentos justifica a já mencionada necessidade de disponibilização do contato e identificação do encarregado.

Nesta seara, cabe ainda ao encarregado a construção e manutenção da cultura de privacidade e proteção de dados, conscientizando e capacitando pessoas, além de aprimorar procedimentos e serviços por meio da divulgação e ampliação das boas práticas dentro da própria empresa.

No que se refere ao segundo caso, com a manutenção do compliance, as ações do encarregado deverão ser no sentido de orientar os agentes de tratamento de dados sobre estas medidas de segurança ou *compliance*[99], sem, contudo, assumir responsabilidade pelo seu descumprimento. Seu objetivo principal é fazer valer o que está disposto na LGPD e nas demais Leis de Proteção de Dados do mundo que possam ser aplicáveis, bem como facilitar o acesso dos titulares aos seus direitos.

A figura do encarregado é indispensável para assegurar a *compliance,* bem como se mostra fundamental para a estrutura interna de governança de dados na proteção e controle das informações.

Feita a análise sobre os agentes do tratamento de dados, é preciso dedicar atenção sobre as permissões deste tratamento em matéria de saúde. Cuida o artigo 11 da LGPD em apresentar permissões para o tratamento de dados sensíveis, indicando, primeiramente, a hipótese do consentimento por parte do titular ou seu responsável legal. Destaca também a possibilidade da realização do tratamento de dados sem fornecimento de consentimento do titular, em uma série de casos específicos, dentre os quais ressalta-se a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, conforme objeto deste escrito.

Em que pese estas disposições, é imperioso recordar que o setor de saúde possui características próprias que demandam uma disciplina específica quanto ao tratamento de dados pessoais sensíveis, quando dispensado o consentimento do titular. A redação do inciso II do artigo 11 da LGPD dispõe que a dispensa do consentimento do titular somente ocorrerá nas hipóteses em que ela for indispensável para a situação disciplinada. [100]

---

99 Como exemplo destas medidas é possível citar o desenvolvimento e gestão dos programas de governança, a estruturação de processos, a atualização de manuais e políticas, bem como acompanhamento e definição de medidas de segurança.

100 LGPD, Artigo 11, 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 compartil-

Deste modo, resta claro que nem toda situação autoriza o uso de dados pessoais sensíveis sem o consentimento de seu titular para fins para de saúde. A regra deve ser aplicada somente a casos em que o procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária dependam efetivamente do tratamento de dados pessoais sensíveis.

Portanto, a possibilidade de tratamento de dado pessoal sensível deverá ser observada conforme a situação concreta que demanda razoabilidade e cautela por parte do profissional de saúde, a fim de se evitar qualquer conduta que venha a ferir os preceitos da LGPD.

Ao tempo em que as tecnologias da informação se apresentam como uma alternativa promissora para a redução dos custos, aumento do acesso e para a melhoria dos serviços de saúde, amplia-se a preocupação com o tratamento destes dados, a partir da enorme e crescente disponibilidade de informações sobre doenças e pacientes.

O acesso facilitado de registros para o paciente e a possibilidade de compartilhá-los com os profissionais de sua confiança pode ser uma grande ferramenta para melhoria dos cuidados de saúde. Todavia, é necessário refletir sobre a relação entre acesso à informação e privacidade, derivada da utilização massiva de registros médicos de pacientes e buscar resposta para uma questão latente: como viabilizar avanço do conhecimento propiciado pelo uso desses dados e, simultaneamente, assegurar a privacidade e o sigilo das informações individuais, garantindo a dignidade do usuário dos serviços de saúde?

Em busca de elementos para aclarar a questão e ampliar os conhecimentos sobre a matéria proposta, dar-se-á início no capítulo seguinte a análise do ordenamento pátrio em matéria de saúde face as tecnologias mais recentes. A partir da discussão quanto a dimensão informativa do direito à saúde, propõe-se analisar a questão da informatização de dados sensíveis, a partir do contexto das constantes evoluções tecnológicas na sociedade da informação.

---

hado 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; 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. BRASIL, op. cit., 2018.

3 Capítulo 2 - O direito à saúde e as tecnologias na sociedade da informação

O segundo capítulo da tese aborda a influência das tecnologias nas questões de saúde e seus desdobramentos face ao ordenamento jurídico brasileiro. Para tanto, se inicia com a discussão quanto a dimensão informativa e do direito à saúde, e discute a delicada questão da informatização de seus dados, enquanto sensíveis. Em matéria de saúde, a informação desempenha papel fundamental no processo decisório, uma vez que auxilia no conhecimento sobre as condições de saúde, mortalidade e morbidade, fatores de risco, além das condições demográficas da população.

Por isso, este capítulo se dedica a apresentar a função da informação, as noções de sigilo e segredo profissional aplicado à saúde, bem como as nuances do consentimento informacional, exigido pela LGPD. Tem-se ainda, considerações acerca da relação médico-paciente e a análise dos procedimentos de coleta de dados.

3.1 A dimensão informativa do direito à proteção à saúde no ordenamento jurídico brasileiro

Ter informação implica em ter conhecimento. A informação compreendida como a ciência de fatos, situações e acontecimentos, sejam estes de interesse geral ou particular, materializa o conhecimento.[101] A informação, sob o prisma jurídico se desmembra em duas vertentes, a saber, o direito de informar e de ser informado.

A Declaração Universal dos Direitos Humanos, em seu artigo 19 afirma que "todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras"[102]. No ordenamento jurídico brasileiro o acesso à informação e ao conhecimento se encontra consagrado

101 A este ponto se faz necessário esclarecer a diferença entre dado e informação. Dados são registros, fatos brutos coletados que não possuem qualquer significado, contexto ou nexo com a realidade. Um dado pode ser uma letra, um número, uma palavra, bem como conjuntos de números e vocábulos desorganizados, o qual não transmite nenhuma informação ou conhecimento. Já a informação seria dados estruturados, organizados, processados, contextualizados ou interpretados. SETZER, V. W. Dado, Informação, Conhecimento e Competência. **Data Grama Zero - Revista de Ciência da Informação**, v. 0, n. 0, 2015. Disponível em: https://www.ime.usp.br/~vwsetzer/dado-info.html. Acesso em 30 ago. 2022., p. 2.

102 ONU, op. cit., 1948.

como direito fundamental de primeira dimensão, elencado no artigo 5º, XIV da Constituição de 1988[103], constituindo o rol das chamadas liberdades públicas. É na realidade o reflexo do chamado "direito humano ao saber", resultante das liberdades públicas conquistadas no processo civilizatório.[104]

Matéria complexa que enseja diversos desdobramentos entre emissor e receptor, o direito à informação apresenta um aspecto passivo quanto ao dever de prestação negativa concernente ao Estado, que não pode impedir o livre acesso do indivíduo às informações de seu interesse[105]. De outro lado, tem-se o aspecto ativo com a garantia do direito de produzir e compartilhar informações, em consonância com o princípio da liberdade de expressão e da transparência.

Mas para além da visão de controle social, as informações consideradas relevantes sob o prisma da realidade social ganham o caráter de bem público, bem como aquelas que são pertinentes a um indivíduo de modo específico. Nesse sentido se posiciona o inciso XXXIII, do artigo 5º da Constituição Federal, ao dispor que todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral[106]. No entanto, na parte final da redação constitucional surge a ressalva quanto as informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

A interpretação mais prudente do inciso XXXIII indica que tais restrições se apliquem especificamente por razões de segurança e saúde pública, e quanto às informações pessoais, nos casos cuja confidencialidade assegura o exercício do direito

103 Constituição Federal de 1988, Artigo 5º: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XIV - e assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; BRASIL, op. cit., 1988.

104 SARLET, I. W.; MOLINARO, C. A. Direito à informação e direito de acesso à informação como direitos fundamentais na constituição brasileira. Revista da AGU, Brasília, ano XIII, n. 42, p. 9-38, out./dez. 2014. Disponível em: https://doi.org/10.25109/2525-328X.v.13.n.42.2014.542. Acesso em 30 ago. 2022, p. 12.

105 O acesso à informação deve ser compreendido como um direito fundamental segundo o qual o próprio Estado atua de forma fáticas e benéficas à coletividade, em seu sentido difuso, conforme direitos de natureza social, voltado à proteção de diversos grupos de pessoas que se exasperam pela necessidade de conhecimento para proteção pessoal, conforme a visão de que "enquanto direitos subjetivos, todos os direitos a prestações são relações triádicas entre um titular do direito fundamental, o Estado e uma ação estatal positiva." ALEXY, R. Teoria dos Direitos Fundamentais. 2. ed. Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros, 2017, p. 44.

106 Constituição Federal de 1988, Artigo 5º: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo- se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XXXIII - Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. BRASIL, op. cit., 1988.

de privacidade. Para aclarar a questão, recorre-se a Lei no 12.527/2011[107], denominada Lei de Acesso à Informação que regulamenta o amplo direito ao acesso à informação pública, determinando deveres estatais de gerir de forma eficiente a documentação governamental ou sob sua guarda, e viabilizar o conhecimento e a consulta a todos.

A Lei de Acesso à Informação, em seu artigo 4º, inciso I, considera informação como dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

A este ponto, é pertinente diferenciar a ideia do acesso físico da informação de seu acesso cognitivo. Enquanto acesso físico, considera-se aquilo que é palpável, geralmente por meio documental escrito, o que permite ao sujeito literalmente "receber em mãos". Já o acesso cognitivo ocorre a partir da aquisição cognitiva do conhecimento, trazendo ao sujeito a compreensão sobre algo que para ele é relevante, o que pode ocorrer de forma verbal ou visual.

A título de ilustração do acesso físico, é possível verificar na seara da saúde, a entrega de um prontuário, ter acesso ao termo de livre consentimento e laudos contendo informações detalhadas sobre sua saúde, permite ao paciente o acesso a informações físicas.

Só se pode chamar de "informação" algo que se compreende, isto é, se existe por parte do sujeito cognoscente, consenso em relação ao seu significado. Do contrário, não é informação.[108] Infere-se que o acesso à informação de qualidade se encontra diretamente relacionado com a dignidade da pessoa humana, tendo amplo papel na proteção e desenvolvimento da coletividade, contribuindo para a efetivação de outros direitos, inclusive o direito à saúde.

No Brasil, as informações de saúde abrangem dados administrativos, dados clínicos e epidemiológicos. Os primeiros se referem a Administração Pública e sua rede assistencial; já os dados clínicos, são aqueles diretamente obtidos do cidadão em procedimentos de assistência individual à saúde; por fim, os dados epidemiológicos são os relativos a populações, que consideram aspectos desde o comportamento até a evolução de problemas de saúde coletiva, com destaque para sua incidência, distribuição, e possível controle dos determinantes das próprias doenças e de seus fatores.

---

107 Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal. Idem.

108 VALENTIM, M. L. P. Informação e conhecimento em organizações complexas. *In:* VALENTIN, M. (org.). Gestão da informação e do conhecimento no âmbito da ciência da informação. São Paulo: Polis, 2008, p. 11.

Quanto ao direito de informação em matéria de saúde, coube a Lei nº 8.080/1990 regulamentar os deveres do Estado quanto ao direito à saúde e a organização e o funcionamento dos serviços públicos de saúde no Brasil.[109] O referido diploma elege como princípios o direito à informação, às pessoas assistidas, sobre sua saúde; a divulgação de informações quanto ao potencial dos serviços de saúde e a sua utilização pelo usuário, além destacar o dever do Estado de fundamentar suas políticas e ações em informações sanitárias e evidências científicas.

A demanda cada vez maior por assistência à saúde decorrente do crescimento populacional, gerou um aumento significativo na produção e armazenamento de dados de saúde, suscitando importantes questões sobre o direito à privacidade, dignidade da pessoa, discriminações, autonomia e informação. Sob a justificativa de que o acesso à informação em saúde possibilita, por meio de pesquisas e compartilhamento de experiências, uma melhor qualidade de vida e a redução de riscos de adoecimento para a coletividade, tem-se legitimado a coleta de dados pessoais sensíveis. Estes, por sua natureza, são aptos a revelar detalhes quanto ao modo de vida, hábitos, questões genéticas, entre outros aspectos da vida privada e intimidade do indivíduo.[110]

Mas a realidade é que o mapeamento das informações de saúde pode ser tão benéfico quanto perigoso para o cidadão. Em fato, certos aspectos da vida privada não devem ser considerados na forma como as pessoas serão vistas ou tratadas. E, no contexto de proteção de dados pessoais sensíveis de saúde, a natureza das informações não caberiam ao conhecimento público ou de terceiros, a menos que haja a anuência expressa do titular da informação.

Voltando ao potencial discriminatório e a possibilidade de interferências nos atos da vida comum, mediante o acesso a informações de saúde, surge a preocupação de que

109 Lei ordinária no 8.080, de 19 de setembro de 1990. Lei Orgânica da Saúde. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. BRASIL. Lei ordinária no 8.080, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Diário Oficial da União, Brasília: Presidência da República, 1990b. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 5 mar. 2023.

110 A classificação em dados pessoais gerais e sensíveis apesar de bastante difundida, não está livre de críticas. Não é tarefa das mais simples determinar se o dado pessoal possui ou não uma potencialidade discriminatória, lesiva a seu titular. Por exemplo, certo dado inicialmente não caracterizado como sensível pela legislação, a depender da situação e do tratamento a que é submetido, poderia resultar em tratamento discriminatório em relação ao seu titular. Tal hipótese pode ser verificada no caso do nome de pessoa transgênera. O nome originalmente registrado na certidão de nascimento e em outros documentos de identificação, poderia revelar aspecto da vida pessoal do titular da informação passível de tratamento discriminatório. LINS, R. G. S. O consentimento e o tratamento de informações pessoais de trabalhadores subordinados: uma análise sob a ótica da proteção cooperativa de dados pessoais. 2021. 173f. Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Norte, Natal, 2021, p.71.

seja designado um arcabouço legal e ético capaz de garantir segurança no tratamento e armazenamento destes dados, bem como a preservação da privacidade e da dignidade do usuário dos sistemas de saúde. Esta preocupação não é recente, mas adquiriu novas nuances com os processos tecnológicos aplicados ao setor.

Ainda na década de noventa, a Lei no 8080/90, conhecida como lei Orgânica da Saúde, tratava do assunto em seu artigo 47, ao determinar que o Ministério da Saúde, juntamente com os Estados e municípios deveriam organizar, no prazo de dois anos, um sistema nacional de informação em saúde integrado[111]. Contudo, o dispositivo não logrou êxito na prática.

O sistema nacional de informação em saúde integrado proposto deveria abastecer gestores, profissionais e mesmo a população quanto às informações de saúde, além de atuar como um meio de divulgação de informações de interesse da coletividade. Mas o que se verificou na realidade foi o surgimento de vários sistemas de informação[112] [113]segmentados e sem qualquer comunicação uns com os outros.

Entre os anos de 1991 e 1999 foram criados o Sistema de Informações Hospitalares - SIH-SUS, em 1991; o Sistema de Informação de Nascidos Vivos – SINASC, em 1992; o Sistema de Informações de Agravos de Notificações – SINAN, em 1993; o Sistema de Informações Ambulatoriais - SIA-SUS, substituto do SAMHPS e do SICAPS, em 1994; a Rede Interagencial de Informações para Saúde – RIPSA, em 1996; no ano de 1998, o Sistema de Informação de câncer de Útero e de Mama – SISCAN, o Sistema de Informação de Atenção Básica – SIAB, a Rede Nacional de informações de Saúde – RNIS; E por fim em 1999, o Sistema de informação do programa Nacional de Imunização - SI-PNI. Em que pese o exemplo dos anos 90, a fragmentação quanto as informações de saúde ainda configuram um desafio.

Com o estabelecimento do Sistema Único de Saúde (SUS), os Sistemas de Informação da Saúde - SIS passaram a contar com uma estrutura desenhada para assegurar a obtenção e a conversão de dados em informação e se encontram concentrados no

111 Lei no 8080/90, Artigo 47: O Ministério da Saúde, em articulação com os níveis estaduais e municipais do Sistema Único de Saúde (SUS), organizará, no prazo de dois anos, um sistema nacional de informações em saúde, integrado em todo o território nacional, abrangendo questões epidemiológicas e de prestação de serviços. BRASIL, op. cit., 1990.

112 No Brasil, onde os primeiros sistemas de informação em saúde (SIS) surgiram na década de 1970, com o objetivo de controlar o faturamento apresentado por prestadores de saúde credenciados ao Instituto Nacional de Previdência Social.

113 Um sistema de informação demanda três tipos de matérias-primas, a saber: dado, informação e conhecimento. O dado é o elemento mais simples desse processo; enquanto a informação é composta de dados com significados para quem os vê; o conjunto de nosso aprendizado segundo algumas convenções, nossas experiências acumuladas e a percepção cognitiva irão transformar em conhecimento uma dada realidade. SIQUEIRA, M. C. Gestão Estratégica da Informação. Rio de Janeiro: Brasport, 2005, p. 13.

Departamento de Informática do SUS, o DATASUS[114], que disponibiliza todos os Sistemas de Informação de Saúde em uso no território nacional.

Dentre as informações fornecidas encontram-se indicadores de Saúde; Assistência à Saúde, com dados sobre internação hospitalar, produção ambulatorial, imunização, saúde da família, vigilância alimentar e nutricional; informações de cunho epidemiológica e morbidade; informações acerca da rede assistencial por meio do Cadastro Nacional dos Estabelecimentos de Saúde - CNES; Estatísticas Vitais, com taxas de natalidade, mortalidade, câncer; informações demográficas e socioeconômicas; inquéritos e pesquisas; dados de saúde suplementar, entre outros.

Tão importante quanto o acesso à informação é definir como fazer uso delas. Já está claro que as informações de saúde são essenciais para o cidadão e para o Estado, visto que fornece base para o processo decisório, ao expressar a realidade de saúde, mortalidade e morbidade, fatores de risco, condições demográficas. Mas ainda se carece, na prática, do esclarecimento dos processos de coleta, armazenamento e tratamento desses dados, levantando a preocupação quanto as técnicas de informatização que estão sendo empregadas e suas possíveis fragilidades.

3.2 A tutela da personalidade na era digital: os dados de saúde como dados sensíveis e o problema da sua informatização

Os direitos da personalidade, adotados pelo Código Civil nos seus artigos 11 a 21, bem como pela Constituição Federal de 1988, em diversos direitos fundamentais, representam uma forma de proteção da pessoa humana, cabendo ressaltar que o rol dos artigos mencionados não é exaustivo, pois não há limites para as manifestações da personalidade humana que devem gozar de proteção legal.

114 No Brasil, o Departamento de Informática do SUS (DATASUS) desempenha um papel de importância vital na condução do processo de informação na saúde, sendo responsável por: Fomentar, regulamentar e avaliar as ações de informatização do SUS, direcionadas para a manutenção e o desenvolvimento do sistema de informações em saúde e dos sistemas internos de gestão do Ministério; Desenvolver, pesquisar e incorporar tecnologias de informática que possibilitem a implementação de sistemas e a disseminação de informações necessárias às ações de saúde, em consonância com as diretrizes da Política Nacional de Saúde; Manter o acervo das bases de dados necessárias ao sistema de informações em saúde e aos sistemas internos de gestão institucional; Assegurar aos gestores do SUS e órgãos congêneres o acesso aos serviços de informática e bases de dados, mantidos pelo Ministério; Definir programas de cooperação técnica com entidades de pesquisa e ensino para prospecção e transferência de tecnologia e metodologia de informática em saúde, sob a coordenação do Secretário-Executivo; Apoiar estados, municípios e o Distrito Federal na informatização das atividades do SUS. DATASUS. Histórico. Datasus – Departamento de Informática do SUS, 2011. Disponível em: https://datasus.saude.gov.br/sobre-o-datasus/. Acesso em: 11 jul. 2022.

São direitos que se encontram em expansão e que mediante a evolução legislativa e o desenvolvimento do conhecimento científico acerca do direito, acabam por se desdobrar a partir do surgimento de novas situações que exigem proteção jurídica e, consequentemente, reconhecimento. Portanto, o rol conhecido dos direitos da personalidade deve ser considerado como uma lista exemplificativa, apta a ser alterada em reflexo da veloz mutação social.[115]

Desta maneira, os direitos da personalidade, por hora, protegem bens jurídicos que integram a personalidade humana, bens estes que podem ser referentes a personalidade física (vida, imagem, etc.) e/ou a personalidade moral (intimidade, nome, reputação, etc.).

Em que pese a importância e coerência de um direito geral da personalidade, sedimentado como um direito subjetivo à abstenção de atos que violem bens jurídicos calcados na personalidade humana, e que, a partir da constatação da respectiva violação a um desses bens, possibilita a reparação de todos os danos causados, este tem sido alvo de algumas ponderações e críticas por parte da melhor doutrina jurídica.

As ponderações feitas no tocante ao direito geral da personalidade aduzem que o direito à personalidade como um direito subjetivo é insuficiente para abarcar proteção e tratamento para todos os casos em que for violada a dignidade da pessoa humana.

> [...] tampouco há que se falar apenas em 'direitos' (subjetivos) da personalidade, mesmos e atípicos, porque a personalidade humana não se realiza somente através de direitos subjetivos, mas sim através de uma complexidade de situações jurídicas subjetivas. [116]

Logo, a tutela da personalidade humana não é suficiente apenas por meio de direitos subjetivos, haja vista que a personalidade humana pode se exprimir também em termos de direitos potestativos, deveres, ônus, poderes, faculdades, estados.[117]

Os desafios da sociedade da informação atingem tanto a esfera privada quanto a pública, resultando na necessidade de um redimensionamento na cultura jurídica face a alteração de valores associados aos direitos da personalidade. A mudança veloz de paradigmas e costumes, fomentada pelas relações e processos do mundo digital, não permite um acompanhamento próximo por parte do ordenamento jurídico.

---

115 BORGES, R. C. B. Disponibilidade dos direitos de personalidade e autonomia privada. São Paulo: Saraiva, 2005, p. 25.

116 MORAES, M. C. B. Danos à Pessoa Humana: uma leitura civil - constitucional dos danos morais. Rio de janeiro: Renovar, 2009, p. 118.

117 Idem, p. 118.

Compreendidos como os "direitos da pessoa de defender o que lhe é próprio[118]", os direitos da personalidade, inferem proteção à vida, identidade, liberdade, imagem, privacidade e honra, bem como materializam a proteção da dignidade humana por meio da positivação dos direitos humanos. São eles um reflexo direto da construção social e, por isso, se movimentam buscando acompanhar as mudanças e inovações nas relações, a partir de uma interpretação extensiva proporcionada pela sua condição de direito fundamental.

Nos termos do artigo 11 do Código Civil de 2002, "com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". Porém, diante do recente fenômeno da personalidade aplicada ao mundo digital, questiona-se os limites e responsabilidades a partir do manuseio de elementos impalpáveis que agora configuram parte do indivíduo, especialmente na seara da saúde.

A recente inclusão da proteção de dados no rol de direitos fundamentais, pela já mencionada emenda constitucional n° 115, impôs ao Estado o dever de assegurar a ao setor, o mais alto nível de proteção, atribuindo à União a competência para organizar e fiscalizar a proteção e o tratamento de dados pessoais, além de legislar, privativamente, o instituto em questão[119]. Trata-se de um grande avanço no sentido da segurança jurídica quanto à aplicação da LGPD, proporcionando uma maior solidez à questão do tratamento de dados que se reflete nas mais diversas áreas, inclusive para a saúde e os fenômenos informacionais oriundos do grande volume de dados sensíveis e informações que transitam no cotidiano de suas instituições.[120]

A informatização, aqui compreendida como o uso da informática[121] e das tecnologias, revolucionou o cotidiano das práticas de saúde, permitindo o aumento da capacidade de registro, transmissão, armazenamento e processamento de dados e

118 DINIZ, M. H. **Curso de Direito Civil Brasileiro**: Teoria Geral do Direito Civil. V. 1, São Paulo: Saraiva, 2022, p. 121.

119 Constituição Federal de 1988, Artigo 21: Compete à União: inciso XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. Artigo 2: Compete privativamente à União legislar sobre: inciso XXX - proteção e tratamento de dados pessoais. Parágrafo único. Lei complementar poderá autorizar os Estados a legislar sobre questões específicas das matérias relacionadas neste artigo. BRASIL, op. cit., 1988.

120 CAVALCANTE, R. B.; PINHEIRO, M. M. K. Política nacional de informação e informática em saúde: avanços e limites atuais. Perspectivas em Gestão & Conhecimento, João Pessoa, v. 1, n. 2, p. 91- 104, jul./dez. 2011, p. 91. Disponível em:
https://cetic.br/media/docs/publicacoes/2/20211130124545/tic_saude_2021_livroeletronico.pdf. Acesso em: 12 ago. 2022.

121 A informática enquanto nicho da informação digital abrange processos de coleta, armazenamento, processamento, transferência e difusão de dados. O termo é oriundo da junção das palavras informação e automática.

difusão das informações que contribuem para uma maior qualidade e celeridade dos atendimentos aos usuários do sistema.

As tecnologias da informação foram rapidamente incorporadas às rotinas, se fazendo presentes na maioria dos de processos de saúde.[122] Médicos, enfermeiros, gestores e pacientes utilizam registros médicos eletrônicos, dispositivos de coleta de dados, como máquinas de sinais vitais, aplicativos para controle de pressão e glicose, além de plataformas de vídeos, e-mails e sistemas de portais online, para otimizar processos, elevando a qualidade dos serviços.

A informação de saúde é considerada ferramenta essencial para o planejamento e gestão dos serviços, desempenhando papel fundamental na tomada de decisões. Relatórios e indicadores de desempenho auxiliam na definição de prioridades, alocação e gerenciamento de recursos. Análises direcionadas, que asseguram decisões mais eficientes, com a redução de desperdícios em direção a melhoria das condições de vida e saúde da população.

Os processos digitais também inibem fraudes sendo possível monitorar tarefas/atividades desempenhadas por cada profissional, o que assegura não apenas qualidade, mas segurança no atendimento ao paciente. O agendamento e as consultas online e demais práticas da telemedicina[123], popularizadas durante a pandemia COVID-19, são outras vantagens que merecem registro.

Com a informatização, a coleta de dados em saúde ocorre de forma ampla tanto em estabelecimentos públicos, como em ambientes privados, gerando um fluxo constante de armazenamento e processamento de dados[124]. Muitas vezes de modo inconsciente,

---

122 A título de exemplo, alguns dados verificados na Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros de 2021: As teleconsultorias, que ocorriam em 15% dos estabelecimentos, em 2019, passaram para 26%, em 2021. O monitoramento remoto de pacientes passou a estar em 20% dos estabelecimentos de saúde, ante 5%, em 2019. Essa variação pode estar associada à necessidade de manter um número reduzido de pacientes nos estabelecimentos de saúde como forma de evitar contaminação por coronavírus, além de disponibilizar maior número de leitos dedicados a pacientes com sintomas graves ou que necessitem de cuidados intensivos devido à COVID-19. Os serviços de telediagnóstico também passaram a ser mais utilizados, registrando um aumento de oito pontos percentuais (de 12% em 2019 para 20%, em 2021). CETIC - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2021. São Paulo: Comitê Gestor da Internet no Brasil, 2021. Disponível em: https://cetic.br/media/docs/publicacoes/2/15303120191017-
tic_saude_2018_livro_eletronico.pdf. Acesso em: 29 abr. 2019, p. 80.

123 A telemedicina pode ser definida como um conjunto de práticas médicas realizada à distância, utilizando tecnologias para troca de informações como as plataformas online, que podem ser acessadas através de eletrônicos disponíveis de alcance total da população; de forma a ser um encontro virtual. REZENDE, E. J. C.; *et al*. Ética e telessaúde: reflexões para uma prática segura. Revista Panamericana de Salud Publica, São Paulo, v. 28, n. 1, p. 58-65, 2010, p.58. Disponível em: https://scielosp.org/pdf/rpsp/2010.v28n1/58-65/pt. Acesso em: 27 jul. 2022.

124 As inovações em TI no que se refere as organizações de saúde, sejam públicas ou privadas, perpassam por

o cidadão fornece seus dados sensíveis para os mais distintos captadores que vão desde a utilização do cartão do plano de saúde, até uma simples compra em farmácia[125].

Para além disso, também é preciso destacar a quantidade crescente de usuários que abastecem aplicativos destinados a controles e informações de saúde, como período fértil, perda de peso, rendimento físico em esportes ou academia; compra e consumo de comidas; redes sociais, entre outros, em um movimento perigoso para a privacidade.

Ocorre que ao se tratar dos avanços tecnológicos na área de saúde, é praxe destacar os inegáveis resultados positivos, omitindo, contudo, os riscos à privacidade e a dignidade da pessoa envolvidos nestes processos. É preciso se atentar ao fato de que os fatores, pesos e informações que alimentam os algoritmos são desconhecidos dentro de um sistema opaco e complexo aos usuários do sistema[126], dando margens a práticas invasivas tais como, a instauração de um ambiente de vigilância, catalogação, ranqueamento e classificação de dados sensíveis.

Os bancos de dados formados a partir das informações de saúde, utilizados de forma indevida, apresentam grande potencial lesivo, podendo culminar em situações de discriminação ou constrangimento que podem prejudicar seriamente o cidadão.[127] Diante deste cenário, é preciso questionar até que ponto os processos de informatização

---

um processo de decisão que envolve duas partes. Em primeiro lugar, deve se decidir comprar, adotar ou adquirir uma inovação e disponibilizá-la à organização. E posteriormente, são necessárias decisões de usuários locais, por exemplo, profissionais da área médica, sobre a forma de utilização destas inovações em sua rotina. FABER, S.; Van GEENHUIZEN, M.; REUVER, M. eHealth adoption factors in medical hospitals: A focus on the Netherlands. International Journal of Medical Informatics, [*S.l.*], v. 100, 2017, p. 80. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1386505617300096. Acesso em: 27 ago. 2022.

125 RODRIGUES, M.; *et al*. Diferenciais na adequação das informações de eventos vitais nos municípios de Pernambuco, 2006-2008. Revista Brasileira de Epidemiologia, São Paulo, v. 15, n. 2, 2012, p. 275. Disponível em: https://doi.org/10.1590/S1415-790X2012000200005. Acesso em: 22 jul. 2022.

126 PASQUALE, 2015, p.95.

127 A inserção de dados pessoais do cidadão em bancos de dados de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computadores. BRASIL. Superior Tribunal de Justiça (Quarta Turma). Recurso Especial nº 22.337-8/RS. Serviço de proteção ao crédito. Cancelamento do registro. Prazo (cinco anos). O registro de dados pessoais no SPC deve ser cancelado após cinco anos. Art. 43, do Código de Defesa do Consumidor (Lei 8.07890). Relator: Ministro Ruy Rosado de Aguiar. Brasília, 1995, p. 6119. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=199200114466&dt_pu. Acesso em: 12 jan. 2023.

dos dados de saúde asseguram um tratamento adequado, evitando que informações íntimas sejam transferidas, manipuladas e divulgadas sem o consentimento de seu titular.

Além dos riscos de violação à privacidade e a dignidade do usuário de sistemas de saúde, é preciso ainda, refletir quanto a possibilidade da aplicação das tecnologias de informação e comunicação em saúde se converterem em um fator de ampliação de desigualdades[128] para grupos com baixos níveis de educação e falta de acesso a essas tecnologias.

Sem acesso a meios eletrônicos ou sem a possibilidade de executar a leitura das informações disponibilizadas, parte da população ficaria à margem do sistema e longe do propósito original de se ofertar a tecnologia como um instrumento para melhoria de serviços de saúde e emancipação social.

Na busca de resposta a tais questões, o Estado iniciou um intenso movimento por seu setor de saúde, conforme se verifica pela leitura da figura abaixo:

128 O princípio da igualdade, "[...] veda a hierarquização dos indivíduos e as desequiparações infundadas, mas impõe a neutralização das injustiças históricas, econômicas e sociais, bem como o respeito à diferença" (BARROSO, L. R.; OSORIO, A. "Sabe com quem está falando?": Notas sobre o princípio da igualdade no Brasil contemporâneo. Revista Direito e Práxis, Rio de Janeiro, v. 7, n. 13, p. 204-232, 2016, p. 207. Disponível em: https://www.redalyc.org/pdf/3509/350944882008.pdf. Acesso em: 7 abr. 2022.). O direito à igualdade pode ser desrespeitado em diferentes vias. Ocorre tanto quando uma característica irrelevante é considerada para que seja oferecido um tratamento diferenciado a determinada pessoa, bem como quando um aspecto relevante é desconsiderado e, por consequência, é destinado um tratamento equiparado a pessoas em condições desiguais, naquilo que se refere a aspectos que deveriam ser considerados. Seria justamente na visão negatória da igualdade que se pode falar em uma garantia de não discriminação. CASTILHO, R. Justiça Social e Distributiva: desafios para concretizar direitos sociais. São Paulo: Saraiva, 2009, p. 97-98.

Figura 1 - Linha do Tempo da Informatização da Saúde no Brasil

LINHA DO TEMPO DA INFORMATIZAÇÃO DA SAÚDE NO BRASIL

DÉCADA DE 1970

- 1974 — Criação da DATAPREV (análise de sistemas, programação e execução de serviços de tratamento da informação e o processamento de dados por computação eletrônica e serviços correlatos)
- 1975 — Primeira reunião Nacional sobre Sistemas de Informação em Saúde
- 1975 — Sistema Nacional de Informações sobre mortalidade (SIM) – Primeiro sistema desenvolvido no âmbito do MS
- 1975 — Sistema de Vigilância Alimentar e Nutricional (SISVAN)

DÉCADA DE 1980

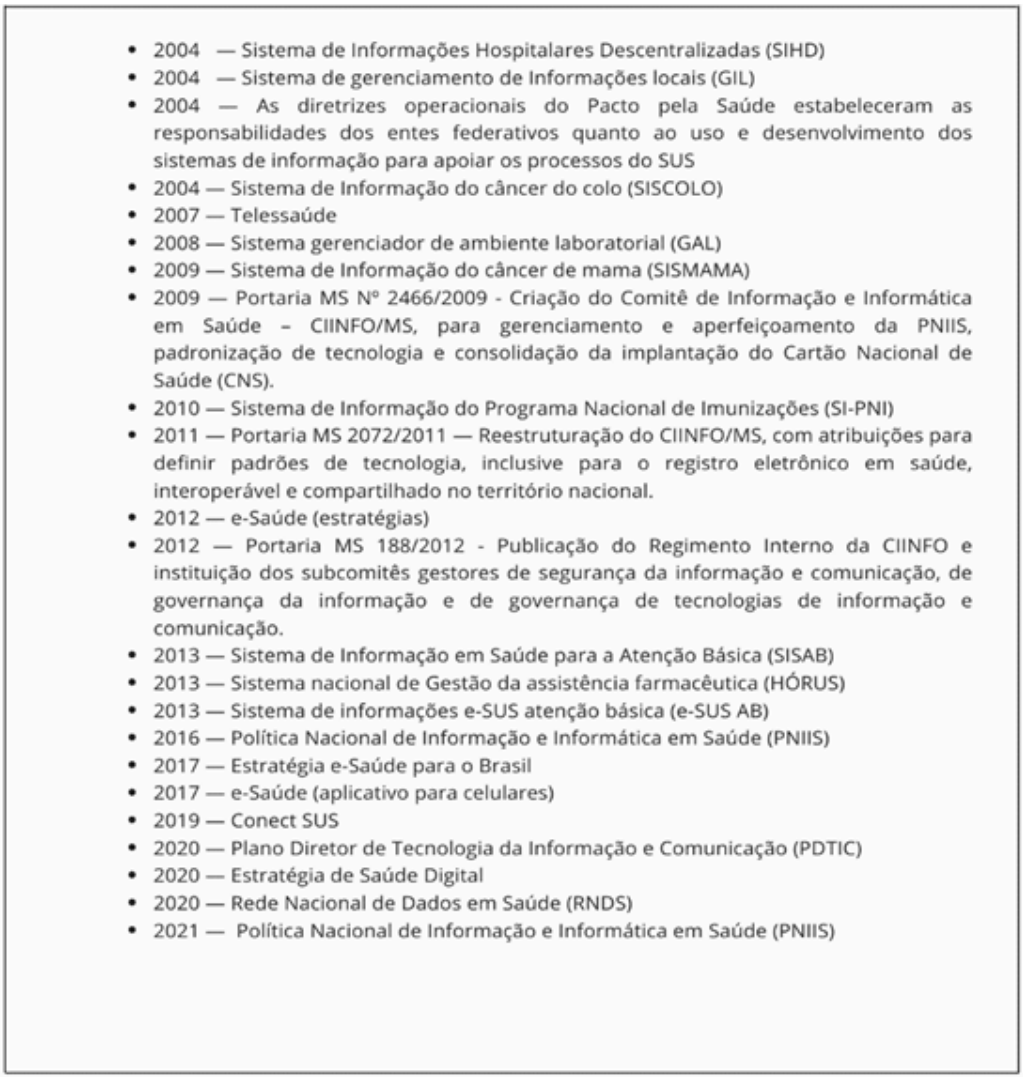
- 1980 — Sistema de Assistência Médico-Hospitalar da Previdência Social (SAMHPS)
- 1980 — Sistema de Informações e Controle Ambulatorial da Previdência Social (SICAPS)
- 1980 — Guia de Autorização de pagamento (GAP)
- 1984 — Sistema de Informações Hospitalares (SIH-SUS)

DÉCADA DE 1990

- 1990 — Sistema de Informação de Agravos de Notificação (SINAN)
- 1990 — Sistema de Informações sobre Nascidos Vivos (SINASC)
- 1991 — Lei 8080/90 Proposição do Sistema Nacional de Informações em Saúde
- 1991 — Decreto 100 de 16.04.1991 - Criação do Departamento de Informática do SUS (Datasus) e da FUNASA
- 1991 — Sistema de Informações Hospitalares (SIH-SUS)
- 1992 — Sistema de Informação de Nascidos Vivos (SINASC)
- 1993 — Sistema de Informações de agravos de Notificações (SINAN)
- 1994 — Sistema de Informações Ambulatoriais (SIA-SUS) – substituto do SAMHPS e do SICAPS
- 1996 — Rede Interagencial de Informações para Saúde (RIPSA)
- 1996 — Cartão Nacional de Saúde (CNS) – "Cartão SUS" (NOAS SUS Nº1/2001)
- 1998 — Sistema de Informação de câncer de Útero e de Mama (SISCAN)
- 1998 — Sistema de Informação de Atenção Básica (SIAB)
- 1998 — Rede Nacional de informações de Saúde (RNIS)
- 1999 — Sistema de informação do programa Nacional de Imunização (SI-PNI)

DÉCADA DE 2000

- 2001 — Sistema Nacional de Regulação (SISREG)
- 2002 — Sistema de Acompanhamento da Gestante (SISPRENATAL)
- 2004 — Politica Nacional de Informação e Informatica em saúde - PNIIS (2004) – GT coordenado pelo DATASUS e, com a participação do CONASS e CONASEMS, elaborou o documento base para a PNIIS



Fonte: Adaptado de EPSJV/ Fiocruz 2017.

A informatização na área da saúde se encontra em claro processo de evolução e expansão. Com a crescente popularização do uso das tecnologias de informação e comunicação na área e o surgimento de novas possibilidades associadas ao telecuidado, há uma ampliação constante dos bancos de dados de saúde. Em que pese o movimento do Estado quanto às regulações eficientes, ainda restam diversos pontos que carecem de maior elucidação quanto ao tratamento dos dados em saúde e desconfianças quanto a oferta de segurança dos sistemas, fortalecida por episódios de vazamento de dados nos últimos anos.

Assim, ao tempo em que se verificam os avanços na coleta e armazenamento de dados dos usuários do sistema de saúde, amplia-se em igual proporção a preocupação com riscos associados ao uso e divulgação indevida de dados pessoais. É importante lembrar, que nesta matéria específica existe uma expectativa de resguardo por parte do usuário, pautada no dever de sigilo inerente às práticas de saúde, que no contexto

atual, deve ser estendido de forma automática a todos aqueles que tiverem acesso ou contato com os dados coletados para fins de saúde.

3.3 Função da informação na área da saúde

Toda informação pressupõe ordenação e organização de dados a fim de transmitir significado e compreensão, conforme determinado contexto, se convergindo em uma base para gerar o conhecimento. Desta forma, para que os Sistemas de Informação em Saúde atuem como ferramentas aptas a auxiliar no desenvolvimento da gestão e dos serviços de saúde, é essencial que os dados coletados e trabalhados apresentem qualidade.[129]

A avaliação da qualidade dos dados disponibilizados na área da saúde, frequentemente se baseia em uma análise subjetiva, segundo a qual são indicados aqueles que se encontram aptos para uso. Todavia, na realidade, a qualidade de um dado reside na acessibilidade, relevância, confiabilidade e capacidade de interpretação pelo usuário. Ou seja, ao falar em qualidade, o que se espera não é necessariamente exatidão, mas que seja integro, relevante, oriundo de fonte confiável e atual.[130]

Importante recordar que o processo de coleta e tratamento de dados, bem como o direcionamento de informações perpassa a individualidade dos responsáveis por seu manuseio, refletindo o contexto político, econômico, social, cultural e institucional, que deve ser considerado no processo de produção e aplicação da informação. Os dados apresentam uma conotação mais "primitiva", configurando uma espécie de "pré-informação", enquanto a informação estaria relacionada a algo mais complexo, à representação contida no dado, chegando ao limiar da cognição.[131]

---

129 Qualidade definida como "fitness for use" (serventia para uso) possui a vantagem de ser simples e explícita num aspecto extremamente importante que consiste no fato da qualidade não existir por si só nas características intrínsecas dos "objetos", mas sim a partir da utilização ou aplicação desses objetos. Assim como a qualidade de um carro só pode ser sentida por quem o usa, a qualidade da informação só pode ser avaliada por quem a consome, e só terá qualidade se quem a consome a considerar como apropriada para as necessidades em causa. OLIVEIRA, J. N.; AMARAL, L. O papel da qualidade da informação nos sistemas de informação. *In*: CONFERÊNCIA ESPECIALIZADA EM SISTEMAS E TECNOLOGIAS DE INFORMAÇÃO, Lisboa, 1999. Anais [...] Sistemas e Tecnologias de Informação: Desafios para o Século XXI", Lisboa, 1999, p. 3. Disponível em: http://repositorium.sdum.uminho.pt/handle/1822/ 2183. Acesso em: 11 ago. 2022.

130 WANG, R. Y.; STRONG, D. M. Beyond accuracy: what data qaulity means to data consumers. Journal of management information systems, [*S.l.*], v. 12, n. 4, 1996, p. 5. Disponível em: http://mitiq.mit.edu/documents/publications/tdqmpub/14_beyond_accuracy.pdf. Acesso em: 15 jun. 2022.

131 DONEDA, op. cit., p. 94.

Dados de qualidade se convertem em informações relevantes para pacientes, profissionais, gestores e para o Poder Público e se tornam um caminho para a otimização de processos, redução de custos e melhoria de serviços. A qualidade dos dados também possibilita a análise de indicadores epidemiológicos estratégicos para o planejamento das ações e tomadas de decisão nos mais diversos setores de saúde.

A informação gerada, configura evidência das necessidades de saúde e se converte em vetor para a proposição de políticas públicas mais robustas, desenhadas conforme as características e necessidades de seus destinatários, contribuindo para a melhoria das condições de vida e saúde da população. Deste modo, pode-se afirmar que a gestão eficiente das informações com a aplicação de técnicas de análise de *Big Data* em saúde, pode gerar impactos verdadeiramente positivos para o setor, especialmente quanto ao aumento de produtividade, otimização do orçamento e ainda, por meio de contribuições em estudos clínicos.

A aplicação do termo *Big Data*[132] em matéria de saúde se justifica face ao grande volume de dados, estruturados ou não, gerados diariamente nas empresas e organizações públicas e privadas. Embora não haja uma definição uniforme, o *Big Data* se apresenta, em linhas gerais, como o agrupamento de grande volume de dados variados, produzidos em alta velocidade, que necessitam de recursos e tecnologias específicas para serem corretamente analisados, viabilizando a conversão dos dados em informações.

Através da aplicação de algoritmos e ferramentas especiais no *Big Data*[133], cientistas de dados, não apenas organizam, mas cruzam diversas fontes de informação, viabilizando que hospitais e outras instituições de saúde passem a criar com maior rapidez e assertividade soluções para otimizar seus processos. Em paralelo, os profissionais da

132 O *Big Data* geralmente é tratado sob a perspectiva dos três atributos: volume, variedade e velocidade. No entanto, há outra dimensão que complementa a relevância do fenômeno e a sua eficácia no processo de tomada de decisão: a veracidade. A importância da veracidade se dá "porque precisamos ter certeza que os dados fazem sentido e são autênticos", ou seja, as tomadas de decisões não devem ser embasadas em cima de dados duvidosos. A veracidade garantiria, então, a confiabilidade dos dados. TAURION, C. Big data. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2013, p.17.

133 Na seara da saúde o *big data* é o impacto da pesquisa, análise e tratamento de dados acaba por ser maior, uma vez que engloba aspectos relacionados a prevenção, diagnóstico e investigação clínica e medicamentosa de doenças. Por este motivo surge o crescente interesse por parte de inúmeras instituições em aderir cada vez mais às plataformas analíticas que permitam gerenciar custos operacionais, dados clínicos, exames, tratamentos e medicamentos. Importante destacar que a posse de um banco de dados não significa necessariamente que esses dados tenham utilidade. É preciso possuir inteligência e ferramentas para extrair informações significativas dos dados armazenados. SONDA, F. T. A sociedade em rede e a informação em saúde: um direito em construção no Brasil. Revista da Defensoria Pública do Estado do Rio Grande do Sul, Porto Alegre, n. 24, 2019, p.27. Disponível em: https://revista.defensoria.rs.def.br/defensoria/article/view/72. Acesso em: 30 ago. 2022.

área da saúde ganham novas possibilidades de análises e uma visão mais completa para tratamentos, prevenção e mesmo cura de doenças.

A gestão de dados, com a aplicação de algoritmos é etapa fundamental para que se chegue efetivamente às informações em saúde, pois "dados não tratados e analisados em tempo hábil são dados inúteis, pois não geram informação".[134]

Ante o exposto, tornam-se inegáveis os benefícios do uso de novas tecnologias para a coleta e tratamento de dados em saúde. Contudo, faz-se necessário observar os desdobramentos oriundos destes procedimentos de manuseio de dados sensíveis na vida prática de seu titular, considerando a relação de confiança estabelecida pelo paciente que busca amparo para cuidados de saúde *versus* a imposição de uma vigilância sob sua vida privada.

Os dados enquanto elementos de informação em saúde apresentam outras vertentes de impacto direto sobre o paciente titular. Primordialmente, as informações de saúde refletem o ato de dar ciência ao paciente sobre suas condições, seja saúde ou enfermidade, bem como seus aspectos de desdobramentos. Ao buscar atendimento de saúde, seja em um hospital, posto de saúde ou consultório privado, o paciente fornece informações sobre seu histórico clínico, resultados de exames, entre outras informações necessárias para a realização de procedimentos de finalidade diagnóstica ou terapêutica.

Tal entrega, vem resguardada pelos princípios da confidencialidade e do respeito à privacidade presentes no exercício das profissões de saúde.[135] Sob tais princípios que indicam o dever de reserva em relação aos dados de terceiro se constrói a base de confiança que norteia a relação profissional-paciente.

O profissional de saúde por meio de sua expertise atua como um mediador, que torna possível a apropriação da informação pelo paciente, fazendo que este consiga compreender o necessário para nortear suas ações e decisões quanto à sua saúde. A leitura de dados, obtidos por diagnósticos, prognósticos, bem como resultados dos exames e prescrições, demandam explicações técnicas que trarão conhecimento ao paciente, de modo a torná-lo um agente ativo em seu processo de tratamento.

---

134 TAURION, op. cit., p. 20.

135 O Juramento de Hipócrates, 460 a. C., em tradução afirma que, "*Prometo que ao exercer a arte de curar, mostrar-me-ei sempre fiel aos preceitos da honestidade, da caridade e da ciência, penetrando no interior dos lares, meus olhos serão cegos, minha língua calará os segredos que me forem revelados, o que terei como preceito de honra; nunca me servirei de minha profissão para comprometer os costumes ou favorecer o crime. Se eu cumprir este juramento com fidelidade, goze para sempre a minha vida e a minha arte de boa reputação entre os homens; se o infringir ou dele me afastar suceda-me o contrário".* FRANÇA, V. **Comentários ao Código de Ética Médica.** 7. ed. Rio de Janeiro: Grupo Gen, 2019, p. 34.

Desta forma, o profissional de saúde não apenas conta com largo acesso a dados sensíveis de seus pacientes e usuários do sistema de saúde, com os analisam e interpretam, afiançados pela confiança no cumprimento de seu dever de sigilo.

Enquanto milhões de dados são inseridos nos bancos de dados de saúde diariamente por todo o país, é preciso atenção especial a estas informações compostas por conteúdo sensível, em virtude dos potenciais danos causados a partir de uma divulgação indevida. Pelo ordenamento de dados é possível se atingir informações extremamente privadas do indivíduo, em uma prática perigosa, mas igualmente lucrativa para certas instituições. Seria possível, por exemplo se atribuir uma probabilidade de uma patologia, estado de saúde, gerando distúrbios e constrangimento para o titular dos dados.[136]

Importante destacar que a LGPD prevê de forma expressa em seu artigo 9º, o direito que assiste ao titular de dados pessoais de ter conhecimento sobre as empresas privadas ou públicas com as quais o controlador de dados pessoais compartilhou os dados.

Segundo o texto legal, em atenção ao princípio do livre acesso, o titular tem direito, de modo facilitado, às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca do uso compartilhado de dados pelo controlador e a finalidade. Esse direito é fortalecido ainda pelo artigo 18 do mesmo diploma que dispõe que o titular dos dados pessoais tem direito de obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

Por outro lado, a mesma LGPD afirma em seu artigo 30 que o compartilhamento de dados poderá ser regulamentado pela Autoridade Nacional de Proteção de

136 Como exemplo da questão "Caso Target": Situação na o pai de uma adolescente se sentiu constrangido pela prática de uma das lojas Target, uma empresa de varejo norte-americana, que estava oferecendo cupons de desconto em produtos de bebê para sua filha. A reviravolta se dá quando, depois de um tempo, o pai liga para o gerente da loja e pede desculpas pelo ocorrido porque havia descoberto que sua filha de fato estava grávida. Trata-se de um caso bastante conhecido, que continua sendo útil para introduzir a temática de proteção de dados. Um ano antes, a Target havia desenvolvido um modelo que era capaz de atribuir uma nota a consumidores relativas à probabilidade daquela consumidora estar grávida a partir de seu histórico de compras. Com esse modelo era possível inferir não só a probabilidade de gravidez, mas, com uma boa precisão, quando o bebê iria nascer. Isso permitia que a empresa enviasse cupons de desconto em estágios específicos da gravidez. Esse é um ótimo exemplo de como a partir do processamento de dados que à primeira vista parecem triviais é possível se chegar a informações sensíveis e relevantes sobre alguém através de inferências. MARTINS, P. B. L. Dados pessoais sensíveis e inferências. DTIBR, 2019, p. 4. Disponível em: https://www.dtibr.com/post/dados-pessoais-sens%C3%ADveis-einfer%C3%AAncias. Acesso em: 7 jun. 2022.

Dados[137], ensenjando margem para que surjam novas regulamentações para a questão do compartilhamento de dados.

Outro ponto fraco pode ser verificado na disposição do artigo 37, que atribui a responsabilidade quanto o registro das operações de tratamento de dados pessoais para seus agentes, no caso, o controlador e o operador[138], o que acaba por configurar um movimento arriscado, dada a possibilidade de adulteração, exclusão ou modificação de modo a se omitir transferências não autorizadas, entre outros casos.

Os usuários dos sistemas de saúde entregam dados a cada ação realizada e pela conversão destes dados em informações, acaba por entrar em um ambiente de exposição, no qual é amplamente visto, sem sequer perceber, abrindo margem para a vigilância praticada por instituições públicas ou privadas. Na realidade capitalista, os dados são insumos de alto valor, que se convertem em instrumentos de poder para empresas e governos, mundo a fora.

Sem garantias efetivas quanto a segurança nas práticas de coleta, tratamento e armazenamento, os dados de saúde se tornaram um dos alvos preferenciais dos cibercriminosos. Conforme pesquisa realizada pela empresa *Check Point Research Software Technologies* divulgados no início de 2022, os golpes virtuais na área da saúde aumentaram 64% (sessenta e quatro por cento), tornando o segmento como o segundo alvo preferencial apara ataques, ficando atrás apenas do varejo[139]. No Brasil, ao longo do ano de 2021 mais de 2,8 bilhões de dados sensíveis foram expostos, colocando o país pelo segundo ano seguido na primeira posição mundial, de acordo com o Relatório de Atividade Criminosa Online no Brasil.[140]

Assim, apesar dos inúmeros benefícios que justificam a coleta de dados e disseminação das informações de saúde no Brasil, é preciso prover meios de enfrentamento aos riscos suportados pelos usuários do sistema, claramente vulneráveis face aos prejuízos de uma exposição não consentida de sua intimidade. As questões associadas às informações em

137 LGPD, Artigo 30: A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais. BRASIL, op. cit., 2018.

138 LGPD, Artigo 37: O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. BRASIL, op. cit., 2018.

139 The 2022 Cyber Security Report gives a detailed overview of the cyber threat landscape and recommendations on how to prevent the next cyber pandemicgf. These gbetween January and December 2021, highlighting the key tactics cyber-criminals are using to attack businesses. CHECK POINT. **Cyber Security Report**. San Carlos: CPR Check Point Research, 2022. Disponível em: https://resources.checkpoint.com/cyber-security-resources/2022-cyber-security-report. Acesso em: 17 mar. 2023.

140 A empresa especializada em segurança Axur publicou em fevereiro de 2022, um documento denominado "Relatório de atividade criminosa Online no Brasil" — um estudo que traz os principais dados referentes a *phishing*, *malwares*, infrações em uso de marca e vazamento de dados em 2021.

saúde, passam pela necessidade de se trabalhar a ética no contexto da privacidade e da confidencialidade, a fim de que não se alimente uma sociedade em rede exposta e regida por interesses meramente capitalistas[141].

A esta altura, vale lembrar que a questão da proteção dos dados também encontra amparo na ética da informação. Ao se tratar da privacidade tem-se um direito legal, mas também um preceito ético extremamente relevante para a vida em sociedade. Na era da informação e das tecnologias, quando se permite que máquinas munidas de inteligência artificial, capazes de realizar processos decisórios sem os devidos cuidados e transparência quanto a formatação de algoritmos e ferramentas, se aceita igualmente a possibilidade de aplicar indícios e padrões discriminatórios e injustos.

Como construção própria do ser humano, a ética não é compreendida por máquinas. Seus temas e reflexos não são percebidos e trabalhados em sistemas eletrônicos, o que amplia a importância de um regulamento adequado para nortear basear programações, especialmente as que tratam de informações sensíveis do indivíduo. Deste modo, no que tange às informações de saúde percebe-se a necessidade não apenas de uma norma jurídica protetiva ao usuário de seus sistemas, mas também da manutenção de bases éticas e morais aplicadas como na Antiguidade, como modo de assegurar a dignidade da pessoa que busca amparo médico.

3.3.1 Do sigilo profissional na área de saúde e a (In)distinção entre sigilo e segredo médico

Entende-se por segredo tudo aquilo que não deve ser dito ou exposto, ou ainda o que não deve ser do conhecimento de outrem. O segredo deixa de existir quando a informação chega ao conhecimento, ou ao fácil acesso, de um número indeterminável de pessoas, tirando de seu titular o controle sobre quem detém ou não essa informação[142]. Já a expressão sigilo indica algo que deve ser protegido e que se encontra associado a um dever legal. O sigilo relaciona-se ao estabelecimento de relação técnica e formal, tendo em vista, geralmente uma relação profissional.

A expressão sigilo, em muitos casos, é substituída pela expressão segredo quando se aborda a privacidade do usuário em questões médicas, mas sempre no sentido da obrigação ética do profissional de saúde. Refere-se ainda à garantia assegurada ao

141 GALEFFI, D. A. Ética, privacidade e confidencialidade de informação em saúde. Informação em Pauta, Fortaleza, v. 5, n. especial, 2020, p. 10. Disponível em: http://hdl.handle.net/20.500.11959/brapci/136594. Acesso em: 16 mar. 2023.

142 ANDRADE, M. C. Direito Penal Médico, SIDA: testes arbitrários confidencialidade e segredo. Coimbra: Coimbra Editora, 2008, p. 1127.

paciente de que as informações por ele fornecidas, no momento do atendimento de saúde, sejam mantidas em segredo, independentemente do teor, da área de atuação do profissional e da condição do paciente, incluindo informações obtidas de menores de idade.

Trata-se de uma medida que permite ao usuário do sistema de saúde resguardar sua intimidade e vida privada, escolhendo o que deseja revelar ao mundo exterior, permitindo o exercício de sua liberdade e dignidade. A obrigação de sigilo não abrange apenas as confidências, mas também os fatos descobertos no exercício, ou por ocasião do exercício, das práticas médicas.

O sigilo deve ser considerado como um direito que assiste ao paciente, enquanto titular dos dados e um dever para todos aqueles que tiverem acesso aos dados pessoais do paciente em razão de sua atividade profissional, que inclusive dispensa a necessidade de solicitação por parte do interessado. Importante destacar que o dever de sigilo é extensivo a todos que tenham acesso a prontuários, banco de dados e exames, incluindo profissionais de T.I, arquivistas, auditores, entre outros.

Para além da ética, encontramos o dever de sigilo sob o prisma legal acostado em diversos diplomas. Do já mencionado artigo 12 Declaração Universal dos Direitos Humanos[143], ao Código Internacional de Ética Médica[144] o sigilo aparece como um dever de proteção para com o paciente.

No Brasil, o sigilo profissional está disposto primeiramente no texto constitucional que afirma em seu artigo 5º, inciso XIV, que é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional[145] e destacada no Código de Ética Médica - CEM, elaborado pelo Conselho Federal de Medicina - CFM, o qual disciplina integral e isoladamente o exercício da medicina, as relações entre médicos, entre médico e paciente e entre médico e instituição de saúde ou Estado.[146]

---

143 "Ninguém será sujeito a interferência em sua vida privada, sua família, seu lar ou sua correspondência, nem ataques à sua honra e reputação. Todo homem tem direito à proteção da lei contratais interferências ou ataques". ONU, op. cit., 12.

144 O Código Internacional de Ética Médica, adotado pela Associação Médica Mundial (WMA) em 1949, estabelece que: "*o médico deverá manter segredo absoluto sobre tudo o que sabe de um paciente, dada a confiança que nele depositou".* CONSELHO FEDERAL DE MEDICINA (CFM - Brasil). Código de ética médica. Resolução nº 1.246/88. Brasília: Tablóide, 1990.

145 Constituição Federal de 1988, Artigo 5º, inciso XIV.

146 Dentre os preceitos contidos no CEM (Resolução CFM 2.217/2018, modificada pelas Resoluções CFM 2.222/2018 e 2.226/2019), destaca-se a confidencialidade, um preceito moral e ético presente nas relações interpessoais e que está diretamente relacionado aos princípios de sigilo profissional, privacidade e liberdade. CÓDIGO DE ÉTICA MÉDICA. Resolução CFM nº 2.217, de 27 de setembro de 2018. Modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019 / Conselho Federal de Medicina. Brasília: Conselho Federal de

A matéria também encontra amparo e detalhamento em outros diplomas pátrios, a exemplo do Código Penal que considera crime a violação do segredo profissional, e atribui em seu artigo 154, pena de detenção, de três meses a um ano, ou multa para quem "revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem". A matéria também é abordada pelo Código de Processo Penal, que dispõe em seu artigo 207 quanto a proibição de depor as pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo.[147]

No mesmo sentido se percebe o posicionamento das normas civis. O Código Civil, em seu artigo 229, inciso I, afirma que "ninguém pode ser obrigado a depor sobre fato a cujo respeito, por estado ou profissão, deva guardar segredo", preceito reforçado pelo artigo 388, inciso II do Código de Processo Civil, segundo o qual a parte não é obrigada a depor de fatos a cujo respeito, por estado ou profissão, deva guardar sigilo[148].

O sigilo se faz presente nos mais diversos códigos deontológicos na área de saúde, agora fortalecidos pela Declaração Universal sobre Bioética e Direitos Humanos, que dispõem em seu artigo 9º que "a vida privada das pessoas em causa e a confidencialidade das informações que lhes dizem pessoalmente respeito deve ser respeitadas. Tanto quanto possível, tais informações não devem ser utilizadas ou difundidas para outros fins que não aqueles para que foram coligidos ou consentidos, e devem estar em conformidade com o direito internacional, e nomeadamente com o direito internacional relativo aos direitos humanos". [149]

Mais recentemente a necessidade de sigilo dos dados de saúde, também encontrou amparo na LGPD, que indica hipóteses que permitem o legítimo tratamento de dados sensíveis. Conforme o texto já visto do artigo 11, resta claro que o tratamento de dados sensíveis requer consentimento por parte do titular ou de seu responsável legal, sendo ainda admitido excepcionalmente, no caso de matéria de saúde, para "a tutela da

Medicina, 2019. 108 p.

147 Código de Processo Penal, Artigo 207: São proibidas de depor as pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho. BRASIL. Decreto-Lei n. 3.689, de 3 de outubro de 1941. Código do processo penal. Rio de Janeiro: Presidência da República, 1941, p. 55.

148 Código de Processo Civil, Artigo 388. A parte não é obrigada a depor sobre fatos: II - a cujo respeito, por estado ou profissão, deva guardar sigilo. Idem, p. 96.

149 Organização das Nações Unidas para a Educação, Ciência e Cultura. Declaração Universal sobre Bioética e Direitos Humanos. ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, CIÊNCIA E CULTURA, op. cit.

saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".[150]

A norma inclusive indica sanções nos casos de violação dos direitos dos titulares de dados que vão deste uma advertência, multa (diária ou com limite de até 2% do faturamento da empresa), bloqueio dos dados pessoais objeto da violação, até a suspensão parcial do funcionamento do banco de dados e proibição parcial, ou total do exercício da atividade relacionada ao tratamento de dados.[151]

Importante ressaltar que a LGPD apresenta exceções permitindo a aplicação ao tratamento de dados pessoais, quando realizados em benefício da coletividade. Neste sentido se posiciona o artigo 4º do diploma, ao afirmar que não se aplica por exemplo, para fins de segurança pública e atividades de investigação e repressão de infrações penais.[152]

Por esta breve análise, é possível afirmar que o sigilo, quanto às informações de saúde, é protegido tanto pelo ordenamento jurídico, quanto pelos conselhos de classe dos profissionais de saúde, só se admitindo o afastamento da regra em casos excepcionais, quando as informações apresentarem interesse coletivo, de ordem moral ou social, ou configurarem situação de risco para terceiros.[153]

---

150 LGPD, Artigo 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: f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Brasil, op. cit., 2018.

151 LGPD, ARTIGO 52: Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Idem.

152 LGPD, Artigo 4º: Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;b) acadêmicos; b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. Ibid.

153 Enfrentando a questão do sigilo na área de saúde, o STF já reconheceu a existência de constrangimento

Sobre o tema, o parecer do Conselho Federal de Medicina nº 5/2020 esclarece que o direito ao sigilo médico ou à intimidade privada podem sofrer certa mitigação, pois em determinadas situações previstas em Lei, em sentido estrito, admite-se eventual restrição mínima desses direitos fundamentais face a interesse de terceiro ou da coletividade[154]. Em exemplos práticos, o sigilo poderia ser quebrado, excepcionalmente, em casos como notificação compulsória de determinadas doenças transmissíveis; suspeita de abuso a idosos ou ao cônjuge; suspeita de abuso ou agressão infantil.

Com o cenário pandêmico vivenciado nos últimos anos, a discussão da mitigação do sigilo profissional ganhou novamente atenção do Poder Judiciário. Uma vez que a lei impõe o dever de o médico comunicar às autoridades competentes, os crimes de ação pública que independem de representação, e a constatação de moléstias infectocontagiosas, as informações quanto aos infectados pelo vírus COVID-19 se enquadrariam em casos de risco público, justificando a quebra do sigilo dos pacientes.

Este foi o argumento que norteou a decisão monocrática do Ministro Ribeiro Dantas, do STJ, no HC 584494 SP/2020[155] que deferiu requisição de relatório

---

ilegal na exibição de prontuário, inclusive limitando tal apresentação apenas a perito credenciado, justamente em virtude da existência do sigilo pericial (RE nº 91.218-5/SP). Em igual sentido, o STJ, no REC nº 159527/RJ, condenou unidade hospitalar em dano moral pela exibição de prontuário médico a operadora de plano de saúde sem o assente do titular. BRASIL. Superior Tribunal de Justiça. **Recurso Especial 159527 RJ**. Sigilo medico. Ética médica. Prontuário. Clinica. Seguradora. Viola a ética médica a entrega de prontuário de paciente internadoa companhia seguradora responsável pelo reembolso das despesas.recurso conhecido e provido. Recorrido: Clínica Médica Cirurgica Botafogo S/A Hospital Samaritano. Relator: Min. Ruy Rosado de Aguiar, 29 de junho de 1998. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/19853876/recurso-especial-resp-159527-rj-1997-0091690-1?ref=juris-tabs. Acesso em: 18 maio 2022.

154 O parecer do Conselho Federal de Medicina nº 5/2020: "Assim, o ordenamento jurídico vigente admite a possibilidade de os direitos fundamentais serem restringidos razoavelmente quando colidirem entre si. Essa colisão pode ocorrer de duas formas: (1) quando o exercício de um direito fundamental - por parte de seu titular - colide com o exercício do direito fundamental por parte de outro titular (colisão autêntica ou em sentido estrito); (2) quando o exercício de um direito fundamental colide com princípios e valores que tenham por fim a proteção de interesses da comunidade (colisão sentido amplo)."(...) Logo, não há dúvidas de que o direito ao sigilo médico ou à intimidade privada podem sofrer certa mitigação, pois em determinadas situações previstas em Lei (em sentido estrito) admite-se eventual restrição mínima desses direitos fundamentais. Entretanto, o que se sustenta é a impossibilidade da divulgação de resultados de exames, de forma a simplesmente garantir o direito à informação, se paciente (está ou não com a COVID19) sem motivo jurídico relevante, como uma investigação criminal, por exemplo". CONSELHO FEDERAL DE MEDICINA. Parecer CFM nº 5/2020. Informações médicas são sigilosas e privativas do paciente, sendo que sua divulgação somente ocorre com seu consentimento formal, exceto em cumprimento de determinação judicial, quando, nesse caso, o sigilo ficará sob a guarda do Juízo solicitante. Brasília: CFM, 2020, p. 14.

155 HABEAS CORPUS Nº 584494 - SP (2020/XXXXX-2) RELATOR: MINISTRO RIBEIRO DANTAS IMPETRANTE: DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO ADVOGADOS: DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO GUILHERME PAULO MARQUES - SP321424 IMPETRADO: TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO PACIENTE: FERNANDO HENRIQUE MODESTO COSTA RIBEIRO (PRESO) INTERES.: MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. DECISÃO: "...INDEFIRO o pedido formulado, de concessão de prisão albergue domiciliarem favor do sentenciado Fernando Henrique Modesto Costa Ribeiro, MTR: XXXXX-2, RGC:31.394.958, RJI: XXXXX-05, Penitenciária de Franca-SP. A decisão judicial deve ser mantida. "... de fato, consoante documento às fls. 142, e-STJ, o Diretor Técnico da Penitenciária de Franca justifica a negativa de fornecimento dos dados na

médico de paciente preso, como forma de comprovar requisitos para enquadramento como público de risco, considerando, além do potencial risco à saúde do paciente, a própria segurança dos demais encarcerados. Tal entendimento encontra amparo no Regulamento Sanitário Internacional, que em seu artigo 45, indica a possibilidade de sopesamento principiológico entre intimidade e dever de informação, independentemente de eventual autorização judicial.[156]

Não há dúvidas que o controle da propagação do vírus COVID-19 no ambiente prisional configurou substancial interesse coletivo, justificando a solicitação do médico. Assim, a crise de saúde pública provocada pela COVID-19, trouxe uma necessidade que se encaixou na excepcionalidade da justa causa, permitindo que o dever de informação viesse a sobrepor o dever de sigilo médico, demonstrando que face a colisão de preceitos fundamentais, o direito à vida e à saúde devem prevalecer sobre a intimidade e o sigilo profissional.

Além da justa causa e do dever legal, o sigilo imposto ao médico só poderá ser afastado por autorização do próprio paciente, afinal todo usuário que busca o sistema de saúde, seja público ou privado, parte da ideia da confiança quanto a confidencialidade de seus dados. Essa visão é essencial para a credibilidade e segurança do cidadão, de modo que toda e qualquer situação de quebra do sigilo deve ser avaliada de forma extremamente cautelosa, mediante justificativa que demonstre a real necessidade de divulgação da informação.

---

necessidade de autorização judicial para prestar tais informações, considerando os sigilos profissional e médico que envolvem a questão. Todavia, levantada a questão em sede de embargos de declaração, o Tribunal de Justiça do Estado de São Paulo indeferiu o pedido de expedição de ofício à penitenciária sob a justificativa de que [...] o writ deve estar suficientemente instruído com provas pré-constituídas suficientes à demonstração da ilegalidade ou abuso de poder supostamente praticado pelo d. Magistrado de Primeiro Grau. A ausência de documentos indispensáveis à comprovação das alegações contidas na petição inicial inviabiliza até mesmo o processamento do mandamus [...] (e-STJ, fls. 147-148). Assim, a ordem merece ser concedida, de sorte que a situação do paciente seja avaliada pelo Juízo de origem com base em prontuário médico a ser fornecido, juntamente com informações acerca das instalações hospitalares no estabelecimento prisional em questão. [...]"(e-STJ, fls. 258-263). Ante o exposto, não conheço do habeas corpus. No entanto, concedo a ordem de ofício a fim de determinar ao Juízo de Direito da Unidade Regional de Departamento Estadual de Execução Criminal - DEECRIM 6ª RAJ, da Comarca de Ribeirão Preto/SP que analise o pleito de concessão de prisão albergue domiciliar ao paciente com base em prontuário médico a ser fornecido, com urgência, juntamente com informações acerca das instalações hospitalares no estabelecimento prisional em questão. Julgo prejudicada a análise da petição de reconsideração RCD XXXXX/2020 (e-STJ, fls. 268-270). Publique-se. Intimem-se. Brasília, 18 de agosto de 2020. Ministro Ribeiro Dantas Relator (STJ - HC: XXXXX SP 2020/XXXXX-2, Relator: Ministro RIBEIRO DANTAS, Data de Publicação: DJ 20/08/2020).

156 Regulamento Sanitário Internacional aprovado pela Organização Mundial de Saúde, se encontra em vigor desde 2007, vinculando diversos países, inclusive o Brasil e teve seu texto revisado promulgado no país pelo Decreto nº 10.212/2020, fazendo menção à relativização da premissa de reserva judicial. BRASIL. Decreto n. 10.212, de 30 de janeiro de 2020. Promulga o texto revisado do Regulamento Sanitário Internacional, acordado na 58ª Assembleia Geral da Organização Mundial de Saúde, em 23 de maio de 2005. Brasília: Presidência da República, 2020.

Trata-se de um mecanismo protetivo, que como visto, desde os primórdios da medicina assegura ao paciente o exercício da liberdade e autonomia

na tomada de decisões quanto a sua saúde e que nos dias de hoje, com a expansão vertiginosa dos bancos de dados de saúde ganha novos contornos e renovada relevância em virtude de possíveis desdobramentos e danos à privacidade de seu titular.

3.3.2 Relação Médico-Paciente

Dentre os profissionais, que por meio de sua atuação profissional, tem contato direto com os dados de saúde, destaca-se a figura do médico. A relação médico-paciente é uma interação complexa, caracterizada pela entrega de confiança por parte de um indivíduo que se encontra em situação vulnerável a um *expert*. Existem diversas expectativas envolvidas nos processos de saúde que ultrapassam o desejo de cura, materializando-se igualmente na busca de uma melhor qualidade de vida, o que pressupõe bem-estar físico e mental.

O médico, desde a antiguidade, atua como referencial provendo ao paciente as informações e direcionamento necessários para seus tratamentos. Para o desempenho de tal função, no entanto, requer-se mais do que conhecimentos técnicos sobre enfermidades, sendo necessário o estabelecimento de um vínculo que permita ao profissional acessar informações de cunho pessoal do assistido, como seu histórico de doenças, contexto econômico e familiar.

Originalmente, se descrevia a atividade médica como pautada em um paternalismo que remonta aos tempos de Hipócrates, quando cabia ao paciente obedecer as ordens de seu médico sem questionamentos, em uma relação assimétrica, marcada pela fragilidade de um lado e pela força do conhecimento técnico do outro[157]. Assim, os médicos se movimentavam de forma unilateral apoiados na visão de que detinham conhecimento suficiente para indicar o que era melhor para seus pacientes[158].

Por óbvio, se reconhece que o médico é a pessoa mais habilitada para indicar as melhores opções de tratamento e de prevenção de doenças. Porém, é essencial que

157 Na relação hipocrática, analisar a questão da capacidade não tem significado, pois o médico assume o papel principal, determinando o tratamento, enquanto o paciente permanece submisso dentro da relação hierárquica. Porém, ao se estabelecer a autonomia do paciente, o profissional deve investigar sua vontade e trabalhar com informações compreensíveis, sem fazer prevalecer sua indicação, para que o paciente se manifeste livremente. AZEVEDO, A. V.; LIGIERA, W. R. **Direitos do paciente**. 1. ed. São Paulo: Saraiva: 2012, p.35.

158 BEIER, M.; IANNOTTI, G. C. Algumas considerações sobre o Paternalismo Hipocrático. Revista Médica de Minas Gerais, Belo Horizonte, v. 20, n. 2, 2010, , p.388. Disponível em: http://rmmg.org/artigo/detalhes/320. Acesso em: 1 abr. 2022.

na relação médico-paciente seja preservada, tanto quanto possível, a autonomia[159] do assistido, com a possibilidade de escolha do tratamento que será por ele suportado.

A noção de autonomia está relacionada à própria condição de humanidade e suas capacidades e aptidões. Porém, tendo em vista as especificidades das matérias de saúde, a capacidade de discernimento do paciente acaba por ser nublada pelo desconhecimento técnico, dependendo da mediação profissional do médico para uma tomada de decisão consciente. Por este motivo, todo o processo informativo ao paciente deve ser realizado por meio de uma comunicação clara e objetiva, sob a luz do princípio da beneficência.

Na visão da bioética, o princípio da beneficência [160]indica a obrigatoriedade de o profissional de saúde promover e zelar pelo bem do paciente. Fundamentado na ideia da confiança, o princípio em via prática demanda fazer o bem; não causar dano; cuidar da saúde; favorecer a qualidade de vida; e por fim, manter o sigilo médico. Tem-se aqui a demanda de que se observe os interesses relevantes e legítimos dos indivíduos e que se evitem danos.[161]

Toda relação médico-paciente se pauta na interação entre as duas partes, com a abertura de uma comunicação entre estas, sempre que se trata de pessoas racionais e dotadas de linguagem. Se não for este o caso, se recorrerá a uma figura intermediária, como um cuidador ou responsável legal, apto a estabelecer a relação comunicativa[162].

O dever de informação é parte integrante dos serviços médicos e pode ser compreendido como a exposição de forma clara e inteligível ao paciente, ou ao seu representante legal, acerca do diagnóstico, tratamento, técnicas a serem empregadas, bem como suas vantagens e desvantagens, possíveis riscos, custos, e demais esclarecimentos que se mostrem relevantes ao paciente. De outro lado, cabe ao paciente, com maior

159 A expressão autonomia associada a relação médico-paciente será compreendida como poder de decisão. Etimologicamente, o signo autonomia é uma palavra que vem do grego autos, que significa "próprio, si mesmo" e nomos, como sendo utilizada pela referência à de autogestão. Ou seja, configura-se como o direito de poder gerir sua própria vida, respeitando a capacidade de cada ser humano fazer suas próprias escolhas sem qualquer interferência. WANSSA, M. C. D. Autonomia versus beneficência. Revista Bioética, Brasília, v. 19, n. 1, p. 105-117, 2011. Disponível em:
https://revistabioetica.cfm.org.br/index.php/revista_bioetica/article/download/611/627. Acesso em: 6 maio 2022, p.109.

160 O princípio da beneficência é o mais antigo da ética médica e da bioética e remonta diretamente a Hipócrates. Para Beauchamps e Childress, esse princípio "refere-se à obrigação moral de agir em benefícios dos outros, promovendo seus interesses legítimos e importantes". BEAUCHAMP, T. L.; CHILDRESS, J. F. Princípios de Ética Biomédica. São Paulo: Loyola, 2002, p. 282.

161 SANTOS, L. N. Biodireito E Princípios Bioéticos Fundamentais. Revista Clóvis Moura de Humanidades, Teresina, v. 5, n. 1, 2019, p. 78. Disponível em: https://www.tjpi.jus.br/revistaejud/index.php/escolajudiciariapiaui/article/download/105/93/409. Acesso em: 22 jan. 2023.

162 CAMPOS, C. F. C.; FÍGARO, R. A Relação Médico-Paciente vista sob o Olhar da Comunicação e Trabalho. Revista Brasileira de Medicina de Família e Comunidade, Rio de Janeiro, v. 16, n. 43, p. 2352, 2021, p. 352. Disponível em: https://rbmfc.org.br/rbmfc/article/view/2352. Acesso em: 11 ago. 2022.

precisão possível, informar seu médico sobre seu histórico médico, sintomas e qualquer outra peculiaridade que puder influenciar no julgamento do profissional médico.

Logo, a comunicação pautada em informações recíprocas entre as partes configura ponto essencial para uma relação adequada e positiva entre o profissional médico e o paciente. Para atender aos preceitos constitucionais que pregam a inviolabilidade dos desígnios relativos ao próprio corpo, bem como o modelo, a regra deontológica indicada pelo conselho profissional se exige do médico informar adequadamente seu paciente e obter deste o devido consentimento para a coleta e tratamento de dados pessoais sensíveis.

Para uma decisão livre e consciente por parte do paciente é imprescindível o alicerce de informações completas, adequadas, imparciais, confiáveis e inteligíveis. Neste sentido, destaca-se a importância da atuação do médico enquanto mediador, provendo ao paciente o conhecimento necessário para embasar suas decisões e o colocando como coparticipe na autogestão do seu corpo e escolhas terapêuticas.

Deste modo, uma vez inclinado a determinado tratamento ou procedimento conforme suas experiências e critérios individuais, cabe ao médico defender seu ponto de vista na escolha das alternativas existentes, mas quando for o caso, acatar a recusa de sua indicação frente a vontade do paciente.[163]

O que se pretende é, especialmente, trazer ao assistido o conhecimento sobre seu estado de saúde, incluindo prognósticos e diagnósticos, bem como os tratamentos necessários à sua enfermidade. Para tanto, se faz necessária uma prática informativa coerente, que seja de fato acessível ao paciente, conforme suas condições culturais e intelectuais, preservando sua dignidade e interesses pessoais.

Nesta feita, o preâmbulo da Recomendação do Conselho Federal de Medicina nº 1/2016, afirma que o "consentimento livre" deve ser compreendido como um "ato de decisão, concordância e aprovação do paciente ou de seu representante, após a necessária informação e explicações, sob a responsabilidade do médico, a respeito dos procedimentos diagnósticos ou terapêuticos que lhe são indicados".[164]

---

163 SZTAJN, R. A responsabilidade civil do médico: visão bioética. Revista de direito mercantil, industrial, econômico e financeiro, São Paulo, v. 36, n. 108, 1997, p.12. Disponível em https://repositorio.usp.br/item/000986240. Acesso em 16 mai. 2022.

164 Em situações normais, somente após devidamente esclarecido o paciente poderá manifestar sua anuência, ou não, decidindo por si, de forma autônoma e livre de influência ou de qualquer intervenção de elementos de erro, simulação, coação, fraude, mentira, astúcia ou outra forma de restrição. As informações e os esclarecimentos dados pelo médico têm de ser substancialmente adequados, ou seja, em quantidade e qualidade suficientes para que o paciente possa tomar sua decisão, ciente do que ocorre e das consequências que dela possam decorrer. O paciente deve ter condições de confrontar as informações e os esclarecimentos recebidos com seus valores, projetos, crenças e experiências, para poder decidir e comunicar essa decisão, de maneira coerente e justificada.

Seguindo a tendência norte-americana, o Código de Defesa do Consumidor adota a natureza contratual para a relação médico-paciente, todavia, sse posicionamento encontra exceções que abrem margem para discussões nos campos doutrinário e jurisprudencial.

Sem a pretensão de analisar profundamente a matéria, pontua-se para fins deste estudo que na maioria dos casos, a relação médico-paciente apresenta os pressupostos da relação contratual, sendo tradada pelo prisma negocial. Porém, a prática médica verifica situações nas quais a prestação do serviço é exercida sem o atendimento de tais requisitos. Seria este o caso, por exemplo, do paciente atendido sem que tenha chance de externar sua vontade dada situação de inconsciência ou, ainda, o que se nega a ser tratado, como o suicida ou o religioso da Testemunha de Jeová[165]. Nestas situações, haveria uma natureza extracontratual.

Em que pese as controvérsias verificadas quanto a natureza contratual ou extracontratual, a questão médico-paciente demanda um olhar transdisciplinar que considere preceitos éticos e legislativos que assegurem que tanto a vontade do paciente seja resguardada, quanto a atuação do profissional da medicina. Com os avanços da telemedicina e as práticas de saúde digital, a atuação do médico ganha novas dinâmicas e abre espaço para uma série de desdobramentos da relação médico-paciente que ainda não encontram resposta direta dos códigos deontológicos ou tribunais, sendo necessária a análise do caso concreto para a aplicação das proteções devidas às partes.

Conselho Federal de Medicina. Recomendação CFM nº 1/2016. CONSELHO FEDERAL DE MEDICINA. Recomendação CFM nº 1/2016. Dispõe sobre o processo de obtenção de consentimento livre e esclarecido na assistência médica. Disponível: https://bit.ly/2Pokq4y. Acesso em 26 ago. 2022.

165 Em razão da dificuldade de se estabelecer critérios quanto à primazia do direito à vida ou à autodeterminação (estando esse vinculado à dignidade da pessoa humana), o Ministério Público Federal (MPF) apresentou a Arguição de Descumprimento de Preceito Fundamental 61839. A referida demanda, entre outros pontos, questiona o alcance da Resolução CFM 1.021/1980, solicitando a retirada do item 2 do Parecer Processual CFM 21/1980, adotado como anexo daquela Resolução, que prescreve: Se houver iminente perigo de vida, o médico praticará a transfusão de sangue, independentemente de consentimento do paciente ou de seus responsáveis. A fundamentação do MPF faz clara referência à autonomia da vontade, entendendo que, ao se preservar o poder decisório do paciente, mesmo em casos-limite, respeita-se a sua dignidade, que poderá prevalecer inclusive quando em conflito com o direito à vida. Sob o ponto de vista do paternalismo libertário, a recusa do tratamento, com fulcro no argumento de que este violaria a dignidade do paciente, também seria lícita, sendo o paciente responsável por tal decisão. O médico, por seu turno, poderia desaconselhar tal conduta apontando consequências físicas e técnicas, porém não teria o direito de impor tratamento ou procedimento não consentido. Conselho Federal de Medicina. Resolução nº 1.021, de 26 de setembro de 1980. Adota os fundamentos do parecer anexo como interpretação autêntica dos dispositivos deontológicos referentes a recusa em permitir a transfusão de sangue, em casos de iminente perigo de vida. CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 1.021/1980. O Conselho Federal de Medicina usando da atribuição que lhe confere a Lei nº 3.268, de 30 de setembro de 1957, regulamentada pelo Decreto nº 44.045, de 19 de julho de 1958. Publicada no Diário Oficial da União, de 22 de outubro de 1980, Seção I, Parte II. Brasília, 1980. Disponível em: https://bit.ly/36Dc5nP. Acesso em 23 ago. 2022.

A realidade é que a atividade médica tem se estendido além dos consultórios, ocupando banco de dados, aplicativos e até mesmo redes sociais, diversificando não apenas as formas de comunicação, mas também de procedimentos, o que gera preocupação quanto a possibilidade de uma exposição indevida dos dados do paciente.

No meio médico, inteligência artificial, realidade virtual e impressão 3D são algumas das recentes ferramentas tecnológicas que impactam o cotidiano, quebrando paradigmas e mudando decisões clínicas. As recentes tecnologias modificaram as práticas médicas, alterando além de procedimentos, medicações e tratamentos, a comunicação, e o acesso à informação em saúde.

Informações técnico-científicas em saúde podem ser disseminadas diretamente na rede mundial de computadores[166] ou resguardadas em bancos de dados protegidos por tecnologias de segurança digital, em um movimento que demanda ao profissional de saúde novas formas de relacionamento com seus pacientes. Trata-se de uma reconfiguração do dever de informação pelo profissional que impõe um novo formato de tomada de decisões clínicas.

Mediante o alto quantitativo e o acesso facilitado à informação, a internet acaba por auxiliar no processo de protagonismo do paciente, que abandona a posição de mero receptor e passa a agir diretamente nas decisões de saúde. No universo da comunicação digital, o dever de informação pelo profissional da saúde ganha nova finalidade,

166 A privacidade e a segurança parecem mais discutidas do que nunca e os dados se tornaram ouro – mas, infelizmente, também para os golpistas. Na área da saúde, cibercriminosos buscam brechas para se apossarem de dados de pacientes, clínicas e profissionais. Segundo dados da *Check Point Research* divulgados no início deste ano, golpes virtuais na saúde aumentaram 64%. O segmento é o segundo alvo preferencial dos cibercriminosos, ficando atrás apenas do varejo. Em uma visão macro, o Brasil lidera o ranking de vazamentos de dados no mundo. No ano passado, mais de 2,8 bilhões de dados sensíveis foram expostos, colocando o país pelo segundo ano seguido na primeira posição mundial, de acordo com o "Relatório de Atividade Criminosa Online no Brasil". Na área da saúde, dados pessoais do paciente, como número de telefone, e-mail e informações sensíveis como condição de saúde, estilo de vida, orientação sexual e ainda informações genéticas e biométricas são ativos valiosos para golpistas. Os hackers, além de monitorarem dados de hospitais e planos de saúde, estão atentos a aplicativos de *healthtechs* e plataformas de telemedicina. "Todas essas ferramentas contam com diversos links nas cadeias de acessos e podem proporcionar facilidade para hackers e brechas de segurança cibernética. Se ocorrido, os vazamentos de dados podem gerar prejuízos incalculáveis, pois se trata de uma gama de informações sensíveis que podem ser usadas para, por exemplo, acesso ao perfil de redes sociais, tentativas de empréstimos, envio de links fraudulentos e até acesso a contas bancárias", revela Luis Albinati, CEO e fundador da plataforma Vitalicia. Grandes vazamentos de dados de saúde já ocorreram recentemente no país, prejudicando milhares de pacientes. Exemplo disso foi o vazamento de dados do Ministério da Saúde, que deixou milhões de dados expostos. "Mesmo com a Lei Geral de Proteção de Dados (LGPD), empresas do setor de saúde no país não contam ainda com a devida segurança. O investimento na privacidade de informações focada na tecnologia é tido como desnecessário por muitas organizações. Com isso, cada vez mais empresas tendem a ser vítimas de ataques cibernéticos e alvo de penalizações", revela o executivo. Enquanto as incertezas sobre o tratamento de dados por parte de algumas empresas persistem, Albinati ressalta que algumas boas práticas podem ser adotadas para proteger informações e evitar golpes cibernéticos. No início do atendimento hospitalar, solicite acesso à visualização dos dados que foram coletados; MELLO, op. cit., 2022.

auxiliando também no filtro de conteúdos de saúde disponibilizados de forma ampla em sites e plataformas digitais.

Surge, a figura do paciente especialista, que no anseio de obter conhecimentos sobre seu quadro de saúde, acaba por acessar informações que nem sempre são seguras, competindo ao médico intervir. O esclarecimento do paciente, indicando a pertinência dos conteúdos, evitando que as informações incompletas, distorcidas ou equivocadas venham a comprometer o tratamento indicado[167], passa a fazer parte do cotidiano do profissional.

Outra questão que merece atenção é a mediação de aparelhos e plataformas nas comunicações entre profissionais e seus pares, e entre profissionais e pacientes. Uma pesquisa realizada entre médicos no ano de 2021, indicou que 82 (70,7%) dos 116 entrevistados fazem uso de mídias sociais e aplicativos de mensagem instantânea com finalidades profissionais, enquanto 34 (29,3%) negaram a utilização com essa finalidade. Dentre os médicos que afirmaram fazer uso de mídias sociais e aplicativos de mensagem instantânea com finalidades profissionais, o *WhatsApp* (68,1%) e e-mail (30,2%) foram as mídias e aplicativos mais utilizados.

A grande maioria dos entrevistados que afirmaram se utilizar desses recursos no exercício de sua profissão têm entre 31 e 40 anos (34,1%), são mulheres (63,4%) e se formaram há menos de cinco anos (35,4%).[168]

Os dados relatados indicam a predominância de uma visão segundo a qual os benefícios e a eficiência da comunicação mediada pelas tecnologias sobrepõem os riscos à privacidade e à confidencialidade das informações de saúde do paciente. Mas é válido recordar que qualquer divulgação de informações sobre saúde que não se encontre especificamente amparada por lei, demanda consentimento do titular ou de seu responsável.

A expectativa do paciente é receber de seu médico informações confiáveis para embasar suas decisões e condutas na busca de reparar sua saúde ou de melhorar suas condições de vida. Partindo de um pressuposto de confiança, o paciente dificilmente reflete sobre a possibilidade do vazamento de suas informações de saúde, permanecendo em muitos

167 MEIRELLES, A. T. Medicina e Direito: Informação e Compreensão como pressupostos fundamentais à interface harmônica. CVMed – Direito Médico Comentado, [*S.l.*], 2019, p. 65. Disponível em: http://cvmed.com.br/2019/09/16/medicina-e-direito-informacao-e-compreensao-como-pressupostos-fundamentais-a-interface-harmonica/. Acesso em: 08 mai 2022.

168 LETTIERI, G. K. *et al*. Sigilo médico na era digital: análise da relação médico-paciente. Revista Bioética, Brasília, v. 29, n. 4, p. 814-824, 2021. Disponível em: https://doi.org/10.1590/1983-80422021294515. Acesso em: 20 ago. 2022.

casos, alheio aos riscos por ele suportados. De outro lado, temos a responsabilidade do profissional médico que recebe e fornece informações, que nortearão as decisões do paciente, devendo este se resguardar tanto quanto possível.

Percebe-se no acesso à informação o meio direto para a concretização do direito à autodeterminação, assegurando a liberdade e autonomia do paciente nos processos decisórios acerca dos tratamentos e cuidados aos quais deverá se submeter. Através da informação prestada pelo médico ao paciente que se viabilizará, ainda o exercício do consentimento, instrumentalizado no documento escrito denominado termo de consentimento livre e esclarecido – TCLE,[169] que tem por finalidade demonstrar a manifestação do consentimento por parte do paciente.

No TCLE, o paciente deve encontrar todas as informações pertinentes ao seu caso clínico, com informações não apenas sobre diagnóstico, mas também sobre as alternativas terapêuticas, a fim de embasar sua tomada de decisão. Sob o prisma da assistência à saúde, o TCLE atua em duas frentes[170], sendo a primeira jurídica visto que seria o documento para eventual defesa profissional, e a segunda ética, por meio do processo contínuo de esclarecimento na relação médico e paciente, assegurando a autodeterminação do último.[171]

3.3.3 Consentimento Informacional

Por tratar de área essencial da vida humana, as relações de saúde devem se pautar em um ambiente de confiança, horizontalidade e respeito. Contudo, o cenário constantemente alterado por inovações biotecnológicas, pelas pressões de um mercado que visa o máximo lucro, bem como por aplicações imprudentes da tecnologia da informação e da comunicação, nem sempre se mostra propício para concretizar esse preceito.

As informações de saúde despertam interesses negociais, constituindo-se em alvos de constantes ataques cibernéticos que colocam em risco a privacidade e a dignidade de seus titulares. O vazamento de dados sensíveis de saúde pode gerar uma série de

169 Na literatura podem ser encontrados dois enfoques sobre o TCLE: o da assistência à saúde, que será empregado ao longo deste estudo e o das pesquisas envolvendo seres humanos.

170 O Código de Ética Médica – CEM, em seu artigo 22 indica a obrigatoriedade de o profissional de saúde obter o consentimento do paciente ou de familiar responsável após elucidá-lo acerca do procedimento a ser realizado, salvo em casos de risco iminente de morte. O mesmo documento em seu artigo 34 exige que o profissional informe o paciente acerca de seu diagnóstico, objetivos do tratamento, riscos e prognóstico, a não ser quando tal informação possa lhe causar dano, situação em que a comunicação é direcionada ao representante legal.

171 MINOSSI, J. G.; SILVA, A. L. Medicina defensiva: uma prática necessária? **Revista do Colégio Brasileiro de Cirurgiões**, Rio de Janeiro, v. 40, n. 6, p. 494-501, 2013. Disponível em: https://doi.org/10.1590/S0100-69912013000600013. Acesso em: 20 jul. 2023.p. 494.

conjecturas sobre a probabilidade do desenvolvimento de doenças, incapacidades e até sobre a expectativa de vida de um indivíduo, influenciando as percepções e ações de terceiros. Além disso, informações sobre enfermidades graves, infecciosas, psiquiátricas, bem como uso de medicamentos controlados possuem alto potencial discriminatório, que podem culminar em prejuízos pessoais, profissionais e sociais.

Dado o alto potencial lesivo de um vazamento de dados sensíveis de saúde, faz-se necessário buscar proteções aos gigantescos bancos de dados gerados diariamente. Neste sentido, destaca-se a importância do consentimento quanto a coleta e tratamento de dados. O usuário dos sistemas de saúde, enquanto titular[172], revela seus dados pessoais e consente na sua utilização por profissionais e organizações, em razão da busca por uma solução terapêutica ou melhoria de sua qualidade de vida.

Trata-se de uma concessão temporária ao acesso de dados pelo profissional ou instituição de saúde, a partir da configuração da necessidade de assistência, limitado pela obrigação de guarda e sigilo. Segundo inciso I do art. 7º da LGPD, o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.[173]

Para o ato de consentir é fundamental que sejam previamente esclarecidos em linguagem clara, precisa e apropriada ao nível cultural do paciente, a pertinência, a finalidade, a adequação e o tempo da coleta dos dados[174]. Requer-se ainda a indicação sobre como será procedido o armazenamento, tratamento e a transmissão dos dados obtidos, de modo a viabilizar escolhas conscientes, permitindo-se que o titular dos dados decida pela alteração, o uso, a cessão, e a disponibilidade, ou mesmo a recusa daquele que consente.

Conforme o princípio da finalidade do tratamento de dados, somente será legítima a declaração de vontade do paciente quando embasada por um objetivo específico para seu tratamento[175], sob pena de nulidade. Assim, declarações em formato genérico

172 Os dados de saúde são propriedade de seu titular, o paciente e, diferentemente do que se entendia no passado, a titularidade da informação de saúde não é do profissional ou da organização de saúde. MEIRELLES, op. cit., 2019, p. 72.

173 LGPD, Artigo 8º: O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. BRASIL, op. cit., 2018.

174 O tratamento de dados e especialmente a sua coleta "não pode ser tomada como uma "rede jogada ao mar para pescar qualquer peixe". Ao contrário, as razões de coleta, principalmente quando se tratarem de "dados sensíveis", devem ser objetivas e limitadas". MORAES, M. C. B. Apresentação. *In*: RODOTÁ, S. A vida na sociedade de vigilância: privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 9.

175 LGPD, Artigo 8º: § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. BRASIL, op. cit., 2018.

não serão consideradas válidas para fins de tratamento de dados pessoais sensíveis. Para a efetividade do ato de consentir deve existir uma relação direta entre este e uma finalidade específica.

O consentimento livre e informado é, em síntese, uma das principais garantias que norteiam a relação do paciente com os profissionais da saúde, atuando como elemento na proteção dos dois polos. Para a construção do processo de consentir é preciso afastar toda e qualquer forma de coação, o que implica na utilização de linguagem não diretiva, bem como na ausência de qualquer tipo de incentivo ou influência.

A este ponto é importante considerar o desequilíbrio na relação entre o titular de dados pessoais e o responsável pelo tratamento na análise da validade do consentimento. A manifestação livre do ato de consentir pressupõe que aquele que nega seu consentimento se encontra protegido de qualquer tipo de prejuízo, direto ou indireto, imposta por aquele que o requereu[176]. Novamente, tem-se o protagonismo do assistido, enquanto sujeito na condução e na construção de sua própria vida, a partir do acesso a condições, inclusive temporais e informacionais, para a tomada de decisão livre, esclarecida e autônoma em um cenário de responsabilidade.[177]

O consentimento outorgado pelo paciente, parte de seu convencimento de que lhe foram prestados os indispensáveis esclarecimentos sobre o procedimento, assim como riscos, benefícios e consequências. Por tanto, além de compreender a informação, o paciente tem de aceitá-la como verdadeira e não manipulada. Neste sentido, a relação com os dados pessoais requer transparência desde o momento da coleta, indicação de finalidade, forma e tempo de armazenamento, até as especificações quanto ao tratamento e à transmissão dos dados.

Em uma breve retomada histórica, pode-se afirmar que a base ética e jurídica para a proteção das informações de saúde em ambiente digital já se encontra firmada em instrumentos internacionais como o Código de Nuremberg; a Declaração Universal

176 Válida a leitura do artigo "The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment. The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR". EUROPA. The working party on the protection of individuals with regard to the processing of personal data. Article 29 Working Party. Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017. p. 5. Disponível em: https://ec.europa.eu/newsroom/article29/items/623051. Acesso em: 27 ago. 2021.

177 BRÜGGEMEIER, G. Protection of personality rights in the Law of delict/torts in Europe: mapping out paradigms. *In*: BRÜGGEMEIER, G.; CIACCHI, A. C.; O'CALLAGHAN, P. (ed.). Personality rights in european tort law. Cambridge: Cambridge University Press, 2010, p.20.

dos Direitos Humanos - DUDH; Convenção Europeia dos Direitos Humanos; Declarações de Helsinque, Carta dos Direitos Fundamentais da União Europeia e Tratado de Lisboa. Estes, entre outros diplomas vêm reconhecendo princípios como a dignidade, a liberdade e a autonomia do ser humano em conformidade com os valores estruturantes das sociedades, ora marcadas pelas tecnologias da informação.[178]

Entretanto, apenas com o RGPD a União Europeia passou a uniformizar o regime de tratamento de dados, reconhecendo a autonomia, a liberdade, dignidade, a privacidade e o livre desenvolvimento da personalidade como alicerces de qualquer sistema de proteção de dados pessoais, em particular no ambiente digital. Tal visão acabou por refletir diretamente no nível da proteção da privacidade dos titulares de dados, em diversos países, inclusive no Brasil.

Seguindo a linha do RGPD, a LGPD consagra o consentimento informado como alicerce da proteção da pessoa humana e, mais especificamente, da sua autodeterminação. Conforme a LGPD afirma em seu artigo 20, ao paciente deve ser assegurada a deliberação livre, direito de revisão e consequentemente a possibilidade de retirada da anuência do acesso a seus dados de saúde a qualquer tempo, evitando riscos de danos materiais e imateriais.[179] Além disso, o diploma brasileiro também trouxe o direito à portabilidade de dados, fortalecendo a ideia da autonomia de seu titular[180].

Ao colocar a transparência como elemento central, a LGPD exigiu que todos os procedimentos envolvendo dados pessoais sejam compatíveis com a finalidade da coleta e minimizados em uma política de uso racional, sobretudo em razão da sua perenidade. Com a vedação de uso de dados sensíveis para fins discriminatórios e a exigência de consentimento para a coleta e tratamento de dados, salvo as já mencionadas exceções, amplia-se a proteção contra a divulgação e o acesso indevido a informações privadas do cidadão em razão da estrutura aberta da internet.

178 SARLET, G. B. S.; CALDEIRA, C. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. Civilistica.com – Revista Eletrônica de Direito Civil, Rio de Janeiro, v. 8, n. 1, 29 abr. 2019, p. 23. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 22 jan. 2023.

179 LGPD, Artigo 20: O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Brasil, op. cit., 2018.

180 LGPD, Artigo 18, inciso V: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial. Idem.

Não restam dúvidas de que o consentimento informacional se converteu em uma das principais ferramentas de proteção para dados. Porém, com uma visão mais apurada, surge o questionamento quanto a "efetividade de um quadro normativo focado no poder de escolha dos indivíduos".[181] Observa-se que o consentimento, apontado ponto central para a abordagem regulatória da proteção de dados é subtraído em determinadas hipóteses concretas, consideradas igualmente válidas, exercendo uma posição de igualdade umas em relação às outras. É precisamente o que se constata na previsão do artigo 11, incisos I e II da LGPD, quando se apresenta a possibilidade do tratamento de dados sensíveis por meio do consentimento do titular, e em sequência se elencam hipóteses nas quais se independe da manifestação de autonomia. Neste caso, tem-se uma posição de igualdade entre estas hipóteses, e não verdadeiramente a prevalência do consentimento.[182]

Mediante a aceitação pelo legislador de situações de tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados, como ocorre por exemplo, quando for indispensável para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, além de outras hipóteses que se referem, em grande medida, a interesses públicos e a interesses do próprio titular de dados.

Surge um contraponto a visão da obrigatoriedade consentimento como via fundamental para a proteção de dados. Logo, é preciso cautela em relação ao "mito do consentimento".[183] Fala-se em mito, pois não diante os casos de supressão, não é viável atribuir ao consentimento o caráter de solução para todos os problemas relacionados às operações de tratamento de informações pessoais, como se a anuência estivesse sendo dada pelo titular em uma relação fática neutra, sem desigualdades.[184]

---

181 BIONI, B. Proteção de Dados Pessoais: o que você sabe sobre o assunto? GEN jurídico, 2018, p. 114. Disponível em: https://blog.grupogen.com.br/juridico/areas-de-interesse/civil/bruno-bioni/. Acesso em: 24 mar. 2023.

182 BIONI, B. R. Proteção de Dados Pessoais - a função e os limites do consentimento. São Paulo: Editora Forense, 2020, p. 115 e 116.

183 DONEDA, op. cit., p. 121.

184 Em um sistema de índole patrimonialista, por exemplo, o consentimento assumirá uma função predominantemente legitimadora, ao servir como instrumento para colocar os dados pessoais no mercado e proporcionar, no extremo, a chamada *commodification* dos dados pessoais – a sua transformação em uma *commodity*. Por outro lado, em um sistema que privilegie a visão da privacidade como uma liberdade negativa e que confie ao indivíduo a autodeterminação de sua esfera privada, o consentimento é o instrumento por excelência para o exercício desse poder. Além disso, existem sistemas nos quais é reduzido o alcance do consentimento, e a utilização de dados pessoais dependerá, em um maior número de ocasiões, de uma específica disposição legislativa ou de um instrumento designado em lei. O consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade. Sua utilização como instrumento paradigmático para a tutela dos dados pessoais deve ser observada a partir de seus efeitos na sua concreta aplicação ao caso dos dados pessoais e seus efeitos – o que já foi denominado como mito do consentimento. Idem, p. 292.

Para assegurar que o consentimento do titular de dados seja real e efetivo, e atinja seu propósito protetivo, é imperioso a observação dos princípios da finalidade específica e da transparência. A concordância consciente com a operação de tratamento de seus dados, depende diretamente da compreensão por parte do titular quanto a extensão da utilização de suas informações pessoais, o que demanda a indicação mais específica possível quanto a finalidade do tratamento.

É precisamente por meio da especificação das finalidades das operações de tratamento de dados que se possibilita garantir juridicamente graus adequados de proteção a cada categoria de dados pessoais, com a indicação de determinadas espécies, que por seu caráter sensível, demandam maior cuidado por parte dos controladores e operadores de dados pessoais.

O consentimento informacional, ainda que se apresente como um requisito absoluto representa ponto crucial para a proteção de dados, sendo reconhecido nas mais modernas legislações sobre o tema. A LGPD, a exemplo do RGPD, se posiciona na busca pela garantia de um consentimento real e efetivo, exigindo que este venha livre, informado, explícito, em um processo que se convencionou chamar de "adjetivização do consentimento".[185]

Logo, verifica-se a crescente tendência pela qualificação do consentimento. Quanto maior a sensibilidade dos dados trabalhados, maior devem ser as especificações, esclarecimentos e cuidados quanto aos mesmos. É precisamente o que se verifica quanto aos dados sensíveis de saúde, nos quais se faz essencial que o titular tenha conhecimento básico sobre o fluxo de suas próprias informações, evitando que em virtude de desconhecimento, venha a fornecer autorizações para o tratamento de seus dados que coloquem em risco a sua dignidade.

3.4 O ciclo de vida do tratamento dos dados pessoais em saúde

A produção e interpretação de dados em saúde representa um grande desafio no que se refere a qualidade, periodicidade e veracidade necessárias para melhor orientar

185 Em meio a esse processo evolutivo, o consentimento passou a ser adjetivado, como devendo ser livre, informado, inequívoco, explícito e/ou específico, tal como ocorreu no direito comunitário europeu. Essa distribuição de qualificadores acaba, portanto, por desenhar um movimento refratário em torno do papel de destaque do consentimento quase como sendo sinônimo de autodeterminação informacional. O progresso geracional normativo da proteção dos dados pessoais assinala, destarte, um percurso no qual o consentimento emerge, é questionado e se reafirma como sendo o seu vetor central. Com isso, o titular dos dados pessoais permanece sendo o seu ponto focal, o que é replicado até os dias de hoje. A construção e a própria interpretação das normas a respeito da proteção dos dados pessoais têm seguido esse norte regulatório. BIONI, op. cit., 2020, p. 112.

o processo de tomada de decisão em políticas da área, sendo urgente o avanço nas práticas de análises de dados complexos e desestruturados, ora denominadas como *data mining* ou mineração de dados.[186] A multiplicidade de sistemas de informação na área de saúde requer um cuidadoso movimento de integração, que tendo em vista a diversidade de suas fontes de informações, conteúdos e parâmetros, exige metodologias próprias para a leitura adequada dos gigantescos bandos de dados.

Originalmente, as técnicas de análise de dados foram criadas para extrair informação a partir de poucos dados, em geral estáticos, limpos, amostrados cientificamente e seguindo suposições claras, em oposição direta ao cenário atual do verificado tanto na saúde pública, como na esfera privada. Nesse sentido, a área de Informática em Saúde passa a buscar novos referenciais para lidar com este tipo de dados e extrair seu melhor uso.

Não restam dúvidas quanto ao imenso potencial da ciência de dados aplicada a Saúde, que permite a sistematização de diversas fontes de dados, em um caminho para inovação da vigilância epidemiológica.[187] Contudo, para atingir uma medicina de precisão e predição de cenários, além de meio para redução de custos, ampliação do acesso e melhoria dos serviços de saúde. Nasce uma nova configuração para a saúde, que atua por meio de um método misto, o qual busca na abordagem indutiva da ciência de dados a construção de novas hipóteses sem necessitar de apoio ou confirmações clínicas, *a priori*, e na abordagem dedutiva para a verificação destas hipóteses com o rigor científico necessário para a construção de políticas públicas.[188]

As tecnologias de ciência de dados[189] aplicadas à saúde possibilitam um significado prático para profissionais e usuários do sistema, convertendo dados em informações

186 As organizações não estão imunes à realidade de geração e interpretação de informações. Nesse contexto, a Mineração de Dados (Data Mining) surge como ferramenta indispensável para a aplicação de algoritmos na busca por conhecimento implícito e útil. Ela é considerada uma das etapas do processo de Descoberta de Conhecimento em Bases de Dados (KDD) ou até mesmo equivocadamente vista como sinônimo deste termo. GOLDSCHMIDT, R.; PASSOS, E.; BEZERRA, E. Data mining: conceitos, técnicas, algoritmos, orientações e aplicações. Rio de Janeiro: Elsevier, 2015.

187 A Vigilância Epidemiológica é definida pela Lei nº 8.080/90 como "um conjunto de ações que proporciona o conhecimento, a detecção ou prevenção de qualquer mudança nos fatores determinantes e condicionantes de saúde individual ou coletiva, com a finalidade de recomendar e adotar as medidas de prevenção e controle das doenças ou agravos". Seu objetivo principal é fornecer orientação técnica permanente para os profissionais de saúde, que têm a responsabilidade de decidir sobre a execução de ações de controle de doenças e agravos, tornando disponíveis, para esse fim, informações atualizadas sobre a ocorrência dessas doenças e agravos, bem como dos fatores que a condicionam, numa área geográfica ou população definida. BRASIL, op. cit., 1990.

188 SALDANHA, R. F. Da aquisição à visualização de dados: aplicações da ciência de dados em saúde. 2021. 167f. Tese (Doutorado em Informação e Comunicação em Saúde) - Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, Fundação Oswaldo Cruz, Rio de Janeiro, 2021, p. 71.

189 Embora esse estudo não tenha por objetivo o aprofundamento nas técnicas e algoritmos em mineração de dados, é válido citar que a ciência de dados trabalha a partir de três grandes modelos de processamento esta-

técnicas que nortearão processos e tomadas de decisão. Através de uma análise apurada de informações se alcança uma maior aproximação da realidade, o que permite aos gestores trabalhar diferentes possibilidades de políticas públicas, otimizar questões orçamentárias e processos, bem como apresentar informações relevantes para o público em geral.

Sempre válido lembrar que o setor da saúde ainda padece com problemas associados a gestão de recursos mal utilizados, gerados em muitos casos pela falta de informação que culmina em procedimentos e exames desnecessários, onerando tanto o sistema, quanto o próprio usuário.[190]

Contudo, na busca por informações adequadas aos objetivos de otimização na gestão de saúde, é preciso se atentar para o fato de que o nível crescente de complexidade dos dados sensíveis de saúde, bem como a delicada questão de sua proteção exige uma abordagem diferenciada, a ser enfrentada por equipes transdisciplinares altamente treinadas. A capacitação dos operadores da saúde também configura um grande desafio para os estabelecimentos, sejam públicos ou privados, na adequação às tecnologias e às exigências técnico-jurídicas demandadas a partir de sua utilização.

O tratamento adequado de dados pessoais requer, por parte do órgão e de sua equipe de profissionais o conhecimento sobre os dados pessoais que gerencia, bem como quais são os processos, projetos, serviços e ativos que perpassam o ciclo de vida do deste tratamento. A LGPD em seu artigo 5º, inciso X, considera como tratamento toda operação realizada com os dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração e apresenta todo um detalhamento a cerca destes procedimentos. Todavia, o tratamento de dados não é matéria privativa da LGPD no ordenamento jurídico brasileiro.

A gestão documental é hoje parte integrante essencial da gestão de informações. Na área da saúde, a gestão de documentos se materializa em um trabalho arquivístico iniciado nas instituições públicas, em meados século XX em virtude da necessidade de organização da grande massa documental acumulada.[191]

---

belecidos e reconhecidos: Knowledge Discovery in Databases - KDD, Sample, Explore, Modify, Model, Assess - SEMMA e o Cross-Industry Standard Process for Data Mining - CRISP-DM.

190 NEGRI, S. M. C. Á.; KORKMAZ, M. R. D. C. R. A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana. Revista de Direito, Governança e Novas Tecnologias, Goiânia, v. 5, n. 1, p. 63-85, 2019, p. 31. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 20 jun.2022.

191 CUNHA, F. J. A. P. Gestão de documentos, aprendizagem e inovação organizacional em hospitais. **Infor-**

O trabalho arquivístico tem por objetivo organizar e tratar documentos a fim de propiciar acesso e recuperação das informações pertinentes e importantes para as tomadas de decisões e, no ano de 1991, por meio da Lei de Arquivos, nº 8.159, passou a ser amparado pela legislação brasileira. Conforme o artigo 3º, da mencionada norma, a gestão de documentos pode ser compreendida como o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.

Tal visão segue perfeitamente atual e em conformidade com as práticas dos modernos sistemas digitais, não devendo ser subestimada. A expansão das tecnologias, embora crescente, ainda não atingiu por completo todos os ambientes e instituições de saúde, nas quais ainda se verifica a frequente presença de prontuários e outros documentos físicos. Além disso, as funcionalidades de organização da gestão documental podem auxiliar e melhorar a qualidade das informações junto aos sistemas informatizados.

Outro diploma a ser mencionado é a Lei de Acesso à Informação – LAI, nº 12.527/2011, a qual promove o direito de acesso às informações públicas, passando a auxiliar e incentivar o aprimoramento de programas voltados a gestão de dados. Em seu artigo 6º, encontram-se indicações sobre o princípio da transparência e proteção da informação, com ênfase na importância do sigilo e resguardo da informação pessoal.[192]

Logo, no que se refere a operações envolvendo dados pessoais, a LGPD deve ser considerada conjuntamente com os dois diplomas, em uma interpretação sistemática com o objetivo de assegurar tanto a qualidade das informações de saúde quanto o direito de privacidade dos usuários do sistema.

Os bancos de dados em saúde se estruturam visando à atribuição de valor ao dado coletado com a sua conversão em uma informação verídica e útil, o que permite a composição de um verdadeiro ativo imaterial. Este objetivo fica nítido quando se percebe a importância da utilização das bases de dados de saúde no controle de

---

mação Arquivística, Rio de Janeiro, v. 3, n. 2, 2014, p.13. Disponível em: http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/106. Acesso em: 21 jul. 2022.,

192 Lei de Acesso à Informação – LAI, nº 12.527/2011, Artigo 6º: Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação; II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. BRASIL. Lei ordinária no 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal. Diário Oficial da União 2011; 18 nov. Brasília: Presidência da República, 2011.

doenças, pesquisas científicas, bem como pela indústria farmacêutica, como forma de mapeamento de doenças e, consequente, e produção de medicamentos.

De outro lado, verifica-se o risco a privacidade suportado pelo usuário dos sistemas de saúde mediante práticas abusivas de criação e indexação de perfis, alimentados por históricos médicos e indicadores regionais, com foco de proteger interesses econômicos, como por exemplo, o caso da limitação a cobertura dos planos de saúde de alguns pacientes com propensão genética a certas enfermidades. Neste sentido, é necessário especial cuidado na prática de tratamento de dados pessoais aplicados a saúde, de modo a assegurar que os inúmeros benefícios das informações digitais não custem a dignidade do paciente.

Visando organizar e orientar a prática do tratamento de dados pessoais, divide-se as ações realizadas em etapas que compõem o chamado ciclo de vida do tratamento de dados pessoais. São cinco fases, com correspondência direta com as operações definidas pela LGPD, que se iniciam no momento da coleta do dado e encontram finalização com a eliminação ou descarte deste.

Conforme já mencionado, o ciclo de vida de tratamento de dados pessoais se inicia com a fase da coleta, ou seja, a partir da obtenção, recepção ou produção de dados pessoais, independente do meio utilizado para este procedimento. A coleta pode ser realizada tanto por documento em papel, documento eletrônico como por meio de sistemas de informação, aplicativos, entre outros.[193]

A fase de coleta indica o recebimento do dado pessoal pela instituição e, consequentemente, marca o início das responsabilidades com relação aos mesmos. Para minorar riscos e resguardar o usuário dos sistemas de saúde, deve-se observar os princípios da necessidade e da finalidade dos dados coletados conforme a finalidade pretendida. Neste sentido, o artigo 6º, inciso III da LGPD dispõe que se deve limitar o 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.[194]

193 Existem em uso no Brasil, duas naturezas de registro de informações de saúde que caracterizam o Prontuário do Paciente em suporte de papel (PP) e o Prontuário Eletrônico do Paciente (PEP). Nos dois casos encontra-se vantagens e desvantagens. Embora se verifique uma tendência a ampliação do uso do prontuário eletrônico, mas ainda não há uma substituição total do prontuário tradicional por algumas instituições da saúde, caracterizando uma resistência cultural devido a sua confecção e preenchimento ser considerado simples e acessível. MACEDO, S. R. S. **A gestão documental de prontuário do paciente em saúde pública municipal em Aracaju**: da situação real para a ideal e sua inovação. 2019. 138 f. Dissertação (Mestrado Profissional em Gestão da Informação e do Conhecimento) - Universidade Federal de Sergipe, São Cristóvão, SE, 2019, p.23.

194 LGPD, Artigo 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados

Após a coleta, inicia-se a fase de arquivamento ou armazenamento de dados pessoais. O armazenamento de dados nas instituições de saúde brasileiras é verificado tanto em mídias físicas, tais como formulários impressos e outros tipos de documentos em papel, a exemplo de mídias eletrônicas como arquivos em nuvem, banco de dados, conforme recursos e possibilidade de acesso das instituições envolvidas e partes interessadas.[195]

Em ambos os casos, as práticas de armazenamento de dados de saúde demandam preocupações com ferramentas, protocolos técnicos e administrativos que possam assegurar a segurança da informação armazenada. Visando a proteção contra incidentes de violação de segurança[196], o acesso e processamento de dados pessoais, especialmente na seara de saúde devem ser restritos a profissionais que realmente se encontrem inseridos em processos para os quais, seu tratamento seja essencial.[197]

Na etapa de processamento, mais uma vez surge a indicação de que a classificação, utilização, reprodução, avaliação ou controle da informação, extração e modificação de dados pessoais, observe sempre a necessidade real da instituição. Neste ponto, tem-se uma série de processos técnicos que resultaram em um filtro, assegurando a identificação de informações úteis. Somente por meio de um processamento adequado de dados, é possível o obter a confiabilidade, integridade, e disponibilidade, que caracterizam a informação de qualidade, apta para uso.

Em sequência, surge a fase de compartilhamento. Conforme seu artigo 5º, inciso XVI, a LGPD entende por uso compartilhado de dados, a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais. Ainda pode ser entre esses e entes privados,

---

ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; 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;

195 LGPD, Artigo 19, § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. BRASIL, op. cit., 2018.

196 LGPD, Artigo 6º, inciso VII: princípio da 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; Idem.

197 Segundo dados da empresa especializada em privacidade *SurfShark*, o Brasil ficou em 12º lugar entre os países que mais contabilizaram episódios de vazamento de dados no primeiro trimestre deste ano. Embora essa colocação desperte preocupação, é possível dizer que houve uma melhoria no desempenho dos sistemas de segurança – afinal, entre outubro e dezembro de 2021, o país estava em 5º no ranking. O levantamento mostrou que, no início de 2022, dados de 286 mil brasileiros ficaram expostos através de suas informações na internet. Os vazamentos revelaram endereços de e-mail, senhas, números telefônicos, documentos e outras informações sensíveis. SURFSHARK. Data breach statistics by country: first quarter of 2022. Q1'2022 data breach statistics by origin, TOP 20, 2022. Disponível em: https://surfshark.com/blog/data-breach-statistics-by-country. Acesso em: 28 ago. 2022.

reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Conforme a LGPD, em seu artigo 9º, assiste ao titular dos dados o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, inclusive quanto ao uso compartilhado de dados pelo controlador e a finalidade;

Desta forma, infere-se que dados pessoais poderão eventualmente ser compartilhados, de forma interna ou externa, desde que observados requisitos legais e cuidados específicos para a transferência destes, bem como a idoneidade de empresas ou instituições terceiras para as quais compartilham os seus dados. Importante lembrar que a partir do compartilhamento de dados pessoais, as partes envolvidas assumem a condição de responsáveis solidárias no caso da ocorrência de episódios de violação de segurança nas empresas para as quais compartilharam os seus dados.[198]

O término do tratamento de dados pessoais conforme o artigo 15 da LGPD, indica a eliminação dos dados, dando início à última fase do ciclo de tratamento dos dados pessoais. São hipóteses de término do tratamento de dados, a verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; o fim do período estabelecido para o tratamento; a comunicação por parte do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou quando houver a determinação da autoridade nacional.

Mas o diploma legal também prevê possibilidades excepcionais de conservação dos dados destinados ao cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, desde que anonimizados os dados.[199]

198 LGPD, Artigo 42: O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. BRASIL, op. cit., 2018.

199 LGPD, Artigo 16. Idem.

Uma vez finalizado, o tratamento de dados sem a verificação de qualquer das mencionadas excepcionalidades, chega ao fim o ciclo de vida do tratamento de dados por meio da etapa de eliminação, compreendida como exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

A eliminação de dados é um direito que consiste na paralisação total das operações de tratamento, e o consequente descarte dos dados pessoais ou do banco de dados, o que não permite a posterior retomada do tratamento. Por isso, necessita ser cuidadosamente avaliado e expressamente autorizado pelo titular, especialmente nos casos de saúde em que as informações podem ser pertinentes inclusive para gerações futuras.

A LGPD aponta ainda a eliminação dos dados pessoais também como uma forma de sanção administrativa nos termos de seu artigo 52, inciso VI, segundo o qual os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos a eliminação dos dados pessoais a que se refere a infração.

Por fim, o direito à eliminação de informações pessoais conecta-se ainda ao direito ao esquecimento[200] e, mais recentemente, com "*right to erasure*" ou direito de apagar dados expressão que ficou conhecida no caso Google *vs* Mario Costeja González, julgado pelo Tribunal Europeu, em 2014[201]. Explícito no texto do RGPD, o direito

200 O direito ao esquecimento, em fevereiro de 2021, foi pauta dos noticiários jurídicos bem como objeto de comentários de juristas em todo o Brasil. E não é para menos, o assunto é relevantíssimo: o STF decidiu, no RE 1.010.606/RJ1, por maioria de votos, que o direito ao esquecimento é incompatível com a Constituição Federal. O tema possui fundamento na Constituição Federal e é também tratado pelo Código Civil, além de possuir aspectos práticos importantes, o que explica toda a comoção com o mencionado julgamento. O direito ao esquecimento traz consigo inúmeros princípios e direitos essenciais ao indivíduo e à coletividade. Sob a névoa do tema, de uma forma bem simples, podemos dizer que de um lado temos: o direito à liberdade de expressão e comunicação, proibição de censura, direito de comunicação da imprensa. De outro lado, também com gigantesca importância, temos a garantia constitucional da dignidade da pessoa humana expressada principalmente no resguardo da inviolabilidade da personalidade, nos direitos à imagem, à honra, à vida privada e à intimidade. É um tema sensível que traz à tona direitos individuais e coletivos importantes, em ambos os lados. O STF decidiu que o direito ao esquecimento não pode ser utilizado de forma abstrata para proibir a veiculação de fatos verdadeiros, obtidos de forma lícita, após a passagem de um longo período de tempo. Essa é a regra geral. Todavia, caso alguém seja vítima de abusos poderá recorrer ao Poder Judiciário que fará a análise do caso concreto para compatibilizar o exercício do direito à liberdade de expressão e imprensa com outros direitos importantes, como a intimidade e a vida privada. ROSSI, A. T. Direito ao esquecimento e a decisão do STF no RE 1.010.606/RJ. Migalhas, [*S.l.*], 2021. Disponível em: https://www.migalhas.com.br/depeso/340982/direito-ao-esquecimento-e-a-decisao-do-stf-no-re-1-010-606-rj. Acesso em: 30 ago. 2022.

201 No ano de 1998, o jornal espanhol La Vanguardia veiculou notícias sobre um leilão público com a indicação da venda de um imóvel de propriedade do advogado Mario Costeja González, em razão de um débito contraído com a seguridade social da Espanha. Costeja, que evitou a venda com a quitação do débito de forma regular, foi surpreendido anos depois, ao pesquisar seu nome no provedor de busca Google e se ver vinculado a antiga e defasada notícia do La Vanguardia sobre o débito já extinto. Em busca de resolver a situação, solicitou a remoção das notícias pelo La Vanguardia em 2009, mas teve seu pedido negado. Assim, restou a Mario Costeja ingressar, em 2010, com um processo administrativo perante a Agência Espanhola de Proteção de Dados

ao esquecimento, definido como a possibilidade de desconsideração e abstração de fatos vexatórios ocorridos no passado, não encontra correspondência direta na LGPD brasileira, mas pode ser entendida como um desdobramento do direito à privacidade garantido a cada indivíduo.

Para uma melhor compreensão acerca da matéria, a figura a seguir sintetiza as fases do ciclo de vida do tratamento de dados pessoais:

Figura - Fases do Ciclo de Vida do Tratamento de Dados Pessoais



Fonte: Adaptado Guia De Boas Práticas Lei Geral De Proteção De Dados - LGPD

Quando se trata de instituições de saúde vinculadas à Administração Pública, é importante observar os preceitos da Lei nº 8.159/1991 e suas regulamentações, pois nestes casos, os dados pessoais coletados pelo poder público passam a constituir o que se denomina arquivo público e sua eliminação deverá obedecer aos procedimentos de gestão de documentos[202]. Deste modo, resta claro que as operações de tratamento de

(AEPD), que chegou ao Tribunal de Justiça da União Europeia em 2014. O julgado ficou conhecido como González vs Google Espanha e teve como principal efeito o advento de um "direito à desindexação" de dados de pesquisa, relacionado com o direito fundamental à privacidade. EUROPA. Tribunal de Justiça da União Europeia. **Processo C-131/12, de 13 de maio de 2014**. Disponível em: https://curia.europa.eu/juris/liste.jsf?language=pt&num=C-131/12. Acesso em: 30 maio 2022.

202 Lei nº 8.159/1991, Artigo 7º - Os arquivos públicos são os conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias. Art. 9º - A eliminação de documentos produzidos por instituições públicas e de caráter público será realizada mediante autorização da instituição arquivística pública, na sua específica esfera de competência. BRASIL. Lei n.8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, 9 jan. 1991. Disponível em: http://www.unesco.org/culture/natlaws/media/pdf/bresil/brazil_lei_8159_08_01_1991 _por_orof.pdf. Acesso em: 21jun. 2022.

dados pessoais se encontram interligadas com os procedimentos e operações da gestão de documentos nas diversas fases do ciclo de vida do documento, devendo sempre ser observados conjuntamente.

3.4.1 Impactos da utilização dos Bancos de Dados em Saúde

O vertiginoso crescimento da tecnologia de informação em saúde vem desempenhando um papel fundamental na otimização dos processos de saúde. Além de assegurar maior rapidez e eficácia de atendimentos e procedimentos técnicos em ambientes de cuidados de saúde, as ferramentas digitais apresentam capacidade de gerar e/ou sintetizar evidências de várias fontes; apoiar a decisão para incorporar protocolos baseados em evidências clínicas; garantir a compreensão entre os sistemas através de vocabulários clínicos; facilitar a comunicação médico-paciente através de plataformas ligadas a web; e ainda acelerar pesquisas científicas, bem como construção de bases para o aprendizado e melhoria institucional.[203]

Por tanto, o sistema de tecnologia da informação em saúde contribui diretamente para a melhoria da qualidade, da eficiência e da eficácia do atendimento em saúde, vez que permite o gerenciamento da informação necessária para que profissionais de saúde otimizem suas atividades.[204] Na prática, ganha-se com a facilitação das comunicações, integração de informações e a possibilidade de coordenar ações entre os membros da equipe profissional de atendimento, com maior precisão quanto ao apoio financeiro e administrativo que deverá ser empregado para cada caso.

Percebe-se que além de benefícios em serviços médicos, a aplicação de tecnologias da informação em saúde também proporciona meios para a redução dos custos nas operações[205], sinalizando uma solução para uma preocupação permanente do Estado.

No que se refere as tecnologias da informação aplicadas ao setor de saúde podemos identificar três grandes grupos. O primeiro é composto por sistemas isolados

---

203 GONÇALVES, M. J. Adoção da tecnologia da informação em saúde sob a perspectiva do custo efetividade. 2019. 91 f. Dissertação (Mestrado em Engenharia Mecânica) - Centro Universitário FEI, São Bernardo do Campo, 2019, p. 15. Disponível em: https://doi.org/10.31414/EM.2019.D.131097. Acesso em: 10 mar. 2022.

204 As inovações em TI nas organizações, incluindo hospitais, constituem um processo de decisão que envolve duas partes. Em primeiro lugar, uma decisão de adoção formal para comprar, adotar ou adquirir uma inovação e disponibilizá-la à organização. Seguido por decisões de usuários locais (por exemplo, profissionais da área médica) sobre se realmente usarão a inovação e como. Este tipo de tecnologia traz muitos desafios e, portanto, compreender a sua adoção torna-se um fator importante para alavancar o potencial de resultados na gestão da saúde. FABER; Van GEENHUIZEN; REUVER, op. cit., p. 77.

205 ACETO, G.; PERSICO, V.; PESCAPÉ, A. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. Journal of Network and Computer Applications, [*S.l.*], v. 107, p. 125-154, 2018, p. 21. Disponível em: https://doi.org/10.1016/j.jnca.2018.02.008. Acesso em: 18 fev. 2023.

direcionados a uma finalidade específica de aplicação. Geralmente, os sistemas incluídos nesse grupo são direcionados a laboratórios, controle financeiro, radiologia, eletrocardiografia, controle de funções pulmonares, sistema de farmácia e nutrição. Na área da saúde pública, os sistemas de imunização também podem ser considerados exemplos dessa categoria.[206]

O segundo grupo é composto de sistema de informação hospitalar, materializado em uma rede de comunicação, um componente clínico e um componente administrativo e financeiro. O componente geral de comunicação integra essas três grandes partes em um sistema de informação coeso, que possibilita ter terminais de computadores em cada posto de enfermagem, assim como terminais que estão ou podem ser acessados em cada área do hospital. Em geral, são direcionados para a prestação de cuidado intensivo e organizados de acordo com as funções de cada departamento.[207]

Já o terceiro grupo contém os sistemas corporativos de informação em saúde. Tais sistemas capturam e armazenam informações mais completas, provenientes da assistência à saúde contínua realizada por diferentes organizações, usando um modelo integrado de prestação de serviços. Esses registros são capturados e depositados em diversos tipos de mídia, incluindo som, imagem, animação e impressão.[208]

Interessante destacar que os mencionados registros podem ser armazenados de modo central, em um formato total e abstrato, por meio de sistemas que realizam tratamento de dados, mas também poderiam ser armazenados através de registros, que podem ser físicos no ponto de captura. O registro físico seria posteriormente ligado a um registro digital, que será unido em caso de solicitação para atender à demanda dos cuidados, gerando a possibilidade de compartilhamento de informações entre os profissionais que se encontram vinculados ao caso.

Por meio das tecnologias, torna-se possível o acesso rápido e o compartilhamento de documentos, como o histórico médico e exames de um paciente independente de estar ele ou não, em ambiente hospitalar. O uso compartilhado de dados embasado no artigo 5º, inciso XVI da LGPD, consentido pelo seu titular[209], permite a eliminação

206 No inglês *stand-alone*. São sistemas limitados quanto ao objetivo e ao escopo. Como exemplo, são aqueles dedicados para calcular a carga horária dos enfermeiros que vários 15 hospitais possuem. HANNAH, J. K.; BALL, M. J.; EDWARDS, M. J. A. Introdução a Informática em Enfermagem. 3. ed. Porto Alegre: Editora Artmed, 2009, p. 10.

207 Idem, p. 11.

208 Ibid, p. 11.

209 LGPD, Artigo 7º § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. BRASIL, op. cit., 2018.

da coleta de dados, exames e procedimentos em duplicidade, resultando em uma importante economia de tempo e de recursos.

Outra vantagem a ser considerada a partir do emprego das tecnologias da informação em saúde é o processamento contínuo e atualizado de dados, que com organização sistemática pode ser integrado a outros sistemas de informação, gerando a facilitação na consulta de dados. Cria-se assim uma integração entre setores administrativos e assistenciais com registros legíveis e rastreáveis, aptos a facilitar ainda pesquisas científicas.

Em seu artigo 13, a LGPD disponibiliza o acesso a bases de dados pessoais para fins de estudos em saúde pública, a órgãos de pesquisa, com a orientação de que observem sempre que possível, a anonimização ou pseuanonimização dos dados, bem como padrões éticos relacionados a estudos e pesquisas[210]. Para fins de estudos na área de saúde pública, a norma equipara a posição de pesquisadores à de profissionais que têm o dever de conferir sigilo às informações recebidas no exercício de sua atividade profissional, a exemplo do que já se detalhou no caso dos médicos.

Para fins administrativos, a digitalização de dados trouxe importantes mecanismos para a melhoria do planejamento e controle hospitalar, o que tem permitido economia de tempo e de recursos humanos, além de direcionar o processo de tomada de decisões. Por meio dos bancos de dados digitais de saúde foi possível eliminar a necessidade de espaço físico para armazenamento de documentos, facilitar a produção de relatórios técnicos, controle de estoque e direcionamento adequado de recursos.[211]

Já para os profissionais de saúde as tecnologias foram responsáveis por uma facilitação da execução da rotina de atendimento e uma maior efetividade do cuidado.

---

210 LGPD, Artigo 13: Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências. § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Idem.

211 Um estudo realizado pela *International Data Corporation*, aponta que até final do ano de 2022, serão investidos US 1,931 milhões — o equivalente a R 10 bilhões — no setor de saúde apenas na América Latina, reforçando a evolução tecnológica que é realidade no segmento e deve ganhar ainda mais força nos próximos tempos. BRASIL. **Mercado Brasileiro de Software**: panorama e tendências, 2020. 1.. ed. São Paulo: ABES - Associação Brasileira das Empresas de Software, 2020.

Com os recursos digitais e acesso a informações sistematizadas, tornou-se possível prevenir erros de diagnóstico na prescrição e interação de medicamentos e reduzir o tempo de atendimento, por meio da otimização de processos burocráticos como registro do prontuário do paciente ou controle de custos de procedimentos médicos, agora digitais. Além disso, a popularização da telemedicina [212] apresenta a enorme vantagem do acesso à saúde sem barreiras geográficas.

A figura abaixo ilustra as principais aplicações das tecnologias da Informação no setor de saúde e revela o papel central do prontuário eletrônico [213]na difusão dos dados de saúde para os demais setores competentes.

212 Em abril de 2020, foi sancionada a Lei 13.989 que autorizou a prática de telemedicina no país durante a crise sanitária da pandemia de COVID-19. Na ocasião. a legislação respondeu a uma demanda por atendimentos a distância no contexto da pandemia, visto que as próprias autoridades de saúde orientaram reduzir o contato físico de pacientes com médicos e outros profissionais de saúde, como forma de minorar os riscos de contágio. Até então, não se permitia a realização de atendimentos médicos à distância, como teleconsultas. Importante destacar, que a lei apresentou originalmente um caráter de excepcionalidade e só autorizou a realização de consultas e atendimentos a distância no contexto da pandemia. Porém, uma complementação aprovada posteriormente permitiu que após o fim da emergência sanitária essas práticas sejam regulamentadas pelo Conselho Federal de Medicina (CFM). Tal regulamentação foi materializada por meio da Resolução nº 2.314/202 do CFM, que define e regulamenta a telemedicina no Brasil, como forma de serviços médicos mediados por tecnologias e de comunicação. CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 2.314, de 20 de abril de 2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. 2022. Disponível: https://www.in.gov.br/en/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852. Acesso em 23 ago. 2022.

213 O prontuário eletrônico deve ser compreendido como um repositório de informações mantidas de forma digital, ao longo da vida de um indivíduo. Trata-se de um arquivo no qual se armazenam as informações de saúde, clínicas e administrativas do paciente, voltado para a produção de dados, de forma padronizada e com informações que agregam conhecimento e são fontes de pesquisa para a saúde. A forma eletrônica do prontuário do paciente promete agilidade ao processo de gravação, assim como rapidez e precisão no processo de recuperação e uso da informação, atenuando os riscos de perda de dados e maior facilidade de catalogação. MACEDO, op. cit., p. 24. Atualmente, os prontuários eletrônicos do paciente – PAP são regidos pela Lei nº 13.787 de 27 de dezembro de 2018, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente e pelas resoluções do Conselho Federal de Medicina. BRASIL. **Lei nº 13.787 de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 14 fev. 2023.

Figura 3 - Usos das tecnologias de Informação na Área da Saúde



Fonte: Adaptado de GONÇALVES, op. cit.

Com tantas vantagens, o cenário das tecnologias da informação aplicadas ao setor de saúde se torna mais do que atrativo, sendo um objetivo desejado pelas instituições públicas ou privadas, voltadas para o setor. Contudo, na prática, se verificam outros tipos de impacto que merecem atenção por parte de gestores, profissionais e usuários dos sistemas de saúde.

O primeiro ponto a ser considerado quanto as desvantagens da utilização de bancos de dados em saúde é o investimento financeiro. Para trabalhar com as ferramentas digitais é necessário realizar investimentos de alto custo em hardwares, softwares e equipamentos, programas de segurança e empresas de manutenção. É preciso ainda considerar os gastos para contratação e manutenção de uma equipe de T.I, bem como o treinamento dos demais profissionais envolvidos diante da complexidade do sistema de informação.

A alteração de rotina ocasionada pela utilização das tecnologias e banco de dados também costuma ser sentida pela equipe de profissionais de saúde, que por vezes resistem a adaptar suas práticas, alegando inclusive perda de autonomia. Levantam-se questões como a impessoalidade na relação médico-paciente, o risco de exposição de condutas clínicas e o aumento do tempo de trabalho burocrático. A título de exemplo, é possível citar a questão dos prontuários eletrônicos em saúde, os quais, devido à condição de usabilidade, processos de inserção dos dados, intercorrências assistenciais,

trabalho eficiente versus satisfação, dentre outras irregularidades, pode acarretar o estresse, esgotamento e insatisfação do profissional responsável.[214]

No que se refere ao assistido, há que se pensar nas condições de acesso e manuseio dos sistemas e aplicativos. Infelizmente os aspectos de analfabetismo digital ainda estão presentes em grande parte dos usuários do setor de saúde no Brasil, fato que dificulta o uso mais aprofundado dos serviços fornecidos pelos sistemas tecnológicos. Outros pontos de frequentes descontentamento residem nas quedas e instabilidade dos sistemas e plataformas[215], sem que se tenha suporte técnico adequado, além das questões de segurança e privacidade de dados.

A realidade é que na perspectiva dos riscos aos usuários dos sistemas de saúde, a questão revela desdobramentos tão ou mais profundos do que o próprio acesso à saúde frente a uma possível paralisação de atendimentos mediante falhas dos sistemas. As tecnologias da informação abrem risco[216] para a disseminação indevida de dados pessoais dos usuários dos sistemas de saúde, resultando em múltiplas possibilidades de danos, que na maioria dos casos, sequer chegam a ser considerados. Ainda se carece de uma consciência ampla acerca dos interesses envolvidos na vigilância e comercialização de dados de saúde.

3.4.2 Segurança da Informação em Saúde

A inserção das tecnologias nas organizações de saúde requer a coexistência de diversos sistemas para suportar as operações de gestão e assistência. Além dos sistemas tradicionais para registro eletrônico de dados do paciente, websites e aplicativos para prover serviços variados, encontra-se sistemas modernos permeados por inteligência artificial, especificamente desenvolvidos para diferentes práticas médicas. Dentre

214 PIPER, D. *et al*. The impact of patient safety culture on handover in rural health facilities. BMC Health Services Research, [*S.l.*], v. 18, n. 1, p. 889, 2018, p. 12. Disponível em: https://www.ncbi.nlm.nih.gov/pubmed/30477488. Acesso em 30 ago. 2022.

215 A título de exemplo, a queda do Sistema Conecte SUS em dezembro de 2021, amplamente divulgada pela imprensa nacional. Na ocasião o site do Conecte SUS e a página do Ministério da Saúde sofreram um ataque hacker prejudicando milhares de usuários em diversos pontos do país. O grupo que assumiu o ataque afirmou que 50 TB de dados internos foram 'copiados e excluídos. O Conecte SUS é o aplicativo responsável pela emissão do Certificado Nacional de Vacinação COVID-19, que na época era exigência obrigatória para acessar locais públicos. A queda dos sistemas teve reflexos pelo país: em Salvador, onde o comprovante começou a ser exigido na rodoviária, passageiros não conseguiram embarcar. No Piauí, houve filas para a vacinação. No Acre, quem perdeu o comprovante em papel não consegue tomar a 2ª dose ou a dose de reforço; o mesmo aconteceu no Oeste de Santa Catarina. O governo do Tocantins afirmou que não conseguiu notificar casos e mortes de Covid, entre outros prejuízos e dificuldades.

216 Risco pode ser definido, nesse contexto, como a probabilidade de um agente de ameaça aproveitar a vulnerabilidade, ou ainda "combinação da probabilidade de ocorrência de dano com a gravidade desse dano" (ABNT ISO/TR 18638:2019, 2019).

outros, pode-se mencionar os agendamentos de exames e consultas, informações, sistemas de logística, administração, finanças, recursos humanos e em alguns casos, educação e pesquisa

Com o aumento das demandas por novas funcionalidades que atendam as necessidades do processo de assistência de saúde eficiente à população, é necessária a integração de dados e a sistematização do imenso volume de informações gerado diariamente pelo setor. Configura-se aqui um cenário desafiador para os departamentos de tecnologia da informação (TI), encarregado de prestar suporte às organizações, especialmente no que se refere a performance e estabilidade dos sistemas, integridade dos dados e segurança das informações.

Os dados sensíveis de saúde indicam condições físicas e mentais da pessoa, e mediante seu potencial exploratório, despertam interesses escusos. A exposição de fragilidades dos indivíduos é considerada um produto valioso, apto a gerar vantagens econômicas para aqueles que exploram o mercado de medicamentos, planos de saúde [217]e seguros, por exemplo.[218]

É necessário trabalhar um equilíbrio entre a necessidade de se garantir a confidencialidade dos dados e a privacidade de seu titular e os benefícios gerados a partir da sua disponibilidade em formato eletrônico nas organizações de saúde. Vale ressaltar que o dado em si não pode ser considerado perigoso ou discriminatório, mas sim enquanto instrumento de desenvolvimento para área de saúde. A atenção deve ser centrada na finalidade para qual esse dado será utilizado, sempre observando os limites legai, a fim de reduzir a potencialidade lesiva de sua utilização.[219]

Nos termos da LGPD, as informações ou dados são coletados, manipulados e processados por três figuras distintas, a saber: o controlador, enquanto responsável

---

217 Como já mencionado anteriormente a LGPD veda expressamente às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. Artigo II, § 5º.

218 Para ilustrar essa visão, segue julgado do Tribunal de Justiça do Estado de São Paulo: Responsabilidade civil. Indenização por danos morais. Ação cominatória. Tratamento de dado sensível pela Lei nº 13.709/2018. Autora, que, após perda gestacional, recebeu oferta da ré a respeito de serviços de coleta e armazenamento de cordão umbilical. Ré que confirma ter recebido informações a respeito da autora de terceiros. Dados sensíveis, a respeito da gravidez da autora, que não poderiam ter sido objeto de compartilhamento, nos termos do art. 11, § 4º, da Lei nº 13.709/18. Ré que fez uso indevido de dado sensível pertencente à autora com finalidade lucrativa. Prospecção de novos clientes. Ato ilícito caracterizado. Violação do direito de privacidade da autora. Indenização corretamente determinada na sentença (R$ 10.000,00). Ré que tem a obrigação legal de identificar o responsável pela coleta do dado da autora, o que se deu sem consentimento. Sentença de procedência dos pedidos mantida. Recurso desprovido. TJ-SP - AC: XXXXX20218260100 SP XXXXX-35.2021.8.26.0100, Relator: Alexandre Marcondes, Data de Julgamento: 17/05/2022, 1ª Câmara de Direito Privado, Data de Publicação: 18/05/2022.

219 DONEDA, op. cit., p. 161.

pelo tratamento da informação; o operador, figura responsável por executar as ordens do controlador em relação ao processamento das informações e o oficial de dados[220], responsável pela execução das diretrizes definidas pelo controlador e operador , encarregado de cuidar das questões relativas à proteção dos dados da organização e de seus clientes.

Com relação ao tratamento de dados, o artigo 50 do diploma legal, concede aos controladores e operadores, no âmbito de suas competências, liberdade para a formulação e definição de regras de boas práticas e de governança para o tratamento de dados. O objetivo é estabelecer condições de organização, regime de funcionamento, procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.[221]

Conforme o mesmo artigo, ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular, bem como deverão apresentar as informações à Autoridade Nacional de Proteção de Dados.

Segundo o artigo 50, § 2º, inciso I da LGPD, o programa de governança em privacidade deve considerar transparência; gestão de riscos; adaptação à realidade; dimensão do tamanho e volume das operações da organização; governança com controles e monitoramento; monitoramento contínuo; efetividade do programa; aplicação de boas práticas, elaboração de código de conduta, com políticas e procedimentos e atualização periódica.

Embora a LGPD tenha apresentado, de forma clara, as definições de funções e meios para a elaboração de regras de controle das informações no processo de tratamento de dados, ainda existem riscos que precisam ser considerados. Os riscos enquanto ameaças a privacidade, devem ser conhecidos e neutralizados de modo a evitar possíveis vazamento de dados pessoais sensíveis dos pacientes na esfera da saúde individual e coletiva, seja no setor público ou privado.

220 *Data protection officer*, ou DPO, em referência a sigla em inglês.

221 LGPD, Artigo 50. Brasil, op. cit., 2018.

O quadro abaixo segue a norma ISO/IEC 29134:2017 que trata de técnicas de segurança para a avaliação de impacto à privacidade e apresenta os principais riscos verificados a partir do tratamento de dados e seus escopos.

Quadro 1 - Riscos Verificados a Partir do Tratamento de Dados e seus Escopos

Riscos Verificados a Partir do Tratamento de Dados e seus Escopos	
Riscos	Escopo do risco
Acesso não autorizado	Acesso indevido (permissões indevidas) a um ambiente físico ou lógico.
Coleção excessiva	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.
Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	Instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais - LGPD, art.27.
Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 23 da LGPD. Art. 17. O titular dos dados pessoais tem direito a obter do controlador mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
Falha ou erro de processamento (Ex.:execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.)	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.
Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma transparente e clara ao detentor dos dados pessoais.
Modificação não autorizada	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.
Perda	Perdas provocadas por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, e provenientes de ações não intencionais como falhas em sistemas, sobrescrita de dados, falhas em hardware, entre outras.
Reidentificação de dados e pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento simples de dados pessoais (LGPD, art. 12 e 13).
Remoção não autorizada	Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local.

Riscos Verificados a Partir do Tratamento de Dados e seus Escopos	
Retenção prolongada de dados pessoais sem necessidade	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro(a) dos dados pessoais.
Roubo	Dados roubados nas dependências interna do controlador/operador19, falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras.
Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Controlador de dados pessoais não obtém consentimento do titular para realizar um tratamento de dados pessoais sem embasamento legal.
Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	A realização de operação de processamento de dados pessoais deve estar em conformidade com a LGPD. Qualquer operação de processamento que não atenda esse requisito pode produzir informações com vinculações ou associações indevidas.

Fonte: Adaptado do Guia de Boas Práticas da LGPD, 2020[222].

Em atenção a necessidade de mitigar os mencionados riscos ao tratamento de dados, a LGPD indica em seu artigo 49 que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. Porém, o cumprimento de tal recomendação se revela extremamente desafiador, especialmente para empresas e organizações de pequeno porte que não se encontram familiarizadas com as políticas de *compliance.* [223]

O *compliance* aplicado a área da saúde se refere especialmente a necessidade de mecanismos que assegurem o cumprimento de regras e determinações referentes ao segmento, além de aperfeiçoar o modelo de gestão da organização por meio da prevenção, monitoramento e mitigação de riscos. Nesse sentido, encontram-se outros dois novos conceitos que despontam como fundamentais na estruturação de sistemas de tratamento de dados pessoais que atendam os padrões de segurança e princípios dispostos na LGPD: *privacy by design* e *privacy by default.*

Em uma conceituação simplificada, a privacidade por design indica a priorização da privacidade no processo de desenvolvimento de um produto ou serviço, sendo elemento central do projeto. Já a privacidade por padrão coloca a obrigatoriedade

222 BRASIL. Guia de boas práticas Lei geral de Proteção de Dados (LGPD). Brasil: Governo, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 11 ago. 2022.

223 O termo *compliance* tem origem no verbo *to comply*, da língua inglesa, e significa 'fazer certo', 'fazer o correto'. No meio empresarial, a expressão tem sido atribuída como uma ferramenta de prevenção de riscos existentes no âmbito de uma organização. Dentre os objetivos de um programa de *compliance* estão o cumprimento às leis e aos princípios éticos que regem as boas práticas empresariais; o estímulo ao desenvolvimento de uma cultura de controles internos; assegurar que a empresa atenda a todos os requisitos dos órgãos reguladores e fiscalizadores. SPÍNOLA, L. M. C. O Compliance no Setor Saúde. Revistas de Ciências Médicas e Biológicas, Salvador, v. 16, n. 2, p131-132, maio/ago. 2017, p. 131. Disponível em: https://doi.org/10.9771/cmbio.v16i2.24558. Acesso em: 30 ago. 2022.

das configurações de privacidade dos produtos ou serviços lançados no mercado apresentarem sempre configurações de privacidade em seu modo mais restrito como padrão, cabendo ao usuário liberar posteriormente acesso à coleta de mais informações.[224]

Logo, cabe aos agentes de tratamento de dados a adoção de medidas de segurança técnicas e administrativas, incluindo contramedidas[225], desde o momento da concepção do produto ou do serviço, até a sua execução, provendo meios de proteção aos dados pessoais de acessos não autorizados de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.[226]

Os dados em saúde são considerados valiosos em virtude de seu detalhamento, impactos na vida prática e possibilidade de identificação pessoal, tendo se tornado alvo preferencial de ataques cibernéticos. Logo, a garantia da segurança da informação se apresenta como prática essencial para as organizações de saúde, sejam públicas ou privadas, com atuação em qualquer segmento da atividade.

Em face da notável alteração nos padrões de cuidados à saúde acarretada pelo uso constante da internet, smartphones, redes sociais, registros eletrônicos em saúde, dispositivos móveis que permitem o monitoramento de dados clínicos, dentre outras inovações tecnológicas, surge uma urgente demanda pela segurança dos dados relacionados aos pacientes, usuários dos serviços de saúde, e aos seus processos assistenciais.

É preciso trabalhar medidas de gerenciamento e políticas de proteção aos sistemas de informação em saúde, evitando o acesso não autorizado, uso e divulgação indevidos, interrupção, modificação ou destruição de informações. Na sociedade da informação, os riscos, ameaças e vulnerabilidades devem ser medidos a partir de seu potencial de comprometer um ou todos os princípios fundamentais da segurança da informação.[227]

---

224 LEME, R. S.; BLANK, M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. Cadernos IberoAmericanos de Direito Sanitário, Brasília, v. 9, n. 3, p. 210-224, 2020, p.219. Disponível em: https://doi.org/10.17566/ciads.v9i3.690. Acesso em: 29 ago. 2022.

225 A contramedida ou salvaguarda da informação se refere a uma aplicação, configuração ou procedimento que mitiga o risco de vazamento de dados. Por exemplo: gerenciamento de senhas forte, um guarda de segurança, mecanismos de controle de acesso dentro de um sistema operacional, a implementação de senhas básicas do sistema de entrada/saída (BIOS) e treinamento de conscientização de segurança. As contramedidas ou salvaguardas nessa situação são atualização das assinaturas e a instalação do software antivírus em todos os computadores. HINTZBERGEN, J. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport; 2018, p. 262. Disponível em: https://pt.scribd.com/books. Acesso em 13 ago. 2022.

226 LGPD, Artigo, 46. BRASIL, op. cit., 2018.

227 SILVEIRA, S. A. Segurança da informação e proteção de pessoas: estudo de caso e proposta de dados de

A segurança dos dados pessoais sensíveis encontra-se diretamente conectada com segurança do paciente, enquanto indivíduo, uma vez que violações ou falhas no processo de garantia da integridade dos dados podem gerar prejuízos de ordem material, moral e até mesmo físicos, afetando a saúde daquele que tem sua intimidade invadida.

Embora as práticas de segurança cibernética de saúde sigam em constante evolução, certamente há necessidade de melhorias. O aumento da frequência de ataques ao sistema do Ministério da Saúde e outros bancos de dados do setor chama atenção para a necessidade de investimentos a serem empregados diretamente nas questões de segurança, bem como a demanda de recursos humanos capacitados para o manuseio dos sistemas.

Ao se tratar de segurança da informação, em sistemas de saúde, é importante ter em mente que os esforços para mitigação de riscos e falhas deve ser constantes. Sempre que se corrige uma vulnerabilidade, é preciso permanecer atento ao surgimento de outra, possivelmente, com maior potencial lesivo. São ciclos constantes que demandam políticas permanentes, as quias vão desde o controle de compras de equipamentos adequados às exigências de segurança, pesquisas e ações de atualização, até a capacitação de profissionais especializados em segurança cibernética aptos a propor constantemente melhorias na gestão da segurança da informação em saúde.

A informação em saúde, não é apenas valiosa, mas uma fonte de poder e por isso, demanda medidas de controle a fim de evitar abusos e ilegalidades por quem venha a ter acesso irrestrito aos dados, evitando-se que, em algum momento, o uso destes seja desviado.[228] Trata-se de uma preocupação que deve estar presente no cotidiano de entidades públicas e privadas, com a observação constante dos princípios balizadores do tratamento de dados pessoais sensíveis de saúde indicados na LGPD, de modo a assegurar os direitos fundamentais a saúde e a vida.

governança para serviços de saúde. 2021. Dissertação (Mestrado Profissional em Inovação Tecnológica) - Universidade Federal de São Paulo, São José dos Campos, 2021, p. 24.

228 PINHEIRO, P. P. Pandemia: gestão de crise e proteção dos dados pessoais. In: PALHARES, F. (org.). Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil, 2020, p. 508.

4 Capítulo 3 - Marcos da privacidade de saúde digital para o Brasil: uma retrospectiva documental

O terceiro capítulo da tese aborda a construção das políticas brasileiras de saúde digital. Neste tópico é realizada uma detalhada análise documental, considerando os pontos fortes e as fragilidades dos norteadores das principais políticas públicas em saúde que utilizam a tecnologia como ferramenta primária. Serão objeto deste estudo documentos formais endossados pelo Ministério da Saúde, tais como a Política Nacional de Informação e Informática em Saúde - PNIIS, as Estratégias de Saúde Digital para o Brasil, o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC e o Programa Conecte SUS, considerando a evolução teórica da matéria especificamente entre os anos de 2016 e 2021 e os dados coletados neste período.

Tal recorte temporal se revela apropriado em razão da disponibilização, no mencionado período, de documentos mais robustos e compatíveis com o cenário atual. No entanto, antes de iniciar a análise desse arcabouço, cabe apresentar uma linha do tempo a fim de contextualizar a posição de cada um dos textos escolhidos dentro do universo da informação em saúde no Brasil.

Quadro 2 – Atos normativos do cenário da informação em saúde no Brasil

Ano	Ato Normativo	Descrição
1990	Lei 8.080/1990	Lei Orgânica da Saúde. Art. 47 estabelece que o Ministério da Saúde, em articulação com os níveis estaduais e municipais do SUS, organizará, no prazo de dois anos, um sistema nacional de informações em saúde Sistema Nacional de Informações em Saúde (SNIS).
1991	Decreto 100/1991	Cria o Departamento de Informática do SUS (DATASUS) como parte da Fundação Nacional de Saúde (FNS), a partir da incorporação de bens da Empresa de Processamento de Dados da Previdência Social (Dataprev).
1996	Portaria GM/MS 2.390/1996	Institui a Rede Integrada de Informações para a Saúde (RIPSA).
1998	Resolução CNS 227/1998	Cria a Comissão Intersetorial de Comunicação e Informação em Saúde (CICIS).
1999	Lei 9.782 de 1999	Define o Sistema Nacional de Vigilância Sanitária e cria a Anvisa.
2000	Lei 9.961 de 2000	Cria a Agência Nacional de Saúde Suplementar (ANS).
2002	Portaria GM/MS 1.919/2002	Cria a Rede Interagencial de Informações para a Saúde (RIPSA).
2004	Relatório da 12a Conferência Nacional de Saúde	Publicação da Política Nacional de Informação e Informática em Saúde após discussão e recomendações da 12a Conferência Nacional de Saúde.
2005	Resolução CNS 349/2005	Reforma a Comissão Intersetorial de Comunicação e Informação em Saúde (CICIS).
	Instr. Normativa ANS 114/2005	Cria o Comitê de Padronização das Informações em Saúde Suplementar (COPISS).
2006	Portaria GM/MS 495/2006	Determina a reestruturação da Rede Interagencial de Informações para a Saúde (RIPSA).
2009	Portaria GM/MS 2.466/2009	Cria o Comitê de Informação de Informática em Saúde (CIINFO/MS).

Ano	Ato Normativo	Descrição
2011	Decreto 7.579/2011	Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) com a finalidade de definição da política de gestão de recursos de tecnologia da informação do poder executivo federal.
	Portaria GM/MS 2.072/2011	Reformula o Comitê de Informação de Informática em Saúde (CIINFO/MS).
2015	Portaria GM/MS 589/2015	Institui a Política Nacional de Informação e Informática em Saúde (PNIIS).
2016	Resolução CIT 05/2016	Institui o Comitê Gestor da Estratégia e-Saúde.
2017	Resolução CIT 19/2017	Aprova a Estratégia de e-Saúde para o Brasil.
	Portaria de Consolidação 1/2017	Consolidação das normas sobre os direitos e deveres dos usuários da saúde, a organização e o funcionamento do Sistema Único de Saúde.
2019	Decreto 9.795/2020	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Saúde, criando o Departamento de Saúde Digital.
	Resolução CIT 46/2019	Institui o Comitê Gestor da Estratégia de Saúde Digital e define a sua composição, as suas competências e as suas unidades operacionais na estrutura do Ministério da Saúde, em substituição ao Comitê Gestor da Estratégia de e-Saúde no Brasil.
2020	Decreto 10.230/2020	Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), do Poder Executivo Federal.
	Decreto 10.332/2020	Institui a Estratégia de Governo Digital para o período de 2020 a 2022.
	Portaria GM/MS 1.434/2020	Institui o Programa Conecte SUS e altera a Portaria de Consolidação GM/MS 1/2017, para instituir a Rede Nacional de Dados em Saúde (RNDS).
	Portaria GM/MS 3.632/2020	Institui a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28).
2021	Portaria GM/MS 1.046/2021	Estabelece as regras para integração dos resultados de exames realizados para a detecção da COVID-19 por laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional na Rede Nacional de Dados em Saúde (RNDS).
	Portaria GM/MS 1.068/2021	Institui o Modelo de Informação de Resultado de Exame Laboratorial COVID-19 na RNDS, plataforma de dados do Ministério da Saúde que visa a troca da informação assistencial entre os diversos pontos de atenção à saúde.
	Portaria GM/MS 1.768/2021	Aprova a Política Nacional de Informação e Informática em Saúde (PNIIS).

Fonte: GONÇALVES, *et al.*[229]

4.1 Política Nacional de Informação e Informática em Saúde (PNIIS)

As inovações tecnológicas características da quarta revolução industrial se tornam ainda mais evidentes nas matérias científicas e na área de saúde. A Organização Mundial de Saúde (OMS) afirma que a ideia de saúde deve ser compreendida em sentido amplo, como um estado de completo bem-estar físico, mental e social e não somente enquanto ausência de afecções e enfermidades.

Logo, trata-se de um processo em constante evolução. Diante da incorporação de tecnologias no setor da saúde[230], testemunha-se a cada dia a descoberta de novos

229 GONÇALVES, L. H. N.; *et al*. Dimensões subjetivas na Saúde Digital. **Liinc em Revista**, [*S.l.*], v. 18, n. 2, p. e6053, 2022. Disponível em: https://revista.ibict.br/liinc/article/view/6053. Acesso em: 15 jul. 2023.

230 Desde a década de 1970, as inovações tecnológicas no setor de saúde desenvolvem o que se denominou de e-Heath ou Saúde Eletrônica. Ver em: BRASIL. **A experiência brasileira em sistemas de informação em saúde**.

métodos para cuidar e melhorar a qualidade de vida da população, bem como o surgimento do que a OMS convencionou chamar de "*e-Heath*" ou "e-Saúde", com a criação de sistemas de informação e comunicação, que resultam na prática de atenção facilitada e aperfeiçoada para aquele que busca cuidados.

No Brasil, o e-Saúde[231] foi substituído pelo conceito de Saúde Digital que enfatiza a ampliação do alcance das diretrizes às soluções digitais para a saúde, tendo por foco o cidadão como protagonista de sua saúde frente à utilização de recursos tecnológicos. Tal visão, abrange assistência ao paciente, pesquisa, educação e capacitação da força de trabalho e monitoração e avaliação em saúde e se apresenta como resposta à necessidade de materializar o disposto no artigo 196 da Constituição Federal.

Segundo a referida norma constitucional, a saúde consiste em direito de todos e dever do Estado, a ser garantido mediante políticas sociais e econômicas que visem à redução dos riscos de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação. Dessa forma, a saúde é considerada digna da tutela protetiva estatal, apresentando-se como um dever do Estado a ser observado de forma plena, não apenas por meio de regulação legal, mas também através da efetivação de políticas públicas governamentais.

A responsabilidade do Estado pela criação e implementação de políticas públicas que assegurem acesso aos serviços necessários à promoção da saúde é instrumentalizada por meio de normas infraconstitucionais, tais como a Lei nº 8.080/90, que regulamenta o Sistema Único de Saúde, bem como estabelece princípios e diretrizes para a saúde em nosso país. Contudo, mediante o desafio de abarcar os novos paradigmas oriundos da influência da tecnologia, surge a necessidade de se propor novas regras para o setor de saúde. As propostas para o desenvolvimento e implantação da saúde digital foram sistematizadas e apresentadas pelo governo brasileiro nos últimos anos e embora afirmem a necessidade da proteção da privacidade dos dados de saúde, não se verifica até o presente momento, um aprofundamento adequado da questão.

Em que pese a elaboração de princípios e a indicação de atividades norteadoras e práticas futuras, a realidade atual carece de respostas concretas que ainda não se encontram disponíveis por meio de uma normativa específica. Para analisar este cenário e identificar as principais lacunas quanto a matéria, propõe-se a seguir uma

v. 2. Brasília: Editora do Ministério da Saúde, 2009.

231 O uso do conceito "e-Saúde" espelhava uma estratégia para a adoção de padrões de informática em saúde para o atendimento de diretrizes propostas pelas políticas de informação em saúde mundiais. Ver em: BRASIL. **Política Nacional de Informação e Informática em Saúde**. Brasília: Ministério da Saúde, 2016.

retrospectiva documental, que considerou os principais documentos expedidos pelo governo brasileiro entre os anos de 2016 e 2022, quando se realizou a coleta dos dados que embasa o presente texto.

No ano de 2016, foi apresentada a Política Nacional de Informação e Informática em Saúde - PNIIS com o objetivo de nortear ações de tecnologia da informação e comunicação (TIC) de todo o sistema de saúde brasileiro[232]. Para além de representar um marco significativo no contexto da proteção de dados e da utilização da tecnologia da informação na área da saúde no Brasil, referida política propôs estratégias para otimizar a gestão e o uso das informações em saúde, inclusive por meio da aplicação de tecnologias de informação e comunicação. Foi introduzida uma série de diretrizes, normas e ações com o objetivo de fomentar a melhoria da qualidade, da eficiência e da segurança dos serviços de saúde, de fortalecer o sistema de informação em saúde e de garantir a proteção dos dados pessoais de seus usuários.[233]

Em busca da aproximação com um modelo já adotado no cenário internacional, o texto da PNISS, formulado pelo Ministério da Saúde, previu o uso e a disseminação da tecnologia da informação entre instituições de saúde e seus profissionais, mediante a compatibilização e modernização dos sistemas de informação do SUS. Dessa forma, a informação em saúde deixou de ser vista sob um prisma meramente instrumental e passou a ser trada como ponto estratégico para a gestão do SUS, inclusive com caráter essencial na avaliação de serviços e promoção das Políticas de Saúde.

---

232 O texto da PNIIS, de caráter orientador, apresenta princípios e diretrizes norteadores de uma organização institucional, tais como: a melhoria da qualidade e do acesso ao sistema de saúde brasileiro; a transparência e segurança da informação em saúde; o acesso à informação de saúde pessoal como um direito do cidadão; o suporte da informação para tomada de decisão por parte do gestor e profissional de saúde; e, por fim, o desenvolvimento institucional do SUS e de todo o sistema de saúde brasileiro, com ganhos de eficiência na redução do número de sistemas de informação em saúde existentes ou sua simplificação, gestão e formação de pessoas, aquisição de insumos, monitoramento e avaliação das ações, logística, pagamento e transferência de recursos e outros processos-meio, pode ser visto em: Idem.

233 A PNIIS de 2016 (BRASIL, op. cit., 2016), objeto de análise deste estudo, tem por base a PNIIS de 2004 e a revisão de documentos relevantes, tais como o Plano Nacional de Saúde 2011-16, a Política de e-GOV, a Política Nacional de Ciência, Tecnologia e Inovação em Saúde, a série de documentos do Observatório de e-Saúde, da Health Metrics Network da OMS e da recente resolução do Executive Board da OMS sobre Padrões e Interoperablidade, bem como documentos da comunidade europeia sobre e-Saúde. A Política foi aprovada pelo CIINFO, com representantes das instâncias diretivas do MS e das entidades vinculadas ao MS, pela Comissão Intergestores Tripartite (CIT) e pelo Conselho Nacional de Saúde (CNS). Sendo assim, este documento possui representatividade e legitimidade, estando apto a amparar a institucionalização e normatização da informação e da informática no âmbito do sistema de saúde brasileiro. Vale, por fim, destacar, que esta política foi instituída pela Portaria nº 589/15, publicada no Diário Oficial da União (DOU), de 22 de maio de 2015. BRASIL. Portaria n. 589/15, de 20 de maio de 2015. Institui a Política Nacional de Informação e Informática em Saúde (PNIIS). Diário Oficial da União (DOU), de 22 de maio de 2015. Brasília: Ministério da Saúde. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2015/prt0589_20_05_2015.html. Acesso em: 14 fev. 2023.

A PNIIS de 2016 está dividida em seis grandes capítulos, que se iniciam com a apresentação do propósito e de princípios, seguidos por diretrizes relativas aos sistemas e-Gov e e-Saúde, gestão da PNIS e formação de pessoal para o SUS. Na sequência, tem-se um capítulo dedicado aos usos da informação, outro que trata da sustentabilidade e governança da política e por fim, a indicação de recomendações e perspectivas.

No que se refere aos objetivos, a PNIIS de 2016 prioriza o fomento ao uso adequado e ético das informações de saúde, com a indicação de que as informações de saúde sejam utilizadas de maneira segura, respeitando a privacidade e a confidencialidade dos pacientes. Neste sentido, são apresentados mecanismos protetivos comoa anonimização e a pseudonimização, e bem como prevê a necessidade de diretrizes para o compartilhamento seguro e consentido das informações entre os diversos atores do sistema de saúde.[234]

Também se verifica no texto a intenção de fortalecer a integração e interoperabilidade dos sistemas de informação em saúde, por meio da adoção de padrões e tecnologias que permitam a interoperabilidade dos referidos sistemas, viabilizando o compartilhamento e a troca de informações entre diferentes níveis de atendimento. Esse intercâmbio de informações seria essencial para uma melhor coordenação do cuidado, o monitoramento da saúde da população e a realização de pesquisas em larga escala.

Nessa linha, outro objetivo que merece destaque é o incentivo à pesquisa e inovação em saúde a fim de gerar conhecimentos que resultem na promoção da saúde e na melhoria da qualidade dos serviços no Brasil. Para tanto, são apresentadas, de forma tímida, algumas diretrizes para o uso seguro e ético dos dados de saúde. A mencionada política fomenta, ainda, a realização de estudos epidemiológicos e a descoberta de novos tratamentos e tem por pretensão traçar um panorama preciso e abrangente da situação sanitária do país, identificando desafios e demandas específicas de cada região.

A junção destes objetivos converge para a possibilidade de criação de estratégias de otimização de gestão a partir do uso das informações em saúde, por meio da aplicação de tecnologias de informação e comunicação. Seria possível estabelecer um direcionamento mais eficiente de recursos, bem como aperfeiçoar o planejamento de ações preventivas e controle de doenças, inclusive por meio do monitoramento de indicadores de desempenho e de qualidade dos serviços de saúde. Este escopo também se encontra presente na apresentação dos propósitos da PIINIS 2016.

234 Brasil, op. cit., 2016, p.11.

Aprofundando na leitura dos propósitos descritos no documento, destaca-se o trecho inicial no qual se menciona a ambiciosa ideia de promover o uso "inovador, criativo e transformador da tecnologia da informação a fim de melhorar os processos de trabalho em saúde", que resultaria em um Sistema Nacional de Informação em Saúde (SNIS) mais eficiente[235]. A tecnologia seria o meio para materializar uma articulação de informações, inclusive entre o sistema de informação público e o privado, ampliando o acesso, a qualidade e até mesmo humanizando os serviços de saúde. Diante disso, resta inevitável o questionamento quanto à segurança dos dados e à proteção da privacidade dos usuários do sistema de saúde.

Em seu conteúdo, a questão da privacidade surge inicialmente na apresentação de seus nove princípios básicos que incluem a confidencialidade, sigilo e privacidade da informação de saúde pessoal como direito de todo indivíduo. Posteriormente, privacidade figura como um dos pilares da PNIIS junto à infraestrutura de TI, incluindo a conectividade; a governança e a gestão de pessoas na área de informação e informática em saúde; os padrões para garantir a interoperabilidade e as terminologias e o desenvolvimento do arcabouço legal para garantir a privacidade e confidencialidade dos dados identificados em saúde[236].

Sob outro prisma, a privacidade e a confidencialidade são indicadas no documento entre as principais barreiras para a implantação de projetos de TI em saúde, ao lado de financiamentos, falta de evidências do retorno do investimento, infraestrutura inadequada especialmente para pequenas clínicas e falta de cultura no uso do computador. [237]Tem-se, portanto, a questão da privacidade tratada de forma paradoxal: ora como objeto direto de salvaguarda e proteção, ora como obstáculo à concretização dos objetivos propostos pelo aludido diploma.

Além deste ponto conflituoso, a análise da PINIIS 2016 revela lacunas importantes que resultam em questões problemáticas não apenas em termos teóricos, mas sob o viés prático de quem utiliza os sistemas de saúde no Brasil. Com efeito, o texto elaborado há menos de uma década se mostra imaturo em face do alcance da tecnologia e, a despeito de sua importante contribuição, suscita fortes questionamentos especialmente quanto aos aspectos relacionados à segurança e à privacidade e em curto período já demandava atualizações frente a entra em vigor de novos diplomas legais, dentre os quais destaca-se a LGPD.

235 Idem, p. 12.
236 Ibid., p. 14.
237 Ibid.

A PINIIS 2016 não forneceu uma definição clara para dados pessoais e menos ainda para dados sensíveis, o que abre via para a interpretações inconsistentes e lacunas no momento de estabelecer proteção destas informações, ocasionando riscos no momento da declaração de vontade e violação de privacidade. Considerando o potencial lesivo e discriminatório frente a um possível vazamento de dados de saúde, a ausência de salvaguardas específicas para essas categorias de dados poderia expor os indivíduos a riscos de declaração viciadas e violação de privacidade.

Embora o texto aborde alguns direitos dos titulares de dados, como acesso e retificação, a PINIIS 2016 não aborda de forma clara outros direitos importantes, como o direito ao esquecimento, portabilidade de dados e restrições de processamento. Não há previsão expressa sobre o futuro destes dados e, mesmo quando se refere ao manuseio de dados atuais, resta perceptível a existência de lacunas quanto à privacidade e segurança. Por exemplo, não foram especificados os requisitos técnicos ou organizacionais mínimos exigidos para salvaguardar a privacidade dos titulares de dados pessoais inseridos nos sistemas de saúde, o que enseja riscos de vazamento de dados ou acessos não autorizados.

Outro ponto que prejudica a concretização dos objetivos propostos na PINIIS 2016 é a ausência da indicação de um órgão regulador independente, apto a supervisionar a implementação da lei e garantir a conformidade das organizações. Não há como prescindir de uma fiscalização efetiva e constante que assegure a aplicação consistente das provisões de proteção de dados de saúde para órgãos e instituições de caráter público ou privado. Também seriam necessárias disposições que desencorajem práticas abusivas relacionadas aos dados de saúde e a privacidade de seus titulares.

Por fim, o documento também se mostra omisso quanto à proposta de requisitos claros para a conscientização e a educação do público em relação à proteção de dados e a indicação de uma estrutura adequada relacionada para lidar com os desafios emergentes à proteção de dados, como o uso de inteligência artificial, aprendizado de máquina e análise de big data.

A PINIIS 2016 foi um importante avanço face suas versões anteriores, especialmente ao destacar a informação em saúde como um insumo fundamental para o aperfeiçoamento do setor, visto que é a base para viabilizar o planejamento, a programação, a gestão e a avaliação do Sistema de Saúde. Contudo, a necessidade de

avanços principalmente na legitimação e aplicação da política em via prática gerou a abriu vias para novas propostas e atualizações[238].

Destarte, em agosto de 2021, o Ministério da Saúde publicou, a Portaria GM/MS nº 1.768/2021 para dispor sobre a nova PNIIS.[239] Após cinco anos da publicação da PNISS 2016, o novo documento reflete a necessidade de atualização da política pública frente ao contexto global constituído a partir do cenário da rápida evolução das tecnologias de informação e comunicação em saúde, além de considerar alterações no contexto nacional e na própria realidade social brasileira.

A revisão da PNIIS buscou esclarecer dúvidas e sanar lacunas ao abordar temas importantes, como a LGPD, Internet das coisas (IoT), Big Data, Governança de Dados, Inteligência Artificial. A alteração também pretende enfatizar o protagonismo do cidadão no uso das tecnologias nos próximos anos. São propostas que visam especialmente a aprimorar a governança no uso da informação, prover soluções de tecnologia da informação e da saúde digital. A intenção é definir diretrizes e práticas de modo a orientar o processo de informatização das instituições de saúde públicas e privadas; ampliar a conectividade em saúde, aumentar o número de profissionais capacitados e assegurar maior transparência e segurança quanto ao acesso e manuseio das informações. [240]

As alterações da PNIIS refletem um delicado trabalho técnico, favorecido pela colaboração de diversos sistemas digitais do DATASUS e assim como pela tentativa de alinhamento com diversos instrumentos de governança, dentre os quais destaca-se a Estratégia de Saúde Digital para o Brasil 2020-2028 - ESD28, a ser detalhada ainda neste capítulo.

Um ponto a ser destacado na nova versão da PNIIS, é o reconhecimento da Rede Nacional de Dados em Saúde - RNDS[241] como a plataforma digital para a saúde

238 Dentre as atualizações da PNIIS a partir de 2016, destacam-se a portaria GM/MS nº 2.319/17, que dispõe sobre as diretrizes para a Elaboração do Plano de Gestão de Dados Abertos do Ministério da Saúde; A portaria GM/MS nº 4.418/18, que dispõe sobre a governança das tecnologias de informação e comunicação no âmbito do Ministério da Saúde e a portaria GM/MS nº 1.995/21, que institui a Política de Governança Digital no âmbito do Ministério da Saúde. Ibid.

239 BRASIL. Portaria GM/MS nº 1.768/2021, de 30 de julho de 2021. Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). Brasília: Ministério da Saúde, 2021. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2021/prt1768_02_08_2021.html. Acesso em: 12 jan. 2023.

240 BRASIL, op. cit. 2021.

241 A RNDS configura uma das principais ferramentas criadas pelo Ministério da Saúde para implementação da PNIIS, bem serve de alicerce nos termos da publicação da Estratégia de Saúde Digital para o Brasil 2020-2028 (regulamentada pela Portaria GM/MS nº 3.632/2020). BRASIL. Portaria GM/MS nº 3.632/2020, de 21 de dezembro de 2020. Altera a Portaria de Consolidação GM/MS nº 1, de 28 de setembro de 2017, para instituir a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28). Brasília: Ministério da saúde, 2020a.

e como repositório nacional de dados. Desta forma a RNDS se torna a principal ferramenta a ser utilizada na promoção da troca de informações entre os diferentes pontos da Rede de Atenção à Saúde para a continuidade do cuidado, tanto na esfera pública, quanto na esfera privada.

Além desta atualização, um avanço positivo foi o reconhecimento dos dados sensíveis pessoais, com a previsão de princípios como: a promoção do acesso aberto aos dados e à informação em saúde enquanto direito do cidadão; preservação da autenticidade, da integridade, rastreabilidade e da qualidade da informação em saúde; e autonomia do usuário na decisão sobre o compartilhamento dos seus dados.[242]

Ademais, a PNIIS atualizada destaca atribuições para os estabelecimentos de saúde em todo o território nacional, intencionando a realização de procedimentos e adequações necessárias em seus sistemas de informação para uso da RNDS. Há uma preocupação em assegurar o envio de dados e informações referentes aos atendimentos em saúde à RNDS para a composição do histórico clínico dos pacientes, conforme os protocolos operacionais definidos.

Caberá ainda às instituições de saúde disponibilizar as informações definidas como necessárias pelo Ministério da Saúde, Secretaria de Estado da Saúde e Secretaria Municipal de Saúde ou do Distrito Federal, assegurar os procedimentos necessários para propiciar a segurança dos dados pessoais de saúde, bem como zelar pela privacidade e confidencialidade dos dados pessoais de saúde a que tenha acesso[243].

Aos profissionais de saúde, foi atribuída uma responsabilidade pela autoria e pela qualidade dos dados produzidos e colhidos em razão dos serviços prestados, bem como o dever de zelar pela privacidade e confidencialidade dos dados pessoais de saúde a que

---

Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2020/prt3632_22_12_2020.html. Acesso em: 14 jul. 2023.

242 Art. 2º São princípios da PNIIS: IV - promoção do acesso aberto aos dados e à informação em saúde como direito do cidadão; VI - preservação da autenticidade, da integridade, rastreabilidade e da qualidade da informação em saúde, observado o disposto na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados; VIII - autonomia do usuário na decisão sobre o compartilhamento dos seus dados de saúde com profissionais da área de saúde que atuem na sua assistência, com órgãos de pesquisa ou com órgãos ou entidades de saúde públicas e privadas, respeitadas as obrigações legais de compartilhamento para vigilância em saúde e gestão da saúde pública; Portaria GM/MS Nº 1.768, de 30 de Julho de 2021. Brasil, op. cit., 2021.

243 Art. 18. Compete aos estabelecimentos de saúde em todo o território nacional: I - realizar, de maneira gradativa, conforme planejamento estipulado pelas esferas de gestão, por meio do CGSD, as adequações necessárias em seus sistemas de informação relativas ao uso da RNDS; II - enviar os dados e informações referentes aos atendimentos em saúde à RNDS para a composição do histórico clínico dos pacientes, conforme os protocolos operacionais definidos; III - disponibilizar, fidedignamente e em tempo oportuno, as informações definidas como necessárias pelo Ministério da Saúde, Secretaria de Estado da Saúde e Secretaria Municipal de Saúde ou do Distrito Federal; IV - assegurar os procedimentos necessários para propiciar a segurança dos dados pessoais de saúde; e V - zelar pela privacidade e confidencialidade dos dados pessoais de saúde a que tenha acesso. Portaria GM/MS Nº 1.768, de 30 de Julho de 2021. BRASIL, op. cit., 2021.

tenham acesso. Por sua vez, incumbe aos usuários zelar pelo bom uso de seus dados de saúde e das pessoas sob sua responsabilidade, bem como monitorar e participar da ampliação do uso da RNDS como um bem público para toda a sociedade brasileira, por meio dos conselhos de saúde e pelos canais de comunicação disponíveis para os cidadãos.

A preocupação com a segurança dos dados também ganhou ênfase a partir de indicações práticas para o cotidiano das instituições de saúde. Como exemplos, podem ser mencionadas a recomendação de adoção de padrões mínimos de segurança nos sistemas de prontuários eletrônicos; a uniformização de vocabulários, terminologias e nomenclaturas; e a adequada gestão documental de histórico clínico do paciente, garantindo-lhe continuidade na rede de cuidado em saúde As mencionadas recomendações têm em comum o objetivo de estimular a interoperabilidade entre diferentes sistemas e a RNDS, a Política Nacional de Informação e Informática em Saúde recomenda.

Por fim, cabe destacar a inovação trazida pela nova versão da PNIIS, com o reconhecimento da possibilidade de uso de novas ferramentas tecnológicas que incluem, mecanismos de segurança de acesso aos sistemas, dados e informações de saúde, que garantam sua disponibilidade, autenticidade e integridade, com incentivo ao uso de assinatura eletrônica e sistemas biométricos; modelos de informação mínimos nacionais, bem como dos vocabulários e terminologias em saúde; soluções de saúde digital de alto impacto para intervenções comunitárias, de forma a ampliar a cobertura de promoção da saúde para grupos vulneráveis e outros grupos priorizados e inteligência artificial e big data para fornecer evidências para políticas, pesquisa e planejamento, para que as descobertas na saúde digital se traduzam em ações.[244]

Finda a análise da PNII, com a compreensão do caminho evolutivo iniciado em 2016, é relevante compreender os documentos e políticas que lhe servem de base, desenhando um panorama do progresso da saúde digital no Brasil. No cumprimento desta proposta, o próximo item se dedica a analisar as Estratégias de Saúde Digital para o Brasil 2017 – ESD 17.

244 Recomenda-se a leitura da seção IV Ambiente de Conectividade em Saúde e da SEÇÃO VII Ecossistema de Inovação. BRASIL, op. cit., 2021.

4.2 Estratégias de saúde digital para o BRASIL 2017

Um olhar mais concreto sobre a saúde digital foi ofertado por meio do documento intitulado "Estratégia e-Saúde para o Brasil", aprovado pela Resolução CIT nº 19, de 22 de junho de 2017, da Comissão Intergestores Tripartite (CIT), que apresentou diretrizes e princípios para o Sistema Único de Saúde (SUS) e dispôs sobre a política brasileira de governo eletrônico, com destaque para a proposta de Saúde Digital, inclusive apontando mecanismos contributivos para sua incorporação ao SUS.

Conforme tal documento, a e-Saúde estaria incorporada ao SUS na condição de dimensão fundamental até o ano de 2020, possibilitando uma melhoria consistente dos serviços de saúde por meio da disponibilização e uso de informação abrangente, precisa e segura. Seriam as tecnologias aplicadas um caminho para que se atinja um patamar superior de qualidade na atenção e nos processos de saúde, nas três esferas de governo, bem como no setor privado, beneficiando pacientes, cidadãos, profissionais, gestores e organizações de saúde[245].

Nesse documento, foi apresentada uma proposta para o e-Saúde na qual se desenham caminhos e estratégias práticas para que haja uma conexão entre o poder público, instituições de pesquisa e ensino, empresas privadas, de saúde suplementar, de desenvolvimento e fornecimento de sistemas de informação e prestadores de serviços de informática em saúde, apto a viabilizar o aumento do impacto dos sistemas de informação em saúde, otimizando dispositivos e processos no SUS.

A Estratégia e-Saúde para o Brasil 2017 teve o cuidado de embasar suas proposições em uma exposição do contexto do sistema de saúde brasileiro, destacando informações e dados relevantes quanto à saúde no país, bem como abordando a gestão do SUS e seus principais desafios. Em seu segundo capítulo aprofunda o conceito do e-Saúde, citando experiências bem-sucedidas de outros países e defendendo a maturidade institucional e tecnológica brasileira para implementar com sucesso, um ambiente que materialize as propostas expostas no texto do documento.

Neste ponto, também é realizada uma conexão entre os objetivos e diretrizes do SUS e o conceito de e-Saúde. Os objetivos do SUS para 2015 são sintetizados no Plano Nacional de Saúde 2016 - 2019[246]. A previsão é que as diretrizes previamente definidas, inclusive aquelas de caráter transversal, podem ser otimizadas e diretamente

245 BRASIL. **Estratégia de Saúde Digital para o Brasil 2017**. Brasília: Ministério da Saúde, 2017.

246 BRASIL, Plano Nacional de Saúde – PNS: 2016-2019. Brasília: Ministério da Saúde (MS), 2016.

beneficiadas a partir do uso da TIC. A pretensão seria integrar programas e a agregar recursos, viabilizando um cenário no qual as ações de e-Saúde interoperam entre si e com sistemas externos, mesmo que utilizem tecnologias diferentes e estejam em esferas distintas de governo, ou no setor privado[247].

Apresenta-se ainda o objetivo de identificar as políticas, os modelos de governança, os mecanismos de financiamento, a infraestrutura, as tecnologias e os recursos humanos necessários para materializar o que o documento apresenta como "ações estratégicas"[248] necessárias para a implantação da Visão do e-Saúde.

Em sequência, tem-se a descrição de como recursos de e-Saúde[249] podem contribuir para o objetivo da ampliação do acesso e qualidade dos serviços de saúde com propostas de ações transversais que caracterizam a essência da Visão de e-Saúde para o Brasil, tais como o Registro Eletrônico de Saúde (RES), Apoio à Mobilidade, Gestão e Disseminação de Conhecimento, Gestão do Fluxo de Pacientes, Gestão e Operação das Unidades de Saúde, Gestão Integrada do SUS. Cada sugestão de ação é composta pelo conceito e a descrição dos benefícios esperados, porém, o texto não apresenta indicativos de efetivação.

Um ponto que certamente merece destaque é a indicação de pilares próprios para assegurar que a visão de e-Saúde para o Brasil possa ser concretizada de maneira satisfatória. É válido lembrar que embora a estrutura inicialmente proposta siga o modelo internacional, a realidade do Brasil e, em particular, do SUS, apresenta características específicas que demandam adaptação da experiência internacional e criatividade para assegurar o correto desempenho do e-Saúde em solo brasileiro.

Por este motivo, considera-se necessária a seção subsequente, especificamente voltada para identificação e avaliação crítica dos pilares considerados necessários para concretizar a visão proposta para a e-Saúde, os quais foram agrupados em quatro grupos: Governança e Recursos Organizacionais, Padrões e Interoperabilidade, Infraestrutura, e Recursos Humanos. Dentro de cada grupo, foram identificados os construtores necessários, bem como os construtores que já existem na via prática,

247 BRASIL, op. cit., 2017, p. 33.

248 O documento trouxe nove propostas de ações estratégicas em seu capítulo 4, que são apresentadas de forma resumida nos anexos deste trabalho.

249 A noção de e-Saúde trazia como principal objetivo a proposta de contribuir para a ampliação da qualidade, bem como do acesso à atenção à saúde por meio do uso das tecnologias de informação (TIC). Para tanto, o conceito proposto trabalhava os saberes e práticas inerentes a esta área do conhecimento, direcionando-os para promover a qualificação das equipes de saúde e assegurar mais eficiência em seus processos e práticas cotidianas. Previa-se que até o ano de 2020, a e-Saúde estará incorporada ao SUS como uma dimensão fundamental. (WHO - WORLD HEALTH ORGANIZATION. World health statistics 2012. Geneva: World Health Organization, 2012. Disponível em: https://apps.who.int/iris/handle/10665/44844. Acesso em: 25 jan. 2023.

suas características básicas e desempenho. Também foram mapeadas assim iniciativas relevantes, não apenas em saúde, mas em qualquer outra área, desde que apta a impactar positiva ou negativamente a concretização da estratégia de e-Saúde[250].

A iniciativa de buscar identificar as lacunas entre os blocos existentes e os previstos como necessários, foi um ponto extremamente positivo que possibilita a otimização e até a reutilização de recursos e práticas nas áreas de infraestrutura e recursos humanos. Com este diagnóstico também foi possível propor linhas de ação visando superar obstáculos ou, conforme o caso, acelerar o desenvolvimento de uma estratégia de e-Saúde.

No tópico "Governança e Recursos Organizacionais", é mencionada, como exemplo de recurso necessário para a implantação da Visão de e-Saúde, a necessidade de uma legislação específica para que o Sistema de Registro Eletrônico de Saúde possa coletar dados e informações de diversos prestadores, públicos e privados, e apresentá-los a profissionais e indivíduos autorizados a acessá-los. Tal menção, é apresentada em conjunto com questionamentos tais como "a legislação existente é necessária e suficiente? Há a necessidade de legislação adicional e para que fins?" que reforçam o entendimento quanto ao panorama legal incipiente sobre a matéria na época e convidam para uma reflexão sobre o tema no momento presente.

Menciona-se ainda a necessidade da definição de princípios éticos e legais que possam ser utilizados como parâmetros, bem como do estabelecimento de um Plano de Ações Estratégicas e de Investimentos, que garanta o financiamento de longo prazo das ações da e-Saúde. O próprio documento apresenta, em seu diagnóstico, a informação de que as estratégias e os investimentos em aplicações de e-Saúde no Brasil têm sido tradicionalmente definidas e executadas de forma difusa, em iniciativas isoladas nas três esferas de governo (federal, estadual e municipal), que carecem de interação[251]. Outro ponto de fragilidade indicado é a ausência de qualificação de gestores e número insuficiente de profissionais de TI para e-Saúde.

Com efeito, a adoção de tecnologias no setor da saúde não foi absolvida com a rapidez necessária. Verifica-se a dificuldade dos profissionais da área, nos mais diversos setores quanto ao uso dos dispositivos e de dados e informação digital, problema que se agrava com a utilização de sistemas de informação fragmentados e interfaces de baixa usabilidade. O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), também registra o fato de que os instrumentos legais e regulatórios referentes à matéria

250 BRASIL, op. cit., 2017, p. 48.
251 Idem, p. 50.

estavam essencialmente voltados para atender necessidades imediatas, sem apresentar conexão com projetos de médio e longo prazo.

Assim, embora se perceba que há tecnologia, conhecimento e boas práticas já implantadas que podem e devem ser replicadas, há uma carência significativa no tocante à articulação e ao alinhamento de aspectos essenciais para a Visão de e-Saúde como liderança, governança, investimento, políticas, e regulação, o que dificulta otimização de resultados e gera situações de redundância e contradição.

Como solução, são indicadas no tópico quatro, ações estratégicas com objetivo de adequar os recursos e consolidar a e-Saúde como Política de Estado relevante para SUS, integrando programas e agregando recursos. Seriam elas o caminho para fortalecer a intersetorialidade na governança de e-Saúde e firmar o marco legal de e-Saúde no país.

As ações estratégicas são norteadas por diversos princípios que preveem um alinhamento direto com a gestão do SUS. Como exemplo, é possível citar o princípio da adoção das diretrizes do SUS; respeito às instâncias gestoras do SUS; respeito às normas operacionais de gestão do SUS; participação nas instâncias gestoras do SUS; fortalecimento da participação interdisciplinar e multidisciplinar, nas diversas iniciativas governamentais, principalmente as voltadas para ciência, tecnologia, educação, planejamento e comunicações; redução de assimetria das informações em saúde; reconhecimento dos agentes do processo de e-Saúde, enquanto indivíduos, profissionais de saúde, de informação e de informática em saúde e gerências de serviços de saúde, gestores do Sistema de Saúde, legisladores e autoridades governamentais; revisão e adequação da legislação às necessidades de aquisição de serviços de TIC.[252]

A primeira dentre as nove estratégias propostas, tem por objetivo reduzir a fragmentação das iniciativas no SUS e aprimorar a governança da estratégia de e-Saúde. Nesta senda, desde 2013, existe a resolução da Comissão Intergestores Tripartite do Sistema Único de Saúde – CIT[253] a qual estabelece que todos os sistemas de informação ou aplicativos a serem implantados no SUS ou novas versões de sistemas e aplicativos já existentes terão seus modelos, regras de negócio e cronograma de implantação apreciados no âmbito da Câmara Técnica da CIT e pactuados na CIT.

252 Ibid, p. 55.

253 BRASIL. **Resolução CIT n. 6, de 6 de novembro de 2013**. Dispõe sobre as regras para implantação de novos aplicativos, sistemas de informação em saúde ou novas versões de sistemas e aplicativos já existentes no âmbito do Sistema Único de Saúde (SUS) e que envolvam a sua utilização pelo Ministério da Saúde e Secretarias Estaduais, do Distrito Federal e Municipais de Saúde. Brasília: Ministério da Saúde, 2013. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/cit/2013/res0006_06_11_2013.html. Acesso em: 3 jul. 2023.

A proposta de padronização dos sistemas, contudo, consiste apenas na primeira etapa do trabalho. Há, ainda, a clara necessidade de se alinhar e fortalecer as instâncias de governança da informação no SUS/MS, de modo a se direcionar os recursos existentes para a implantação da visão de e-Saúde – o que não se configura como uma tarefa simples, visto que demanda a constituição de um arcabouço institucional apto a orquestrar diferentes ações simultaneamente.

Uma vez colocada esta ação em prática, a previsão seria uma redução de barreiras viabilizando a meta da interoperabilidade entre os sistemas, com a consequente redução da instabilidade administrativa a cada ciclo de gestão; previu-se ainda a existência de ambiente favorável à definição de políticas e a gestão de mudanças, bem como uma estratégia de construção coletiva de e-Saúde consolidada e adoção recorrente das melhores práticas para a construção da e-Saúde.

A segunda estratégia apresentada primou pela ideia de fortalecer a intersetorialidade de governança de e-Saúde, buscando uma dimensão nacional à Visão de e-Saúde para o Brasil. Por meio desta proposta seria possível integrar programas e agregar recursos de todos os setores de governo, da sociedade civil e da iniciativa privada para viabilizar a Visão de e-Saúde. O desenvolvimento desta ação ficou a cargo do Ministério da Saúde, juntamente com outros Ministérios, tais como o das Comunicações; do Planejamento; da Educação, da Ciência, Tecnologia e Inovação; do Desenvolvimento, Indústria e Comércio Exterior; além de entidades setoriais da esfera pública e privada.[254]

Os objetivos do estabelecimento dessa dimensão nacional abrangem desde a proposta de ações intersetoriais e alinhamento estratégico dos programas de governo até a indicação de entidades de referência consolidadas para os demais componentes de e-Saúde, além de modelos definidos e avaliados para a gestão de investimento em e-Saúde nas áreas de pesquisa, inovação, manutenção, infraestrutura, e eixos correlacionados. Haveria a implantação da cultura e prática de intersetorialidade das ações governamentais e a construção coletiva de e-Saúde consolidada.

A terceira estratégia aponta a necessidade da elaboração do marco legal de e-Saúde no País adequado às inovações tecnológicas de informação e comunicação. O documento enfatiza que a proposta deverá ser concebida de forma flexível e robusta, de modo a suportar o modelo de governança descentralizada, característica fundamental do SUS. Seria este o caminho para promover um processo de interlocução permanente com a sociedade, mitigando possíveis descompassos entre os avanços tecnológicos e o marco

254 BRASIL, op. cit., 2017, p. 62.

legal, além de configurar uma oportunidade de consolidar iniciativas governamentais em temas relevantes a e-Saúde.

O que se espera por meio desta estratégia é principalmente a criação de uma legislação, flexível e robusta, que favoreça o desenvolvimento de ações e da visão e-Saúde, com a definição de normas que permitam planejamento e investimento de longo prazo. Consequentemente se prevê a redução dos custos decorrentes de liminares judiciais por ausência de legislação, bem como a redução da ingerência na gestão das informações de saúde. Outra previsão importante, seria a possibilidade de se viabilizar garantias para a privacidade e proteção contra o uso indevido de informações de saúde do indivíduo.

A definição de uma arquitetura para a e-Saúde constitui a quarta estratégia. Parte-se da ideia de uma rede flexível, distribuída, robusta e interoperável de sistemas e serviços, descrita como um processo de longo prazo que requer a definição de métodos e padrões, além de uma sólida arquitetura, escalável e baseada em camadas de blocos reutilizáveis.

Neste caso, se utilizaria tanto a experiência nacional, quanto a internacional em arquiteturas para e-Saúde para nortear os padrões a serem adotados, melhorando processos e replicando boas práticas, considerando blocos reutilizáveis: modelos de informação e artefatos de conhecimento; modelo para interoperabilidade; serviços de terminologia; cadastros nacionais de identificação; consentimento; serviços e sistemas de segurança e privacidade e arquitetura de intercâmbio de informações de saúde[255].

A quinta estratégia apresenta caminhos de materialização e prevê a definição e implantação dos sistemas e serviços de e-Saúde. A pretensão seria de identificar, priorizar, estimular o desenvolvimento e/ou adquirir sistemas e serviços de e-Saúde aderentes à arquitetura de e-Saúde apresentada na estratégia anterior. Para tanto, é fundamental a especificação funcional dos componentes dos processos de atenção à saúde, bem como das aplicações de gestão do SUS. Neste ponto, há a previsão de se indicar critérios para avaliação contínua dos sistemas desenvolvidos e/ou adquiridos, bem como de processos de priorização de sua evolução e expansão.

Com a evidente dependência dos fatores tecnológicos, surge a urgência em disponibilizar serviços de infraestrutura computacional. Tal preocupação se encontra expressa na sexta estratégia, a qual destaca que a estrutura a ser criada deve ser adaptável às rápidas evoluções tecnológicas, e planejada de forma sinérgica, gerando serviços

255 Idem, p. 64.

de infraestrutura sustentáveis, otimizando ações e resultados. Contudo, as questões envolvendo as TIC´s ainda configuram desafios para o poder público em face de sua volatilidade e do consequente volume de investimentos necessário para manter os serviços desejados.

Por outro lado, é preciso analisar referida questão em longo prazo. A disponibilização de infraestrutura computacional e tecnológica como serviço poderá proporcionar diversos ganhos ao poder público, como por exemplo, maior capacidade de gestão, acesso direto a informações, velocidade no atendimento, redução de processos burocráticos, entre outras vantagens.

Para tanto, a mencionada estratégia indica a revisão e adequação da legislação existente para atender às necessidades de aquisição de serviços de infraestrutura de TIC e indica caminhos pelos quais seria possível atingir este objetivo. Dentre os itens mencionados, destacam-se: a ampliação da capacidade de infraestrutura computacional por meio da contratação preferencialmente como serviço; consolidação de infraestrutura de Gestão de TIC responsável e compatível com o alcance proposto para a e-Saúde e baseada em melhores práticas de mercado; fortalecimento do Plano Nacional de Banda Larga; ampliação da infraestrutura computacional para disponibilizar os serviços de segurança; disponibilização de infraestrutura para o provimento de serviços de captura de dados de saúde para a e-Saúde, bem como de repositórios de dados de saúde individualizados; criação e promoção de condições de compartilhamento de recursos de infraestrutura entre os entes do SUS; ampliação e consolidação da infraestrutura de TIC e os respectivos elementos de gestão nos entes públicos das três esferas de governo. [256]

Com isso, seria possível a construção de uma infraestrutura computacional adequada à demanda do e-Saúde, a partir de uma gestão de TIC ampliada, compatível com o alcance proposto e que seria baseada nas melhores práticas de mercado. Neste diapasão incluem-se as propostas de utilização da infraestrutura proposta pelo Plano Nacional de Banda Larga (PNBL) e a disponibilização de serviços de segurança, identificação e autenticação, com infraestrutura adequada para a coleta e armazenamento de dados individualizados para a e-Saúde.

A sétima estratégia propõe a criação de uma arquitetura de referência para sustentação dos serviços de infraestrutura, com foco na plena sustentação dos serviços de TIC para e-Saúde. Pensar uma arquitetura de referência é necessário especialmente por conta da

256 Ibid., p. 65.

necessidade de utilização de instrumentos inovadores para o provimento de serviços de TIC. Os processos de e-Saúde serão dependentes de ferramentas complexas, com clara volatilidade tecnológica, o que demanda atenção especial.

É importante contar com referências e indicações aptas a estabelecer papéis e responsabilidades, capacidades, padrões de qualidade na prestação de serviço, contingência e adaptação entre seus componentes. Aqui se incluem ainda, esforços para ampliar e consolidar o compartilhamento de iniciativas entre os entes federativos, e outros atores públicos e privados, buscando a modernização do parque tecnológico.

A mencionada arquitetura de referência incluiria aspectos como: previsões de contingenciamento e recuperação de desastres; flexibilidade de uso; escalabilidade e modularidade; diversidade tecnológica; sistemas e segurança, com a utilização de certificados digitais, redes virtuais, rastreabilidade de custos, entre outros. E um ponto interessante, seria a possibilidade de revisitar a experiência brasileira de adoção e implantação de modelos de distribuição de recursos de energia elétrica e de telecomunicações.[257]

Se espera por meio desta ação definir uma arquitetura referencial para infraestrutura definida, testada e validada, oferecida como modelo para todos os atores da saúde, com amplo respaldo da legislação, da cultura e da prática de gestão de TI Ademais, por meio de experiências e planos contingenciais, seria possível assegurar uma ampla capacidade de adaptação dos serviços de infraestrutura às novas tecnologias, incorporando serviços novos ou já existentes e resultando em expansão da infraestrutura, com redução de inconsistências e minimização de riscos.[258]

Diante de tantos processos e ferramentas tecnológicos, a próxima estratégia foi acertadamente dedicada à criação de uma certificação em e-Saúde voltada para os operadores do SUS, em razão de diagnóstico preliminar do eixo de recursos humanos que indicou a existência de deficiências na qualificação dos profissionais para manuseio e utilização dos recursos, bem como de carência de profissionais aptos a produzirem recursos para e-Saúde, sobretudo no que tange a geração de dados e informação de qualidade no sistema.

Neste cenário o que se pretende é a implantação de um processo de certificação baseado na formação e atualização profissional em e-Saúde no SUS, orientando e

257 No que se refere a experiência brasileira, é possível destacar a regulamentação da Agência Nacional de Saúde Suplementar (ANS), Agência Nacional de Energia Elétrica (ANEEL) e Agência Nacional de Telecomunicações (ANATEL).

258 BRASIL, op. cit., 2017, p.66.

qualificando profissionais. Uma vez formulado o processo de certificação, com a definição dos perfis de recursos humanos para o e-Saúde, inclusive com a definição de competências, habilidades e atitudes, pretende-se identificar iniciativas que promovam a certificação. [259]

A ideia da certificação abrange também a identificação da disponibilidade, quantidade e distribuição de profissionais de TI no SUS, em termos de perfil; a criação a carreira do profissional de e-Saúde, incluindo cargos, funções e salários; a criação a área de conhecimento da e-Saúde junto aos órgãos de fomento à pesquisa. Além disso, auxiliaria diretamente na adequação da base legal e normativa da e-Saúde, com a articulação com os Conselhos e representação de classe a promoção das boas práticas da e-Saúde e a possibilidade de estabelecer processo de Monitoramento e Avaliação (M&A) das práticas de e-Saúde dos profissionais[260], por exemplo.

Assim, a certificação resultaria primeiramente em uma orientação quanto a carreira do profissional de e-Saúde, com cargos, funções e salários, criada, testada e validada, além da definição de perfis e a manutenção de cadastros de profissionais do SUS. Por outra via, também traria o reconhecimento do e-Saúde como área do conhecimento e fortaleceria a base legal e normativa a ser desenvolvida, consolidando uma cultura de articulação e interlocução com os conselhos e representação de classe para a promoção das boas práticas.

A derradeira ação estratégica apresentada busca promover a facilitação do acesso à informação em saúde para a população, direcionando a implementação de recursos de e-Saúde que facilitem o acesso da população à informação em saúde de qualidade. Seria esta uma forma de otimizar processos e recursos, evitando informações inconsistentes e fragmentadas que frequentemente prejudicam as operações cotidianas, gerando congestionamentos e aumento de custos. Ocorre que embora existam inúmeros recursos de acesso à informação de saúde disponíveis, a forma como são repassadas à população é por vezes é desordenada e problemática.

Para a materialização desta proposta, foi prevista a elaboração de um código de conduta para a publicação de informações em saúde nas mídias digitais; a promoção da articulação entre os diferentes órgãos de governo e da sociedade para facilitação

259 O desenvolvimento da oitava ação estratégica pretende utilizar as experiência e boas práticas acumuladas em projetos e iniciativas como UnaSUS, UAB, proTICs, Programa de Democratização do Acesso e Permanência de Estudantes das Classes Populares (PRODAPE), Escolas Técnicas do SUS, Centros de formação acadêmica - Universidades, Faculdades, Fundações, RUTE (SIGs de Tecnologia), Programas do MS (Telessaúde Brasil Redes, PET, e Provab, entre outros), TIGER/Consórcio Universidades, e RIPSA nos estados.

260 BRASIL, op. cit., 2017, p. 67.

do acesso à informação; a identificação os canais de comunicação (como a web, dispositivos móveis, e outros) com a população; e a adequação a terminologia aos diferentes perfis de consumidores da saúde. [261]

Conforme o documento base, espera-se que desenvolvimento desta ação estratégica resulte ainda na disseminação do e-Saúde de modo que os usuários, profissionais, gestores tenham acesso aos recursos disponíveis para informação em saúde (portais, aplicativos móveis). Tal disseminação, atingiria mídia aberta (TV e grande imprensa, por exemplo) e mídia interna, considerando as instituições públicas e privadas de Saúde, sensibilizando para o seu uso e benefícios;

Dessa forma, as nove ações de caráter multidisciplinar, mencionadas alhures, convergem em um plano inicialmente coerente para viabilizar a visão de e-Saúde no Brasil. O documento deixa expresso que as ações estratégicas propostas deverão ser submetidas à validação das instâncias superiores do MS, do SUS, bem como por outros ministérios, sempre buscando contribuições e ajustes. Contudo, após análise é possível identificar preocupantes lacunas, especialmente no tocante à falta de diretrizes claras e abrangentes sobre a proteção de dados pessoais.

Embora o documento mencione a necessidade de garantir a privacidade e a confidencialidade das informações, não há detalhamento sobre as medidas de segurança que devem ser adotadas para alcançar esses objetivos. Além disso, se carece de uma abordagem clara quanto à questão do consentimento informado dos usuários para o tratamento de seus dados pessoais. Com efeito, não há menção à importância do consentimento, enquanto requisito legal, nem como ele será obtido no contexto do e-Saúde.

Outra lacuna se refere à falta de salvaguardas para garantir o acesso restrito aos dados de saúde. As ações não contemplam de forma específica medidas de controle de acesso, *login* de usuários e restrições de compartilhamento de informações pessoais, o que favorece possíveis violações de privacidade. Tal situação desperta também questionamentos quanto à responsabilidade das instituições de saúde em relação à proteção de dados, visto que não há indicação de medidas técnicas e organizacionais para proteção de dados pessoais.

A Estratégia e-Saúde para o Brasil 2017 foi elaborada antes da entrada em vigor da LGPD, que ocorreu no ano de 2020. Portanto, é compreensível a existência da ausência de uma orientação mais clara quanto às questões que envolvam privacidade e

261 Idem, p. 68.

confidencialidade de dados pessoais, como também já era esperado certo descompasso entre as ações indicadas na Estratégia e as exigências posteriormente apresentadas na LGPD.

Um movimento de adaptação foi igualmente requerido quando da implantação do programa Conecte SUS, designado como ferramenta principal para a materialização das estratégias elaboradas em 2017. O programa foi instituído por meio da Portaria nº 2.979/2019, que estabelece as diretrizes para sua implementação e foi concebido em resposta à necessidade de melhorar a eficiência e a qualidade do atendimento no SUS, bem como promover o compartilhamento seguro de informações de saúde na prática, objetivos que a ser aprofundados no tópico a seguir.

4.3 Programa Conecte SUS

Como meio de concretização da visão proposta para a e-Saúde brasileira foi indicado o programa do governo federal intitulado Conecte SUS[262], composto por um sistema integrador direcionado a fomentar o apoio à informatização e ao intercâmbio de informações entre os estabelecimentos de saúde. Tendo sido disponibilizado por meio de aplicativo aberto ao uso de operadores da saúde e cidadãos em geral, o Conecte SUS segue o mesmo padrão das políticas de privacidade dos demais aplicativos do Ministério da Saúde.

O Conecte SUS nasceu em um contexto no qual o Brasil buscava modernizar e aprimorar a gestão do SUS, visando uma maior eficiência e qualidade no atendimento à população. A criação do Conecte SUS foi influenciada pelo avanço das tecnologias de informação, bem como pelas propostas apresentadas dos planos do Ministério da Saúde, especialmente pelas Estratégias de Saúde Digital para o Brasil 2017.

A estrutura do referido programa utiliza uma série de sistemas e plataformas para viabilizar a integração de informações e o compartilhamento de dados no âmbito do Sistema Único de Saúde. Tal integração, como mencionado anteriormente, tem o objetivo de otimizar processos, melhorar a gestão, a eficiência e a qualidade do atendimento aos pacientes. Dentre os sistemas e plataformas envolvidos no programa encontram-se: Cadastro Nacional de Usuários do SUS (CADSUS); Registro Eletrônico

262 CONECT SUS. Plataforma de saúde para o cidadão, profissionais e gestores de saúde do Sistema Único de Saúde Brasileiro, 2022. Disponível em: https://conectesus.saude.gov.br/home. Acesso em: 22 jan. 2023.

de Saúde (RES); Sistema Nacional de Regulação (SISREG) e o Prontuário Eletrônico do Cidadão;[263]

O CADSUS é um sistema utilizado para cadastrar os usuários do SUS, coletando informações pessoais básicas, como nome, CPF, data de nascimento, entre outras. Ele permite a identificação única de cada cidadão no sistema de saúde e é uma das bases de dados fundamentais para o Conecte SUS. Enquanto o Registro Eletrônico de Saúde é um sistema que tem como objetivo centralizar e organizar as informações de saúde dos pacientes em um prontuário eletrônico, que abrange desde os dados básicos, como histórico de consultas e exames, até informações mais detalhadas, como diagnósticos, prescrições médicas, resultados de exames laboratoriais, entre outros. O RES busca facilitar o acesso e o compartilhamento dessas informações entre os profissionais de saúde.

O SISREG é uma plataforma que auxilia na regulação e no controle do acesso aos serviços de saúde oferecidos pelo SUS. Ele permite o agendamento de consultas, exames e procedimentos, bem como a organização da fila de espera. O SISREG contribui para a otimização da gestão dos recursos de saúde, evitando filas desnecessárias e garantindo um atendimento mais eficiente. E por fim, há que se abrir espaço para o Prontuário Eletrônico do Cidadão.

O Prontuário Eletrônico do Cidadão [264]é uma iniciativa do Conecte SUS que visa reunir e integrar as informações de saúde de cada indivíduo em um único sistema, provendo informação e autonomia para os usuários do SUS. Ele funciona como um repositório centralizado de informações médicas, permitindo o acesso rápido e seguro aos dados do paciente. O prontuário eletrônico permite compartilhamento rápido e supostamente seguro de dados entre os profissionais de saúde, otimizando processos, ao tempo que evita a necessidade de repetir exames e procedimentos, reduzindo custos e melhorando o atendimento.

Por meio da integração destes sistemas é possível uma maior visão mais abrangente e precisa dos pacientes, facilitando a gestão e o acompanhamento de seu histórico

263 O Programa Conecte SUS. Ministério da Saúde.

264 Na rede pública de saúde, se trabalha com o Prontuário Eletrônico do Cidadão (PEC), versão utilizada a partir do Sistema e-SUS Atenção Básica, que é o software médico gratuito para armazenar informações de pacientes. O PEC tem como objetivo favorecer o atendimento, uma vez que mantém os dados relevantes para os médicos reunidos em um só lugar. Entre os benefícios, destacam-se: acesso facilitado aos dados do paciente e seu histórico de saúde; otimização de recursos e redução de custos (menos papel, por exemplo); automação de processos e facilidade para troca de informações entre médicos. Assim, administrações municipais e estaduais de saúde podem contar com esse sistema para favorecer o amparo à população como um todo. BRASIL. O que é Prontuário Eletrônico do Cidadão? **Ministério da saúde**, Brasília, 2017. Disponível em: https://aps.saude.gov.br/noticia/2300. Acesso em: 12 jan. 2023.

de saúde. Mas além desses sistemas, o programa Conecte SUS também utiliza tecnologias e plataformas de telemedicina e telessaúde para permitir o atendimento à distância. Essas soluções envolvem o uso de videochamadas, troca de mensagens e compartilhamento de imagens e exames, proporcionando acesso a serviços médicos em áreas remotas e melhorando a acessibilidade ao atendimento de saúde.

O Conecte SUS iniciou a difusão de uma nova cultura, na qual a tecnologia viabiliza o acesso a serviços médicos à distância. Por meio das TICs, o sistema conecta pacientes e profissionais de saúde que estejam em localidades distintas – um recurso que ganha grande relevância em um país de dimensões continentais como o Brasil, onde muitas regiões enfrentam desafios de acesso à saúde.

A telemedicina, sem dúvidas, contribui para a democratização do atendimento médico e o aumento da eficiência do sistema de saúde, porém ainda desperta questionamentos de diversas ordens, incluindo-se aqui as questões de segurança e privacidade de dados sensíveis. Embora a segurança da informação e privacidade de dados configurem um dos pilares do Programa Conecte SUS, a missão de assegurar a proteção adequada dos dados de saúde dos cidadãos não está concluída, configurando um dos principais desafios para entes, gestores, profissionais e usuários do sistema.

Em busca de segurança, a interface do Conecte SUS apresenta uma série de regras, medidas técnicas, organizacionais e legais com o objetivo de preservar a confidencialidade das informações que serão armazenadas em seu sistema e ainda um documento informativo ao titular dos dados de saúde, no qual se esclarecem importantes aspectos relacionados ao acesso às informações e até mesmo a possibilidade da recusa do compartilhamento dos dados em saúde.

Pela análise do programa é possível identificar a aplicação de criptografia, que consiste na codificação das informações de forma que somente o destinatário autorizado possa decifrá-las. A criptografia é utilizada durante a transmissão de dados entre os sistemas e plataformas do Conecte SUS, como meio de garantir a confidencialidade das informações. A referida plataforma também exerce um controle de acesso entre seus usuários. O controle de acesso visa garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais[265]. Ele envolve a implementação de autenticação, como senhas fortes, e a definição de níveis de permissão de acordo com as responsabilidades e funções dos usuários. Além disso, cumpre mencionar que é possível monitorar e

265 CONECT SUS APLICATIVO. CONECT SUS, 2022.

auditar as atividades de acesso aos dados para identificar qualquer uso indevido ou não autorizado.

A anonimização e a pseudonimização também estão presentes nas ações do referido programa, de modo a contribuir para a proteção da privacidade dos dados. Como já detalhado, consistem em técnicas que visam a minimizar o risco de identificação dos indivíduos por meio dos dados pessoais: a anonimização envolve a remoção irreversível de informações que possam identificar uma pessoa, enquanto a pseudonimização substitui elementos identificáveis por identificadores fictícios, tornando mais difícil a associação direta com um indivíduo real.

Há ainda a previsão de backup e recuperação de dados, com a indicação de um plano de recuperação de dados em caso de incidentes, como falhas de sistema, ataques cibernéticos ou desastres naturais, garantindo a continuidade dos serviços e a recuperação dos dados perdidos. Para um sistema dessa magnitude é essencial implementar políticas de backup regular de dados. Os backups do Conecte SUS devem ser armazenados em locais seguros e separados do ambiente de produção.

Importante destacar que nos planejamentos envolvendo o Conecte SUS, assim como nas Estratégias de Saúde Digital para o Brasil 2017, o treinamento e conscientização dos profissionais envolvidos foi indicado como ponto essencial para a proteção dos dados pessoais. Treinamentos devem ser realizados regularmente para que os usuários estejam cientes das melhores práticas de segurança da informação, incluindo a importância do tratamento adequado dos dados pessoais e a prevenção de ameaças cibernéticas, como phishing e malware[266].

Por estes exemplos, resta clara a preocupação do programa Conecte SUS em assegurar segurança e privacidade para seus usuários, especialmente em face da natureza dos dados e dos riscos decorrentes de um possível vazamento. Entretanto, a utilização prática do sistema já revelou inquietantes falhas neste aspecto, tal como se encontra visível nas informações disponibilizadas diretamente ao usuário.

Por meio da "Nota Informativa ao Titular de Dados de Saúde"[267] o usuário é informado que seus dados de saúde estarão disponíveis por trinta minutos ao

266 O *phishing* é um tipo de técnica de roubo. A ideia aqui é fazer uso de um e-mail, site ou anúncio para tentar se passar por alguém ou alguma instituição que você conhece ou confia. O *malware* é um termo que serve para indicar "*softwares* maliciosos" que tem a capacidade de infectar um dispositivo eletrônico, como smartphones e tablets. Entre esses programas que podem afetar um aparelho, está o vírus, bastante conhecido. Eles conseguem se espalhar facilmente por uma rede e, assim, prejudicar o espaço virtual. Ou seja, a partir de um *phishing*, é possível fazer com que esse software entre no aparelho e traga algum tipo de prejuízo.

267 CONECT SUS APLICATIVO. Nota informativa ao titular de dados de saúde. 2022. Disponível em: https://conectesus-paciente.saude.gov.br/menu/termo-uso. Acesso em: 17 maio 2022.

profissional responsável pelo atendimento, devidamente habilitado a acessar os dados da Rede Nacional de Dados em Saúde, que esteja prestando atendimento a você ou à pessoa que você seja responsável legal. Segundo informa o documento, o profissional habilitado terá acesso a informações de caráter administrativo (por exemplo: data e horários de atendimento, entrada e saída do estabelecimento), informações relativas a medicamentos distribuídos, internações hospitalares, atendimentos ambulatoriais, de vacinação e resultados de exames, considerando dados coletados a partir de janeiro de 2018.

Em nenhum momento, porém, o texto explicita por quanto tempo as informações serão mantidas no sistema e quais as formas de controle para assegurar que apenas o profissional em atendimento terá acesso aos dados de saúde daquele indivíduo. Nas disposições contidas no Termos de Uso e Políticas de Privacidade, diversos tópicos são apresentados aos usuários, tais como a obrigação da observância às normas vigentes e destinação dos serviços apenas para finalidades lícitas nos termos da legislação brasileira; o esclarecimento pela responsabilidade do conteúdo e notas sobre propriedade intelectual[268].

No tópico "Leis, regulamentos, direitos e deveres" é explicitado ao usuário a observação das normas de proteção de dados, o cumprimento de todas as leis e regulamentos aplicáveis, os quais podem ser modificados de tempos em tempos. E mais à frente, surge referência expressa à questão do respeito à privacidade e adequação à LGPD que parecem contrastar com a garantia de sigilo e anonimato ofertada em caráter parcial. Conforme se infere do texto, a garantia de sigilo e anonimato das informações produzidas pelo utilizador do sistema, será relativizada não apenas nos casos de exigência legal, ou para tratar de questões de descumprimento, mas também mediante a possibilidade de utilização interna de informações visando uma contribuição que será vinculada ao apelido do usuário, em substituição aos dados pessoais dos utilizadores.

Ambos os textos silenciam sobre meios e práticas para a efetivação do sigilo e confidencialidade, enfraquecendo a promessa da proteção dos dados sensíveis feita aos usuários do sistema. A fragilidade quanto à questão da privacidade não é o único desafio enfrentado atualmente pelo programa Conecte SUS. Existem outras limitações que têm comprometido o êxito da proposta. É o caso da ausência de infraestrutura tecnológica adequada.

268 CONECT SUS APLICATIVO. Termos de Uso de Aplicativo e Políticas de Privacidade. 2022. Disponível em: https://conectesus-paciente.saude.gov.br/menu/termo-uso. Acesso em: 17 mai. 2022.

A existência de uma infraestrutura tecnológica é essencial para o funcionamento eficiente do Conecte SUS. Neste ponto se inclui a disponibilidade de conexões de internet estáveis e de qualidade em todas as regiões do país, bem como a atualização e a manutenção dos sistemas e equipamentos utilizados. Sem a infraestrutura necessária, o acesso e o uso da plataforma do programa ficam comprometidos.

Outro ponto de atenção é a capacitação dos profissionais de saúde. A implementação do Conecte SUS requer profissionais capacitados para utilizar as ferramentas e os sistemas de forma eficaz e segura. A falta de treinamento adequado pode conduzir a erros no uso das plataformas, comprometendo a qualidade e a segurança dos dados. Deste modo, urge investir em programas de capacitação e conscientização para garantir a adesão dos profissionais ao programa e seu correto manuseio.

Também merece atenção a questão da integração dos sistemas e a interoperabilidade das plataformas, que nem sempre tem sido possível. A diversidade consiste na quantidade de sistemas e tecnologias utilizados em diferentes regiões e instituições de saúde. Sem a integração efetiva dos sistemas, o compartilhamento adequado de informações entre os profissionais de saúde torna-se inviável, prejudicando os principais objetivos do programa.

Neste ponto, também é válido indicar como desafio a aceitação e confiança dos usuários e profissionais de saúde. Por se tratar de um sistema inovador no Brasil, é necessário promover a conscientização sobre os benefícios do programa, bem como assegurar a privacidade e a segurança dos dados pessoais. A transparência no tratamento dos dados e a participação ativa dos usuários na definição das políticas relacionadas à proteção de dados são fatores-chave para a construção da confiança e consequente adesão ao sistema.

Diante da necessidade de implementação de soluções tecnológicas para aperfeiçoar a operacionalização do referido sistema, bem como para corrigir falhas e limitações previamente identificadas, de forma contínua, foi aprovado na 34ª Reunião Ordinária do Comitê Gestor da Estratégia de Saúde Digital, no ano de 2019, e posteriormente pactuado por Ad Referendum em 30 de março de 2020, o Plano de Ação, Monitoramento e Avaliação destinado a identificar, priorizar e integrar, de forma coordenada, programas, projetos e ações de saúde de forma a implantar as iniciativas que compõem o sistema Conecte SUS.

Para o mencionado fluxo de atualizações o programa conta com o auxílio do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). Este configura mais

documento estratégico elaborado pelo governo brasileiro que apresenta diretrizes, metas e ações relacionadas à área de tecnologia da informação e comunicação nos órgãos e entidades da administração pública federal.

4.4 Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)

O PDTIC foi inicialmente instituído pela Instrução Normativa nº 4/2010 da Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão[269]. Dentre seus objetivos se encontrava o estabelecimento das diretrizes gerais para elaboração, aprovação, implementação e acompanhamento dos planos diretores de tecnologia da informação e comunicação no âmbito do governo federal.

Por seu conteúdo, o plano é atualizado periodicamente, ganhando uma nova versão a cada triênio, de modo a acompanhar a evolução tecnológica e as necessidades dos órgãos governamentais quanto as ações envolvendo as tecnologias da comunicação e da informação. Trata-se de um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de TI, que tem sido utilizado especialmente com vistas a orientar o atendimento de necessidades tecnológicas e de informação do Ministério da Saúde, no âmbito do SUS.[270]

A primeira versão do PDTIC analisada nesta pesquisa, continha planejamento para os anos de 2019 a 2021, e posteriormente foram elaboradas diversas atualizações. O principal objetivo indicado na versão PDTIC21 foi apresentar a estratégia de TIC e o conjunto de resultados esperados durante o período de 2019 a 2021 do DATASUS do Ministério da Saúde. Havia então a previsão da realização de diagnósticos,

269 Conforme definição encontrada nas páginas de informação do governo, o Plano Diretor de Tecnologia da Informação – PDTIC é um instrumento de diagnóstico, planejamento e gestão de recursos e processos de Tecnologia da Informação. Tem por objetivo determinar as prioridades de investimento e alocação de recursos nos diversos projetos e ações de TI. O documento permite o alinhamento entre as atividades de TI e o negócio da organização, a otimização dos recursos disponíveis, o acompanhamento do estágio de desenvolvimento dos projetos, solução de conflitos relativos a recursos e monitoramento dos níveis de serviço de TI e suas melhorias. INTI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC. Brasília: INTI, 2017. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/plano-diretor-de-tecnologia-da-informacao-e-comunicacao-pdtic. Acesso em: 12 jul. 2023.

270 Em sua introdução, o PDTIC é apresentado como um planejamento dinâmico para viabilizar a entrega de serviços de tecnologia e soluções digitais seguras ao SUS e aos cidadãos. Apresentação do PDTIC 2022-2024. BRASIL. **Plano Diretor de Tecnologia da Informação e Comunicação** – 2022/2024. Brasília – DF: Ministério da Saúde. 2022. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2022/06/PD-TIC-2022a2024-25mai2022-Final-revisado2.pdf. Acesso em: 30 maio 2022.

planejamentos e ações de gestão dos recursos e processos de TIC, em atenção às necessidades tecnológicas das Unidades Finalísticas do Ministério da Saúde.

O texto do PDTIC21 trabalha enquanto principais elementos metas, diretrizes e ações estratégicas. Com a definição de metas específicas a serem alcançadas em um determinado período, resulta no estabelecimento de prazos palpáveis a serem trabalhados nas ações práticas. As metas em questão podem estar relacionadas à implantação de sistemas de informação, ao aumento da cobertura de serviços digitais ou à melhoria da segurança da informação no SUS. As metas devem ser mensuráveis e contribuir para o cumprimento dos objetivos estabelecidos.

As diretrizes traçadas ao longo do texto têm o papel de nortear a implementação das ações estratégicas e a tomada de decisões relacionadas à tecnologia da informação no SUS. Tais diretrizes transitam entre temas como a interoperabilidade dos sistemas, a segurança da informação, a privacidade dos dados de saúde e a participação dos usuários no processo de desenvolvimento tecnológico.

Por fim, o PDTIC21 descreve as ações estratégicas que serão adotadas para alcançar os objetivos e metas estabelecidos. Essas ações incluem desde a implantação de sistemas de informação, a capacitação de profissionais de saúde em tecnologia da informação, a criação de protocolos de segurança da informação, até a promoção de inovações tecnológica no SUS.

A versão mais recente do referido Plano Diretor foi proposta em 2022, estendendo-se até 2024. Conforme, o recorte metodológico desta pesquisa, serão exploradas neste texto de forma mais profunda as propostas mais recentes, com foco especial no plano 2022 a 2024. O PDTIC trouxe como um dos princípios orientadores das atividades de governança digital, a segurança e privacidade e propôs expressamente a elaboração do marco legal de e-Saúde no país, sempre em conformidade com as políticas públicas de saúde e com a LGPD.[271]

A análise do plano 2022-2024 revela uma importante contribuição para a elaboração de um planejamento estratégico para o SUS frente às inovações de tecnologia da informação e comunicação, bem como aos objetivos e metas da administração pública federal. Trata-se da indicação de instrumentos de planejamento do Ministério da Saúde, com diretivas e objetivos estratégicos, visando a otimizar processos e permitir uma melhor utilização dos recursos disponíveis e a definição de prioridades para

271 Idem.

investimentos em TI[272]. Além de ampliar a eficiência, o PDTIC busca promover a modernização dos sistemas de informação e comunicação utilizados pelo governo como um todo, com o objetivo de tornar os serviços públicos mais eficientes, ágeis e acessíveis aos cidadãos.

Como meio de concretizar esses objetivos o plano apresenta um capítulo intitulado "Inventário de Necessidades de TIC Priorizado" que inclui o inventário das secretarias e demais unidades do MS, inventário das superintendências e hospitais federais, inventário de ativos de TIC e ainda descritivo sintético do inventário de ativos de TIC. Na sequência, apresenta uma série de planos técnicos, que inclui um "Plano de Metas e Ações", "Plano de Gestão de Pessoas", "Plano Orçamentário" e ainda um "Plano de Gestão de Riscos" no qual se detalham protocolos e procedimentos gerenciais.

O plano de gestão de riscos aborda de forma direta as questões de segurança da informação. Em seu conteúdo são indicadas diretrizes para a segurança da informação nos órgãos governamentais, visando à proteção dos dados pessoais e sensíveis dos cidadãos usuários do sistema de saúde. Neste capítulo há a definição de políticas, normas e procedimentos de segurança, bem como a indicação da implementação de mecanismos de controle e monitoramento.[273]

Conforme aponta o escrito, os serviços públicos digitais devem propiciar disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações, além de proteger o sigilo e a privacidade pessoais dos cidadãos na forma da legislação[274]. Dentre as situações de segurança, o documento destaca o manuseio dos prontuários eletrônicos[275]. Nos Estados Unidos e na Europa, onde há anos existe o prontuário eletrônico de pacientes, a discussão está em um nível bastante diferente. Cada médico consegue acessar, automaticamente, os dados completos dos pacientes, mesmo aqueles fornecidos por outros médicos, em consultas e tratamentos anteriores.

Contudo, isso apenas é realizado com o consentimento do paciente. Existem políticas públicas em discussão há alguns anos sobre a matéria. A principal se refere ao estímulo aos pacientes de publicizarem seus prontuários eletrônicos para a pesquisa científica. Com o cruzamento dos dados de saúde de milhares de pessoas, seria mais fácil prever novas doenças e mesmo identificar possíveis tratamentos mais efetivos.

272 Informações mais detalhadas no quadro apresentado nos anexos deste texto.

273 BRASIL, op. cit., 2022, p. 103.

274 Ibid., p. 81.

275 O prontuário eletrônico foi indicado pelo Plano Diretor de Tecnologia da Informação e Comunicação – 2022/2024, o em seus Descritivos de Prioridades do Inventário de Necessidades de Tic. Assim como a Estratégia de Saúde Digital 2028, ESD28, também o incluiu como uma das prioridades para o Plano de Ação – PPA. Ibid.

O Sistema Nacional de Saúde no Reino Unido - NHS[276], por exemplo, desde 25 de maio de 2018, permite que os pacientes autorizem a divulgação de seus prontuários eletrônicos, de forma anonimizada, para finalidades além do seu próprio tratamento. Interessante notar que se presume a aceitação, ou seja, aqueles contrários devem se manifestar e desautorizar expressamente o compartilhamento de informações.

No Brasil, em momento mais recente, foi publicada por meio da Portaria GM/MS nº 3.632, de 21 de dezembro de 2020, a versão mais recente do documento Estratégia de Saúde Digital para o Brasil 2020-2028 [277]que, com base nos avanços obtidos pelos projetos que compõem o Programa Conecte SUS, ratifica a proposta original, enquanto procura sistematizar e consolidar as ações realizadas ao longo da última década, acrescentando uma visão futura, segundo a qual a Rede Nacional de Dados em Saúde (RNDS) estará estabelecida e reconhecida como a plataforma digital de informação e inovação e serviços de saúde, apresentando benefício em diversas esferas.

Dentre as principais ações do PDTIC24 já implantadas para o SUS, além dos prontuários eletrônicos, compartilhados ou não, é possível mencionar a integração dos sistemas de informação, a telemedicina e os aplicativos e sistemas de agendamento. A integração dos sistemas de informação utilizados nos diferentes níveis de atendimento do SUS busca proporcionar uma visão abrangente e integrada dos dados de saúde dos pacientes. Isso facilita o compartilhamento de informações entre os profissionais de saúde e contribui para uma melhor coordenação do cuidado.

A implementação da telemedicina no SUS permite a realização de consultas médicas à distância, por meio de videoconferência ou outras tecnologias. Essa prática possibilita o atendimento de pacientes em regiões remotas, agiliza a triagem de casos e oferece maior comodidade aos usuários. Por fim, o desenvolvimento de aplicativos e sistemas de agendamento online auxilia na marcação de consultas, exames e

276 O Sistema Nacional de Saúde no Reino Unido, conhecido como NHS (National Health Service), é o sistema público de saúde do país. Ele foi estabelecido em 1948 e tem como objetivo fornecer cuidados de saúde gratuitos e acessíveis a todos os residentes do Reino Unido, independentemente de sua renda. Em relação ao Sistema Único de Saúde (SUS) no Brasil, algumas semelhanças e diferenças podem ser destacadas em relação ao NHS. Dentre as principais semelhanças entre os sistemas se encontram as características: universalidade, visto que tanto o NHS quanto o SUS têm o objetivo de fornecer cuidados de saúde universais, ou seja, disponíveis para todos os cidadãos; financiamento público, já que ambos os sistemas são financiados principalmente por impostos e contribuições sociais, e cobertura ampla: tanto o NHS quanto o SUS oferecem uma ampla gama de serviços de saúde, desde cuidados primários até tratamentos especializados. Em termos de diferenças, as mais marcantes são a estrutura de governança, o modelo de pagamento e as desigualdades regionais. NHS. We're here for you. 2023. Disponível em: https://www.nhs.uk/. Acesso em: 17 jun. 2023.

277 Documento que apresenta a Estratégia de Saúde Digital para o Brasil com uma visão de oito anos, isto é, até o final de 2028. Ver em: BRASIL. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília: Ministério da Saúde, 2020.

procedimentos, reduzindo o tempo de espera e proporcionando uma experiência mais ágil e conveniente para os usuários do SUS.

Os quatro exemplos trabalhados são tratados pelo Ministério da Saúde como realizações bem-sucedidas contidas nas políticas de Saúde, tendo resultado na melhoria na acessibilidade e no aumento da eficiência operacional. Todavia, pela análise do PDTIC24, percebe-se mais uma vez as lacunas quanto às questões de segurança e privacidade. Entre as ações e diretrizes contidas nesse documento, poucas linhas são dedicadas à palpitante questão da proteção de dados por operadores e usuários dos sistemas de saúde. Percebe-se que as propostas nesta seara são desenhadas em uma abordagem quase generalista, sem ainda enfatizar peculiaridades verificadas no contexto nacional.

Em fato, as consequências e limites do uso de tecnologias aplicadas à saúde ainda mantêm uma série de incógnitas, tanto no que se refere aos inúmeros benefícios e avanços que se projetam para o futuro quanto aos perigos decorrentes do vazamento de informações. Nas disposições sobre a legislação e a regulação para a saúde digital apresentada, merece destaque positivo a indicação expressa da necessidade de uma norma apta a prover segurança jurídica a todos os envolvidos, garantindo direitos essenciais como os de confidencialidade e privacidade de dados, corroborando a orientação do PDTIC de 2019 e a previsão de definição e adoção de normas e padrões para a representação, armazenamento, troca e utilização de dados de saúde, incluindo as terminologias clínicas e os aspectos legais referentes ao uso da informação, como a LGPD.

Segundo o referido texto, as iniciativas de saúde digital devem se pautar pela Lei Geral de Proteção de Dados e como caminho para essa adequação são indicadas as seguintes atividades: identificação dos pontos críticos de alinhamento à LGPD para a expansão da Rede Nacional de Dados em Saúde (RNDS); identificação de modelos de compartilhamento de dados de saúde alinhados à LGPD; proposição de modelos robustos de consentimento esclarecido e informado de fácil compreensão, implementação e adesão pelo paciente; proposição de modelos de autenticação, segurança, sigilo e privacidade.

Por meio dessas atividades apontadas como prioritárias pretende-se gerar segurança jurídica, enquanto consequência da privacidade e confidencialidade dos dados, o que sem dúvidas beneficia não apenas usuários, profissionais, gestores e organizações, mas também promove o fortalecimento da credibilidade da Saúde Digital, permitindo maior aceitação e alcance do sistema, destacando seus benefícios e minorando seus

riscos. No que se refere à regulação de ambientes de inovação e interconectividade, foi pontuado que além do cumprimento dos ditames da LGPD, as regras de participação, troca de informações, financiamento e utilização dos resultados da colaboração devem ser claramente estabelecidas e alinhadas.

A implementação de uma normativa específica viabilizaria que as colaborações envolvendo dados de saúde se realizem de maneira segura e transparente para cidadãos, órgãos de controle e sociedade civil em geral. Destaca ainda, a pertinência da definição de critérios éticos, de propósito de utilização e de responsabilidade legal quanto aos dados coletados. Para esta proposta, o plano governamental recomenda como primeiro passo identificar e atrair os atores relevantes; estabelecer o arcabouço legal e organizacional para a regulação da colaboração; implementar, avaliar e aprimorar continuamente os processos de regulação.

Ocorre que, em razão do dinamismo ínsito à tecnologia, é preciso trabalhar constantemente com releitura e atualização de planejamentos. Nesse contexto, o Brasil, como os demais países do mundo, enfrenta o desafio de identificar vulnerabilidades, buscar inovações, corrigir processos, capacitar profissionais e instituições, antes que a próxima grande mudança chegue.

4.5 Estratégia de saúde digital para o Brasil 2020-2028

A partir da análise dos documentos anteriormente mencionados, foi possível concluir que as políticas públicas voltadas para a Saúde Digital no Brasil seguem uma estrutura de médio e longo prazos e possuem o desafio apresentar estratégias, ferramentas e ações que consigam aliar positivamente o uso das tecnologias e a saúde. Tal modelo não impediu que fosse identificada a necessidade de correção, bem como de ajustes e de atualização nos planos propostos.

Ainda no ano de 2019, o governo brasileiro iniciou um processo de atualização das Estratégias de Saúde Digital, buscando melhorar a utilização da tecnologia da informação no setor de saúde. Essa iniciativa foi impulsionada pela necessidade de acompanhar os avanços tecnológicos e garantir a proteção adequada dos dados pessoais dos cidadãos, conforme LGPD, que entrou em vigor em setembro de 2020.

Nesta busca, foi instituído o Departamento de Saúde Digital como parte da estrutura administrativa do Ministério da Saúde, com a atribuição de desenvolver as questões relacionadas à Política Nacional de Saúde Digital e Telessaúde SUS. Em

sequência, foi criado o Comitê Gestor de Saúde Digital (CGSD),[278] em substituição ao anterior Comitê Gestor da Estratégia de e-Saúde, com a missão de coordenar, orientar e monitorar a implementação das ações relacionadas à saúde digital no Brasil. Em que pese a importância do aludido comitê, a ausência de previsão de participação popular em sua composição gerou críticas arrazoadas, em razão da perda da oportunidade de obtenção de feedbacks que poderiam ter sido obtidos a partir da experiência prática e da visão direta de quem utiliza os sistemas diariamente.

A instituição do Comitê Gestor da Estratégia de Saúde Digital desempenhou um papel importante ao trazer menção a preceitos da OMS, bem como acolheu a nomenclatura atualizada, determinando a substituição do termo "e-saúde" por "saúde digital" nos documentos oficiais em que haja essa referência. Conforme orientação da OMS, o termo Saúde Digital deve ser compreendido como o uso de tecnologias digitais, móveis e sem-fio como meio para atingir os Objetivos de Desenvolvimento Sustentável - ODS em Saúde e a Cobertura Universal da Saúde[279].

Nessa perspectiva, diante da necessidade de sistematizar e consolidar os esforços realizados quanto à implantação da visão de Saúde Digital para o Brasil, foi apresentada, em 2020, a Estratégia de Saúde Digital para o Brasil 2020-2028 - EDS28, que compreende ações voltadas para a área no período de oito anos. O referido documento se apoia em seus antecessores, referenciando especialmente a PNIIS, revisada em 2020, além da Estratégia de e-Saúde Digital para o Brasil 2017, e do Plano de Ação, Monitoramento e Avaliação de Saúde Digital para o Brasil, aprovado em 2019 e publicado em 2020.[280]

O objetivo desta nova versão é nortear e alinhar as diversas atividades e projetos públicos e privados, potencializando o poder de transformação da saúde digital no Brasil. A proposta é feita com ênfase no usuário final dos processos e serviços de saúde,

278 A Resolução CIT nº 05, de 25 de agosto de 2016, instituiu o Comitê Gestor da Estratégia e-Saúde e definiu sua estrutura. Em 2019, por meio da Resolução CIT nº 46, de 26 de agosto de 2019, e com o objetivo de fortalecer o nível estratégico da Estratégia de Saúde Digital (ESD) para o Brasil, o comitê foi redefinido como Comitê Gestor da Estratégia de Saúde Digital, em que foram estabelecidas a sua composição, as suas competências e as suas unidades operacionais na estrutura do Ministério da Saúde (MS), em substituição ao Comitê Gestor da Estratégia de e-Saúde no Brasil. BRASIL. **O Comitê Gestor de Saúde Digital – CGSD**. Brasília: Ministério da Saúde, 2023. Disponível em: https://www.gov.br/saude/pt-br/composicao/seidigi/saude-digital/Comite-Gestor-de-Saude-Digital/Comite-Gestor-de-Saude-Digital. Acesso em: 3 jul. 2023.

279 O termo Saúde Digital vem sendo usado em substituição a *eHealth, mHealth* e abrange as ações de telemedicina, telessaúde e áreas clássicas de informática em saúde, como gestão hospitalar e prontuário eletrônico. OMS - ORGANIZAÇÃO MUNDIAL DA SAÚDE. Global strategy on digital health 2020-2025. Genebra: OMS; 2021.

280 ESD28 se traduz em um documento formal aprovado em todas as instâncias do SUS, incluindo a Comissão Intergestores Tripartite (CIT). A ESD28 tem como objetivo implementar as diretrizes definidas na PNIIS, a Política Nacional de Informação e Informática em Saúde.

conferindo a ideia de protagonismo ao cidadão. Porém, a ideia de um engajamento individual ou coletivo, perde força mediante a ausência da participação popular na construção da estratégia. Há uma nítida carência de informação das decisões, diretrizes e ações práticas das iniciativas pela população brasileira, que contrasta com a visão de usuários engajados. Sem conhecimento tem-se um usuário passivo, conduzido por outras pessoas a um comportamento determinado[281]. O que coloca em xeque o papel do usuário descrito nos eixos de ação do documento.

A ESD28 foi organizada em três grandes eixos de ação, que também orientam o Plano de Ação de Saúde Digital[282]. O primeiro eixo se dedica às ações do Ministério da Saúde para o SUS, reconhece o Conecte SUS e suas iniciativas como ações essenciais para que a Visão de Saúde Digital seja alcançada; O segundo eixo trata da definição de diretrizes para colaboração, ao tempo em que indica a necessidade de expansão e consolidação da governança e dos recursos organizacionais que sustentarão a ESD28. Por sua vez, o terceiro prevê orientações para a implantação do espaço de colaboração concebido como um espaço conceitual, virtual, distribuído, lógico e físico que viabilize a colaboração entre todos os atores em Saúde Digital, com claras definições de expectativas, papéis e responsabilidades.

No que se refere ao tratamento de dados sensíveis, a ESD28 reafirma de forma atualizada o conteúdo da ES17, e indica que até 2028 a RNDS[283] deverá ser estabelecida como a plataforma digital de informação e serviços de saúde para todo o Brasil, otimizando todo o sistema de saúde. Diante de uma proposta desta proporção, já foram iniciados esforços tanto do Ministério da Saúde, como de gestores públicos e atores do setor privado, quanto a consolidação de dados de saúde na RNDS. A título de exemplo, deste trabalho é possível mencionar os dados referentes a resultados de

281 Lupton, D. The commodification of patient opinion: the digital patient experience economy in the age of big data. Sociology of Health & Illness, [*S.l.*], v. 36, n. 6, p. 856-869, 2014, p.856. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1467-9566.12109. Acesso em: 13 abr. 2023.

282 Para a implementação da Visão de Saúde Digital, foi elaborado um Plano de Ação, associado a etapas evolutivas, para que a mesma seja concretizada. Este Plano é composto por um conjunto de atividades, assim como os recursos necessários para o seu desenvolvimento.

283 A RNDS, uma plataforma digital de inovação, informação e serviços de saúde para todo o Brasil, instituída pela Portaria GM/MS Nº 1.434, de 28 de maio de 2020, tem como objetivo [...] promover a troca de informações entre os pontos da Rede de Atenção à Saúde (RAS), permitindo a transição e continuidade do cuidado nos setores público e privado. BRASIL. Portaria nº 1.434, de 28 de maio de 2020. Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. Diário Oficial da União, Publicado em: 29/05/2020, ed. 102, seção: 1, p. 231, Brasília: Ministério da Saúde/Gabinete do Ministro, 2020.

exame de COVID-19, aplicações de vacina, solicitação de medicamentos no Programa Farmácia Popular, registros hospitalares como o sumário de alta[284].

Originalmente, dados dessa natureza ficavam sob a responsabilidade integral dos municípios e estados que deveriam operacionalizar relatórios e realizar seus envios ao Datasus. Com as indicações mais recentes, essas informações passam a ser diretamente incorporadas à RNDS. A proposta de incorporação e consolidação envolve a coleta de informações de saúde de diferentes fontes, como hospitais, clínicas, laboratórios e postos de saúde, e a integração desses dados em um sistema único.

Figura 4 – Representação esquemática da RNDS como plataforma nacional de inovação, informação e serviços digitais em saúde



Fonte: Brasil, 2020, p.22.

Nesta senda, o objetivo primário da RNDS é fornecer uma visão abrangente e integrada dos dados de saúde de cada cidadão, permitindo um melhor monitoramento

284 Os dados do "vacinômetro" são atualizados a cada duas horas e estão disponíveis em: BRASIL. Vacinômetro.Conselho Nacional de Saúde, Brasília: Ministério da Saúde, 2023. Dsponível em: https://conselho.saude.gov.br/vacinometro. Acesso em: 15 ago. 2023.

da saúde da população em nível nacional. Isso significa que as informações sobre consultas médicas, exames, medicamentos prescritos e outros aspectos relevantes da saúde de um indivíduo podem ser acessadas de forma mais rápida e eficiente. Contudo, emerge a preocupação quanto a segurança desses dados e à privacidade de seus usuários. Embora sob o amparo do texto da LGPD, a ESD28, em muitos momentos silencia sobre a questão da segurança dos dados.

O compartilhamento amplo de dados de saúde, além dos diversos riscos de violação de privacidade e fugas de informações pessoais, poderia resultar no uso inadequado dos dados gerando benefícios indevidos para agentes privados. Os problemas se estendem desde o direcionamento em contratações de serviços, abordagens invasivas e possíveis práticas abusivas e/ou discriminatórias de empresas, como exclusão de cobertura de seguro ou plano de saúde para pessoas com certas condições médicas, ou a distribuição de produtos e serviços questionáveis com base nas informações coletadas.

No conteúdo do documento, a este momento considerado como norteador mais completo e atualizado para a saúde digital no Brasil, prevalecem outras prioridades. O caminho traçado pelos eixos coloca o SUS e o Ministério da Saúde como lideranças naturais e essenciais para o desenvolvimento das estratégias e como já mencionado, não abre o devido espaço para a participação da sociedade e dos setores associados a saúde digital, como centros de pesquisa e ensino, órgãos de fomento à pesquisa e desenvolvimento científico, fornecedores de soluções, outros ministérios, organizações de saúde públicas e privadas, assim como sociedades técnicas e científicas, entre tantos outros[285].

No que se refere a inovações, merecem destaque os eixos de ação 2 e 3 da ESD28. Em conjunto, os mencionados eixos apresentam a proposta de implantação de um Espaço de Colaboração com o objetivo de acolher e motivar todos os atores da Saúde Digital, resultando na produção de conhecimento, serviços e produtos inovadores que venham a beneficiar toda a RNDS. Embora o terceiro eixo apresente definições de expectativas, papeis e responsabilidades, é válido ressaltar que para que o Espaço de Colaboração cumpra seu papel, é essencial a criação de um arcabouço organizacional que detalhe objetivos, legislação e critérios éticos, de modo a orientar suas práticas. Outro ponto importante é estabelecer como os resultados da colaboração deverão ser utilizados.

285 MOURA JÚNIOR, L. A. A Estratégia de Saúde Digital para o Brasil 2020 - 2028. Journal of Health Informatics, [*S.l.*], v. 13, n. 1, 2021. Disponível em: https://docs.bvsalud.org/biblioref/2022/03/1361371/editorial.pdf. Acesso em: 14 jun 2023.

Para que o Espaço de Colaboração, de fato viabilize a cooperação entre atores para o desenvolvimento da Estratégia de Saúde Digital e colabore com a RNDS, de modo a assegurar que esta atinja a abrangência necessária e seja considerada ampla, segura, confiável e positiva para seus envolvidos, é necessário um executor. Conforme já mencionado, a missão de liderança e execução direta da ESD28 coube ao Ministério da Saúde, conforme já mencionado. Mediante o rápido abastecimento de dados da RNDS e a relevância das informações ali contidas, disponibilizadas em sistemas em nuvem pública, com tecnologia *Blockchain*[286], é necessário um posicionamento claro quanto as questões de tratamento, manuseio e armazenamento destes dados. Contudo, as referidas questões ainda não foram devidamente enfrentadas pelas políticas públicas de saúde digital brasileiras.

Destarte, a despeito dos esforços do governo brasileiro para a implantação da saúde digital, mediante a integração das informações de todos os setores, sejam originárias da esfera pública ou privada, e a construção de um arcabouço organizacional, legal, regulatório e de governança que possibilite o desenvolvimento adequado de serviços e procedimentos da área, o aprofundamento das questões sobre privacidade parece ter ficado em um segundo plano. É possível que referida lacuna tenha sido intencional, em compasso de espera pela avaliação das consequências práticas da implementação recente de certos mecanismos, enquanto as situações imediatas permanecem sendo discutidas à luz da visão geral apresentada pela LGPD.

4.6 Avanços e retrocessos verificados na saúde digital de 2020 - 2022 durante o período pandêmico

A pandemia de COVID-19 se tornou um dos eventos mais marcantes do século XXI, afetando países em todo o mundo. Desde o seu surgimento em Wuhan, na China, no final de 2019, o vírus SARS-CoV-2 se desenvolveu rapidamente, evoluiu em um número substancial de casos e mortes. No cenário global, até setembro de 2021, mais de 220 milhões de casos de COVID-19 foram confirmados, com mais de 4,5 milhões de mortes em todo o mundo. Estados Unidos, Índia, Brasil, Rússia e Reino Unido estão entre os países que registraram maior número de casos e de óbitos [287].

286 O blockchain é um sistema de registro que contém todas as transações processadas no sistema. Em tradução livre, o nome significa cadeia de blocos. Uma cadeia de blocos nada mais é do que um conjunto de informações registradas que é ligado a blocos de informações anteriores e sucessores.

287 Os dados mencionados foram obtidos em agosto de 2022 através do site da OMS. Sugere-se a verificação

Durante todo o período pandêmico, diversas nações enfrentaram desafios em termos de sobrecarga dos sistemas de saúde, restrições sociais e psicológicas[288]. Foram vivenciadas uma série de situações sem precedentes no setor de saúde, que aceleraram processos e alteraram rotas em uma velocidade vertiginosa. A rápida disseminação do vírus sobrecarregou os sistemas de saúde em muitos países, incluindo o Brasil. A demanda por leitos hospitalares, ventiladores e outros recursos médicos essenciais aumentaram significativamente, gerando pressão sobre os sistemas de saúde, seus gestores e profissionais.

No Brasil, foram meses de extrema tensão em face da escassez de recursos, da falta de infraestrutura adequada e a falta de profissionais aptos a atender os doentes. Entre as medidas emergenciais propostas pelo governo brasileiro durante a pandemia, estavam a contratação de profissionais de saúde, aumento de carga horária de trabalho e até mesmo a antecipação da colação de grau de acadêmicos de medicina, de modo a ampliar a disponibilidade de profissionais de saúde para enfrentar a demanda crescente por atendimento médico. Essa medida foi tomada para fortalecer a capacidade de resposta do sistema de saúde diante da referida crise sanitária.[289]

A realidade é que os profissionais de saúde foram submetidos a uma enorme carga de trabalho e estresse durante a pandemia. Coube a eles atuar na linha de frente, arriscando suas vidas para atender aos pacientes e experimentando uma exaustão física e emocional. A escassez de recursos, a necessidade de adaptação rápida a novos protocolos e os riscos de exposição ao vírus aumentaram representam algumas das dificuldades enfrentadas pelos profissionais de saúde durante esse período.

---

de informações atualizadas a partir do sistema disponível no sítio eletrônico. WORLD HEALTH ORGANIZATION. Coronavirus disease (COVID-19) pandemic. WHO, 2019. Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019. Acesso em 20 ago. 2022.

288 A pandemia de COVID-19, que teve início em 2019, provocou mudanças na sociedade global. Com o avanço rápido da doença, as autoridades de saúde em todo o mundo tiveram que adotar medidas de emergência para controlar o controle do vírus.

289 A Resolução nº 03/2020, de 28 de março de 2020, do Conselho Nacional de Educação (CNE), estabeleceu diretrizes para a antecipação da colação de grau dos estudantes dos cursos de medicina que frequentam o último período do internato médico, desde que cumpram os requisitos. A resolução permitiu a formação antecipada desses estudantes, que poderiam, então, exercer atividades profissionais no contexto da pandemia. SÃO PAULO. Tribunal de Contas do Estado de São Paulo. Resolução nº 03/2020, de 29 de março de 2020. Dispõe sobre a redução do número de processos e otimização da tramitação dos feitos pelo Tribunal de Contas do Estado de São Paulo. São Paulo: TCESP, 2020. Disponível em: https://www.tce.sp.gov.br/sites/default/files/legislacao/RESOLUCAO-03-2020.pdf. Acesso em: 22 jan. 2023.
Além disso, a Portaria nº 492/2020, de 23 de março de 2020, do Ministério da Educação (MEC), estabeleceu medidas incentivadas para o funcionamento dos cursos de medicina durante a pandemia, permitindo a antecipação de bilhete e internatos, bem como a utilização de metodologias ativas de ensino e aprendizagem. BRASIL. Portaria nº 492/2020, de 23 de março de 2020. Institui a Ação Estratégica "O Brasil Conta Comigo", voltada aos alunos dos cursos da área de saúde, para o enfrentamento à pandemia do coronavírus (COVID-19). Diário Oficial da União, ed. 56-c, seção 1, p. 4, Brasília: Ministério da Saúde, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-492-de-23-de-marco-de-2020-249317442. Acesso em: 14 fev. 2023.

Na tentativa de conter a rápida expansão do vírus, o governo brasileiro implementou medidas de isolamento social e restrição de atividades não essenciais em diferentes momentos da pandemia, como *lockdowns*[290], quarentenas e adoção de horários reduzidos de funcionamento de estabelecimentos comerciais. Essas medidas visavam reduzir a circulação do vírus e conter a eficácia da doença. Neste período também foram realizadas campanhas de comunicação e informação para conscientizar a população sobre a importância das medidas preventivas, como o uso de máscaras, a higiene das mãos, o distanciamento social e a vacinação.

Ainda a assim, o Brasil padeceu sob o vírus que rapidamente contaminou uma parte significativa de sua população. Diante do aumento da demanda por leitos hospitalares, especialmente de Unidades de Terapia Intensiva - UTIs, o governo brasileiro buscou expandir a capacidade hospitalar. Foram criados hospitais de campanha, leitos ampliados em hospitais públicos e privados, e recursos mobilizados para garantir atendimento adequado aos pacientes com COVID-19. Essas ações foram fundamentais para evitar o colapso do sistema de saúde.

Nesse contexto de crise, a saúde digital emergiu como uma ferramenta crucial para fornecer serviços de saúde, monitorar e rastrear a disseminação da doença, e garantir o acesso a informações precisas. As políticas públicas já desenhadas para a saúde digital foram adaptadas de forma emergencial e ao final de um período de aproximadamente 24 meses, foi possível identificar avanços e retrocessos especialmente no que se refere as questões dos dados de saúde[291].

Surgiram as *pandemic-techs*, que podem ser conceituadas como ferramentas tecnológicas surgidas no contexto do enfrentamento da pandemia de COVID-19, e que resultaram em uma larga aceleração do processo de inserção das tecnologias digitais no sistema saúde. Através das citadas ferramentas, podem ser realizados tratamentos, atendimentos, bem como um controle epidêmico. Ademais, há um relevante papel

290 A bem-sucedida abordagem, adotada pelas autoridades chinesas em Wuhan e em outras cidades da China, de impor um confinamento – mais conhecido entre nós pelo termo inglês *lockdown* – como resposta à epidemia pelo novo coronavírus influenciou outros países a tentar fazer o mesmo quando ela se tornou pandemia. Tal medida tem óbvio potencial de impacto negativo na economia e, em regimes menos autoritários, sua implementação foi considerada controversa. NISHIOKA, S. A. Confinamento (lockdown) na pandemia por COVID-19: ter\ês experiências, três interpretações. UNASUS, 2022. Disponível em: https://www.unasus.gov.br/especial/covid19/markdown/554. Avesso em: 17 jul. 2022.

291 O Projeto Piloto do Conecte SUS já se encontrava em fase de execução, as iniciativas tanto da RNDS quanto do Informatiza APS estavam sendo coordenadas com foco em Alagoas. Contudo, diante da ocorrência do estado de calamidade pública provocado pelo novo coronavírus durante o mês de março de 2020, os projetos estruturantes do Conecte SUS tiveram de redirecionar seus esforços para auxiliar no controle da emergência da saúde pública. BRASIL. **Relatório Final do Projeto Piloto Conecte SUS**: análise dos avanços obtidos entre outubro/2019 e junho/2020. Brasília: Ministério da Saúde, 2020a.

destas tecnologias na realização de estudos e pesquisas de medicamentos terapêuticos, bem como na produção de medicamentos e vacinas.[292]

Dentre os principais avanços verificados quanto a utilização de tecnologias de saúde no período pandêmico se encontra a telessaúde e a telemedicina.[293]A pandemia acelerou a adoção dos aludidos serviços de telessaúde e telemedicina em todo o mundo. Por meio de consultas remotas, os pacientes puderam receber atendimento médico e monitoramento de condições de saúde sem sair de casa. Isso ajudou a reduzir a exposição ao vírus e aliviar a pressão sobre os sistemas de saúde.

Seguindo esta tendência, o Brasil adotou a telessaúde e a telemedicina em larga escala durante a pandemia[294], gerando um processo de expansão significativo. A necessidade de distanciamento social e a preocupação com a disseminação do vírus levaram a um aumento na demanda por serviços de saúde remotos, impulsionando o desenvolvimento, a adoção e a popularização dessas tecnologias.

Em linhas gerais, a telessaúde refere-se ao uso de tecnologias de comunicação para fornecer serviços de saúde à distância, enquanto a telemedicina envolve o diagnóstico e o tratamento remoto[295]. Essas abordagens permitem que os profissionais de saúde atendam os pacientes por meio de consultas virtuais, prescrições eletrônicas, monitoramento remoto de pacientes, entre outros serviços.

A partir da análise de relatório divulgado em julho de 2021 pela Associação Brasileira de Medicina Diagnóstica – ABRAMED, constatou-se que, no Brasil, a telemedicina teve um crescimento exponencial durante a pandemia. De acordo com o documento,

---

292 HUMMEL, G. Fatos e ações tecnológicas para mitigar o COVID-19. Digital Healthcare Hospitalar, 2020, p. 3. Disponível em: https://digital.hospitalar.com/pt-br/ti-inovao/fatos-e-aes-tecnolgicas-para-mitigar-o-Covid-19. Acesso em: 11 jul. 2020.

293 Se carece de um consenso sobre a diferença entre as nomeclaturas Telemedicina e Telessaúde, além de termos como eHealth, Telecare, eCare e Móbile Health, várias vezes as ideias se sobrepõem, e, outras vezes, se complementam. Mas, é possível afirmar que existe um ponto de convergência entre estas ideias: todos se referem ao uso de tecnologias de telecomunicações, informática e interatividade para prover ou realizar atividades e serviços de saúde à distância. De sorte que também se diz que Telemedicina e Telessaúde se referem ao uso de tecnologias interativas eletrônicas, de dados e conectividade, para organizar uma "cadeia produtiva de saúde", com finalidade de melhorar a estratégia e logística do sistema de saúde. WEN, C. L. Telemedicina e Telessaúde: oportunidade de novos serviços e da melhoria da logística em saúde. **Revista Panorama Hospitalar**, [*S. l.*], p. 24-26, 2015, p. 24. Disponível em:
https://nuvemdoconhecimento.org.br/wp-content/uploads/2015/03/03132015_Revista_Panorama_Hospitalar_Fev_2015_pag24a26.pdf. Acesso em: 14 maio 2023.

294 BRASIL. **Resolução CFM nº 2.271/2020, de 14 de fevereiro de 2020**. Define as unidades de terapia intensiva e unidades de cuidado intermediário conforme sua complexidade e nível de cuidado, determinando a responsabilidade técnica médica, as responsabilidades éticas, habilitações e atribuições da equipe médica necessária para seu adequado funcionamento. Brasília: Associação Brasileira de Mantenedoras de Ensino Superior. Disponível em: https://abmes.org.br/arquivos/legislacoes/resolucao-CFM-2271-2020-02-14.pdf. Acesso em: 13 fev. 2022.

295 WEN, op. cit., p.23.

o número de consultas médicas remotas realizadas saltou de cerca de 1.000 por mês, antes da pandemia, para mais de 1 milhão por mês no pico da crise sanitária[296].

O Ministério da Saúde, por meio do Programa Conecte SUS, buscou ampliar o acesso à saúde por meio da telemedicina e telessaúde. No entanto, é importante mencionar que popularização das referidas tecnologias no Brasil também trouxe desafios. A falta de acesso à internet em algumas regiões do país, especialmente em áreas rurais e comunidades de baixa renda, por exemplo, dificultou a implementação e o alcance dessas tecnologias. Além disso, houve preocupações relacionadas à segurança dos dados dos pacientes e à qualidade do atendimento remoto em comparação com o presencial.

Com efeito, a utilização da telemedicina implica na transmissão, armazenamento e processamento de informações sensíveis dos pacientes, o que exige uma atenção especial à proteção desses dados pessoais. Suas práticas permitem a troca de informações médicas por meio de plataformas digitais, móveis e outras tecnologias. E é preciso atentar que essas transferências de dados apresentam riscos de segurança.

Se os sistemas de telemedicina não forem protegidos de forma eficaz, pode haver o risco de acesso não autorizado a informações médicas. Hackers ou indivíduos mal-intencionados podem tentar obter acesso aos sistemas e roubar esses dados para fins ilícitos, como extorsão, venda, fraude ou chantagem, tal como aconteceu no ano de 2020 quando uma falha do Ministério da Saúde veio a expor dados de 243 milhões de brasileiros na internet.[297]

Outro ponto de atenção é a questão da comunicação entre profissionais de saúde e pacientes por meio de plataformas de telemedicina, que pode ocorrer por meio de conexões de internet inseguras. Isso pode tornar os dados já interpretados passíveis de interceptações durante a transmissão, especialmente se as medidas de criptografia[298] não forem corretamente integradas.

---

296 ALBUQUERQUE, B. Brasil contabiliza 2,5 milhões de teleconsultas nos últimos 12 meses. Blog Abramge, São Paulo, 2021. Disponível em: https://blog.abramge.com.br/saude-suplementar/brasil-contabiliza-25-milhoes-de-teleconsultas-nos-ultimos-12-meses/. Acesso em: 12 jul. 2023.

297 Uma nova falha do Ministério da Saúde expôs dados de cerca de 243 milhões de brasileiros na internet, de acordo com informações do jornal "O Estado de S. Paulo". O Ministério disse em nota que houve exposição de base cadastral, mas que não houve acesso às informações. Sugere-se a leitura da notícia completa. NOVA FALHA do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. G1, 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 17 jul. 2022.

298 Na Saúde, o principal objetivo com o uso da criptografia é proteger as informações confidenciais dos pacientes e os aplicativos. Porém, apenas um terço dos estabelecimentos de saúde contam com uma política definida sobre segurança da informação, sendo o percentual dos públicos (21%) menor em relação ao dos privados (cerca de 40%). Os dados são da pesquisa TIC Saúde 2021, realizada pelo NIC.br. Entre as ferramentas de segurança,

Ademais, o armazenamento dos dados de saúde colhidos durante as consultas de telemedicina requer cuidados específicos. Se as informações não forem mantidas de maneira segura, seja em servidores ou em dispositivos móveis, podem ocorrer fugas de dados ou acesso não autorizado, comprometendo a privacidade dos pacientes. Falhas no software, ausência de atualizações de segurança e falta de testes adequados podem resultar em vulnerabilidades técnicas que favorecem o vazamento de dados, trazendo sérios riscos aos usuários do sistema de saúde.

Além da telemedicina, a utilização de aplicativos e plataformas de rastreamento de contatos também é um ponto que exige reflexão em termos de segurança de dados. Durante a pandemia diversos países desenvolveram aplicativos móveis e plataformas online para rastrear contatos de pessoas infectadas com o vírus. No Brasil, esta proposta chegou a ser materializada através da atualização do aplicativo Cornavírus SUS no ano de 2020.[299]

Embora a adesão a essas tecnologias tenha sido variável, elas conseguiram um papel na identificação de possíveis cadeias de transmissão e no direcionamento de medidas preventivas. Porém, ainda que se trate de uma ferramenta que permite uma identificação mais rápida de potenciais expostos e que ajude a conter as reações da doença, o sistema carece de garantia da proteção relacionadas à privacidade e aos dados pessoais dos usuários, bem como conduz a um receio quanto à possibilidade de restrição da liberdade das pessoas. No Brasil, particularmente, essa proposta logo perdeu força.

Outro ponto importante que acabou sendo impulsionado pela pandemia foi a utilização da inteligência artificial e da análise de dados na área da saúde[300]. Essas

---

aquelas relacionadas à criptografia apresentaram maior aumento na comparação a 2019, a exemplo da criptografia de arquivos e e-mails, presentes em 52% dos estabelecimentos (contra 41% em 2019). Já a criptografia da base de dados avançou de 36%, em 2019, para 48% em 2021. ASSESPRO. Segurança da Informação e adequação à LGPD são para poucos na saúde no Brasil. Nic.br, 2021. Disponível em: https://www.nic.br/noticia/na-midia/seguranca-da-informacao-e-adequacao-a-lgpd-sao-para-poucos-na-saude-no-brasil. Acesso em: 7 abr. 2022.

299 O Ministério da Saúde lançou uma atualização para o aplicativo Coronavírus SUS que poderá rastrear e alertar sobre a proximidade e o contato com pessoas infectadas pela COVID-19. A tecnologia, chamada API Exposure Notification, já é usada em outros países, como Alemanha, Itália e Uruguai, e só será ativada caso o usuário habilite a função "notificação de exposição" nas configurações do aplicativo. Notícia completa: CORONAVÍRUS SUS vai rastrear contatos de infectados com COVID-19/. Convergência Digital, 2020. Disponível em: https://www.convergenciadigital.com.br/Internet-Movel/Coronavirus-SUS-vai-rastrear-contatos-de-infectados-com-Covid-19-54394.html?UserActiveTemplate=mobile%2Csite&s+id=17. Acesso em: 17 maio 2023.

300 A IA, durante a pandemia, foi a ferramenta utilizada para acelerar a leitura de grandes bancos mundiais e criar informações em tempo real que ajudaram a entender como a incidência do vírus acontecia em todo mundo. Esses dados foram divulgados em Boletim Epidemiológicos: ocorrência, confirmação de casos, óbitos, cidade do diagnóstico, microrregião, região de saúde, região de leitos de UTI, leitos de UTI ocupados e disponíveis e profissionais de saúde alocados. SILVA, D. F.; OLIVEIRA, M. L. Epidemiologia da COVID-19:

tecnologias foram determinantes para que se conseguisse analisar grandes volumes de dados epidemiológicos, identificar padrões, prever tendências e auxiliar na tomada de decisões por parte dos profissionais de saúde e autoridades governamentais, criando padrões e protocolos que auxiliam nas tomadas de decisão.

Em meio aos benefícios e inúmeras possibilidades da aplicação Inteligência Artificial na área de saúde, também é preciso atentar para os riscos gerados. Trata-se de mais um caso no qual uma pequena falha na condução da administração dos processos pode provocar exposição de dados sensíveis. Logo, é preciso uma maior atenção em relação ao tratamento, armazenamento e descarte de dados de saúde, o que só será possível com investimentos em recursos de segurança e treinamento de profissionais, de forma a concretizar o planejamento e os modelos de proteção de dados propostos para o Brasil.[301]

Também é necessário refletir quanto às questões éticas que permearam o processamento de dados no cenário pandêmico. Por diversos momentos, foi possível constatar o comprometimento do equilíbrio entre os direitos individuais e coletivos, colocando em xeque a proteção à intimidade das pessoas[302]. Tomando por exemplo a questão dos aplicativos, verifica-se que os dados coletados são utilizados de forma comercial, visto que dados de geolocalização passaram a ser utilizados para mensurar os índices de isolamento e de visita a hospitais. Dessa forma, resta evidente a tensão entre direitos fundamentais, com uma restrição do direito à privacidade decorrente da implementação de mecanismos de monitoramento da circulação dos indivíduos, em razão da necessidade de privilegiar o direito à vida da população, bem como a concretização de políticas públicas de saúde.

A tensão entre os referidos direitos fundamentais ganhou relevo em razão da carência de uma norma que disciplinasse de forma detalhada a matéria. Isso porque foi necessário, em caráter emergencial, não apenas no Brasil, mas em diversos países do mundo, adotar medidas que deram azo a debates sobre os limites do alcance do interesse coletivo em detrimento da privacidade e da liberdade individual do cidadão. No ano de 2020, Tribunal de Justiça de São Paulo considerou legal a criação do

comparação entre boletins epidemiológicos. **Comunicação em Ciências da Saúde**, Brasília, v. 31, n. 1, 2020. Disponível em: http://10.233.90.10:8080/jspui/handle/prefix/188. Acesso em: 11 abr. 2023.

301 RODRIGUES, P. M. A inteligência artificial médica e o uso de dados pessoais no atendimento aos pacientes. Migalhas, São Paulo, 2020, p. 2. Disponível em: https://www.migalhas.com.br/depeso/ 325245/a-inteligencia-artificial-medica-e-o-uso-de-dados-pessoais-no-atendimento-aos-pacientes. Acesso em: 8 jul. 2022.

302 ALMEIDA, B. A. *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. (2020). **Ciência & Saúde Coletiva**, Rio de Janeiro, v. 25, p. 2487–2492, 2020. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em: 9 jul. 2020.

referido sistema de monitoramento inteligente de smartphones, em tempo real, com o objetivo de identificar índices de isolamento social e orientar a definição de estratégias de prevenção e combate à pandemia no estado, afastando, pois, a alegação de eventuais violações à intimidade e à vida privada dos cidadãos.[303]

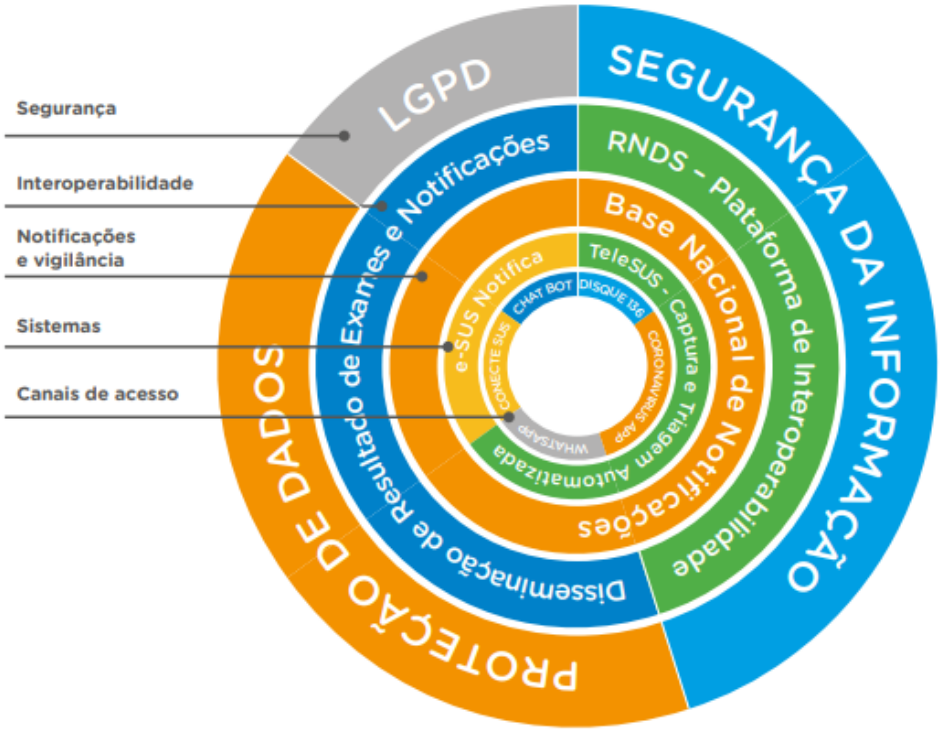
O senso de urgência durante a pandemia de COVID-19 acelerou processos e permitiu a larga utilização das tecnologias no setor de saúde, antes que fosse possível responder a dois importantes questionamentos. O primeiro deles se refere à segurança dos mecanismos adotados para a coleta dos dados de saúde, visto que, mesmo após o processo de anonimização, continua a existir, em certos casos, a chance de identificação de seu titular, em violação ao direito à privacidade. O segundo questionamento – um desdobramento do primeiro –, diz respeito às cautelas a serem observadas por ocasião da eliminação dos dados coletados[304].

O enfrentamento da pandemia exigiu uma movimentação de informações sem precedentes, nos mais diversos níveis, perpassando desde o registro das notificações, óbitos, resultados de exames realizados até o provimento de serviços de prevenção e cuidado. Para atender estas demandas, o Conecte SUS apresentou um ecossistema de atendimento e tratamento de dados em saúde específico para a COVID-19, contendo linhas de segurança da informação, interoperabilidade entre sistemas, processos de notificação e vigilância em saúde, aplicativos móveis e canais de acesso, tal como ilustrado na figura abaixo.

303 SÃO PAULO. Procuradoria-Geral do Estado de São Paulo. TJSP reconhece legalidade do Sistema de Monitora-mento Inteligente (SIMI). São Paulo: PGE, 2020. Disponível em: http://www.pge.sp.gov.br/visualizanoticia.aspx?id=4175. Acesso em: 8 jul. 2020

304 NASCIMENTO, J. C. H. B. et al. Inteligência artificial na saúde e a proteção de dados: reflexos na crise Covid-19. Revista Brasileira De Direitos Fundamentais & Justiça, Belo Horizonte, v. 14, n. 1, p. 207–230, 2020, p. 7. Disponível em: https://doi.org/10.30899/dfj.v0i0.964. Acesso em: 11 mar. 2023.

Figura 5 - Segurança da informação no Conecte SUS



Fonte: Boletim Conecte SUS[305]

O Projeto Piloto da RNDS acabou por ser redirecionado para permitir recepção e integração de notificações e resultados de exames laboratoriais relacionados à COVID-19, bem como a disseminação dos resultados dos exames aos cidadãos e profissionais de saúde pelo Portal Conecte SUS. Nessa senda, o Ministério da Saúde se uniu a laboratórios de análises clínicas, em um esforço para viabilizar o encaminhamento dos resultados de exames de COVID-19 para a Rede Nacional de Dados em Saúde. Segundo o referido Ministério, a plataforma está apta a coletar, armazenar e disponibilizar estes dados de forma segura e com garantia de privacidade, para profissionais de saúde e cidadãos por meio do Portal Conecte SUS.[306] Entretanto, os registros de vazamentos de dados de saúde revelam que ainda há um caminho a ser percorrido para concretizar esta promessa.

A realidade pandêmica permitiu perceber que, embora o cidadão usuário dos sistemas de saúde detenha certa liberdade em relação ao controle de seus dados, diante de situações emergenciais, prevalecem hipóteses específicas para adaptação dos serviços

305 BRASIL. Ministério da Saúde. **Relatório Final do Projeto Piloto Conecte SUS**: análise dos avanços obtidos entre outubro/2019 e junho/2020. Brasília: Ministério da Saúde, 2020. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_projeto_piloto_conectesus_outubro.pdf. Acesso em: 30 maio 2022.

306 Dados coletados no Relatório Final do Projeto Piloto Conecte SUS de 2020. BRASIL, op cit., 2020a.

de saúde aos interesses coletivos. Desta forma, as previsões iniciais sucumbem a adoção de novos processos. Porém, é imperioso que padrões de segurança e privacidade também sejam adaptados, tendo em vista não apenas à infraestrutura virtual, mas também profissionais, técnicos, auxiliares e gestores[307].

Cabe ao Estado, às organizações públicas e privadas do setor de saúde, bem como aos titulares de dados, um esforço conjunto para a proteção de dados pessoais. A LGPD, legitima e permite ações efetivas dos cidadãos no sentido de exigir e fiscalizar o direito à privacidade de suas informações pessoais quando da utilização de sistemas digitais de saúde. Mais do que nunca, é necessário que as organizações privadas se adequem corretamente a normativa legal, adaptando seus recursos humanos e materiais, enquanto o Estado deve assumir fiscalizar o cumprimento da legislação, além de prestar informações e conhecimento à sociedade.

307 REBELO, T. Por que os profissionais e empresas de saúde precisam se adequar à Lei Geral de Proteção de Dados?. Revista Jus Navigandi, Teresina, ano 24, n. 5860, 2019, p. 5. Disponível em: https://jus.com.br/artigos/74825. Acesso em: 15 ago. 2023.

5 Capítulo 4 - Desafios da saúde digital no contexto brasileiro.

O quarto capítulo da tese trata dos principais desafios para a concretização da visão de saúde digital no Brasil, partindo da análise do processo da inserção da proteção de dados como política pública, propõe-se a apresentação de um panorama que revela as principais vulnerabilidades da utilização de novas tecnologias nos serviços público e privado. As práticas de coleta e tratamento de dados pessoais são hoje, fundamentais no sistema da saúde. Os serviços públicos e privados de saúde têm se utilizado de um conjunto cada vez maior de soluções digitais que reduzem custos e otimizam a eficácia e a qualidade do tratamento, tornando a tecnologia indispensável para seus processos e ações.

Como consequência deste rápido avanço emergem riscos à proteção de dados pessoais, envolvendo inúmeras possibilidades de vazamento, falta de transparência dos sistemas e utilização indevida de dados pessoais sensíveis que podem afetar de modo direto pessoas, abrindo novos meios de discriminação. Neste sentido, serão abordadas neste capítulo, as principais vulnerabilidades verificadas na gestão dos dados de saúde, com destaque para o baixo índice de planejamento, ausência de política de segurança da informação e deficiências no quadro técnico e ainda, a possibilidade de desagregação entre a pessoa-fonte e seus dados clínicos face a proteção da dignidade da pessoa humana, bem como a legitimidade do tratamento de dados clínicos com fins sanitários e a possibilidade de novas formas de xenofobia.

5.1 A proteção de dados pessoais e sensíveis e a sua inserção como política pública conforme a LGPD e Constituição Federal

Não há dúvidas de que proteção de dados pessoais é uma questão de extrema importância na sociedade atual, especialmente com o advento das novas tecnologias e a crescente digitalização das informações. A proteção de dados pessoais enquanto política pública representa o reconhecimento da necessidade de o Estado atuar na regulação e promoção de medidas para salvaguardar os direitos e privacidade dos cidadãos. Contudo, a efetivação nesta condição requer o envolvimento de diversos

atores, como órgãos reguladores, empresas, organizações da sociedade civil e a própria população.

A crescente quantidade de dados pessoais coletados e processados pelas organizações de saúde, aliada ao rápido avanço tecnológico, torna essencial a adoção de medidas para proteger essas informações e preservar direitos individuais dos usuários do sistema. É preciso estabelecer mecanismos para preservar a intimidade, a vida privada e a autonomia dos indivíduos, garantindo que suas informações pessoais sejam tratadas de forma segura, mediante consentimento adequado.

Enquanto o Estado desempenha um papel fundamental na promoção da proteção de dados, por meio da criação de leis e regulamentações, da fiscalização e da garantia do cumprimento das normas infringidas, coube a Autoridade Nacional de Proteção de Dados - ANPD exercer o papel de órgão regulador e fiscalizador. A ANPD é responsável por supervisionar a aplicação da LGPD, emitir diretrizes e orientações, aplicar sanções administrativas em caso de desconformidade e promover a conscientização sobre a importância da proteção de dados pessoais[308].

Além disso, a proteção de dados pessoais como política pública implica em estabelecer estratégias e instrumentos para a implementação efetiva das medidas de segurança e privacidade. Isso envolve a criação de políticas de governança de dados, a capacitação de profissionais especializados, a promoção da pesquisa e desenvolvimento de tecnologias seguras, bem como a colaboração com outros países para troca de experiências e boas práticas. Neste sentido, o Brasil apresentou nos últimos anos a Política Nacional de Informação e Informática em Saúde - PNIIS, as Estratégias de Saúde Digital para o Brasil, o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC e o Programa Conecte SUS.

A cada nova versão destes documentos e de seus relatórios de avaliação, é visível a presença da preocupação com as questões de proteção de dados pessoais, contudo ainda se enfrenta uma considerável discrepância entre teoria e prática. Ao falar da segurança no tratamento de dados sensíveis de saúde, o Estado pretende obter a confiança dos cidadãos usuários dos sistemas de saúde, e difundir a presença de inovações tecnológicas nas ações cotidianas da população. Porém estas afirmações não têm sido cumpridas na prática, onde se percebe com frequência a falta de preparo humano e material para resguardar dados sensíveis.

308 LGPD, Art. 55-C. A ANPD é composta de: I - Conselho Diretor, órgão máximo de direção; II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III - Corregedoria; IV - Ouvidoria; V - órgão de assessoramento jurídico próprio; V - Procuradoria; V-A - Procuradoria; e VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. BRASIL, op. cit., 2018.

Conforme discutido nos capítulos iniciais deste texto, no Brasil, a Constituição Federal estabelece princípios e fundamentos que buscam sustentar a proteção de dados como um direito fundamental, e assegurar deste modo, a privacidade dos indivíduos no contexto digital. A exemplo, o artigo 5º, inciso X, que assegura o direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Esse dispositivo constitucional estabelece uma licença para a proteção dos dados pessoais, reconhecendo a importância da privacidade como um direito fundamental. Soma-se a este, o princípio da dignidade da pessoa humana, presente em seu artigo 1º, inciso III, que aduz a importância de respeitar a autonomia e a liberdade das pessoas em relação ao tratamento de suas informações pessoais.

Tal visão foi fortalecida pela Emenda Constitucional nº 115/2022, que acrescentou o inciso LXXIX ao artigo 5º da Constituição.[309] Esse dispositivo estabelece o direito à proteção dos dados pessoais como um direito fundamental, ao afirmar que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Já o artigo 21 passa a vigorar acrescido do seguinte inciso XXVI, segundo o qual cabe a União a responsabilidade de organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei[310]. Por fim, a emenda altera o artigo 22 atribuindo competência legislativa à União para legislar acerca da proteção e tratamento de dados pessoais no Brasil.[311]

O Estado Social e Democrático de Direito é considerado um ambiente no qual os esforços de seus atores convergem para a consecução de objetivos coletivos. Toda a atuação estatal é direcionada à prestação de serviços públicos e ações das mais diversas ordens com o objetivo de prover condições mínimas necessárias ao atendimento da noção preliminar de dignidade dos cidadãos.

Verifica-se o dever de concretizar os direitos fundamentais prometidos pela Constituição Federal, buscando a alcançar a igualdade material, e assegurar aos indivíduos as mínimas condições para desfrutarem o direito à liberdade, a intimidade, a privacidade e a dignidade. Logo, o Estado deve portar-se de forma racional e planejada, conforme a elaboração e implementação de políticas públicas[312].

A entrada em vigor da LGPD reforça o direito à privacidade e à proteção dos dados pessoais mencionados na Constituição Federal, e avança ao dispor sobre autoridades

309 BRASIL, op. cit., 2022.
310 Artigo, 21, Constituição Federal, 1988. BRASIL, op. cit., 2018.
311 Artigo 22, Constituição Federal, 1988. Idem.
312 NUNES, op. cit., p. 4.

competentes, orientações e procedimentos visando assegurar que os indivíduos tenham o controle sobre suas informações, por meio regras específicas para o tratamento desses dados por parte das organizações. Nos termos da lei, coube ao Poder Público o papel de agente de tratamento de dados, conforme expressa previsão contida nos artigos 1º e 23[313], o que automaticamente demanda a indicação de parâmetros específicos para as atividades relacionadas a dados, no âmbito de atuação de cada ente político. Como meio transpor as regras propostas na LGPD para as vivências práticas, o Estado inseriu a proteção de dados pessoais e sensíveis como política pública.

Ao se pensar a noção de política pública[314] é importante recordar sua natureza coletiva enquanto categoria jurídica. É a partir do direito que se estrutura o quadro institucional de determinado programa de ação governamental, a fim de que esteja em conformidade à Constituição Federal no sentido da concretização dos direitos fundamentais e projeção da cidadania.[315] O conceito de política pública, portanto, deve ser considerado na dimensão jurídica e direcionado a missão de criar um ciclo de formação com ênfase na atuação do Poder Judiciário, mediante o exercício do controle judicial.[316] São elas, o caminho para buscar formas de concretização dos direitos humanos e sociais.

A política pública, enquanto um programa ou plano de ação governamental, formulado a partir de um conjunto de medidas articuladas, possui a finalidade de movimentar o Poder Público e demais agentes no sentido de realizar um objetivo específico de interesse coletivo ou concretizar um direito.[317] Assim, a inserção da

313 LGPD, artigo, 1º: Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. Artigo 23, caput: O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. BRASIL, op. cit., 2018.

314 Ronald Dworkin ao conceituar a política pública (policies) no âmbito da Teoria do Direito, considerando-a como "(...) aquele tipo de padrão que estabelece um objetivo a ser alcançado, em geral uma melhoria em algum aspecto econômico, político ou social da comunidade". DWORKIN, Ronald. Levando os direitos a sério. Tradução: Nelson Boeira. São Paulo: Martins Fontes, 2002. Coleção direito e justiça, p. 36.

315 NUNES, A. R. S. **Políticas públicas**. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017, Tomo: Direitos Difusos e Coletivos, p.12. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/376/edicao-1/politicas-publicas. Acesso em: 18 fev. 2023.

316 CARVALHAES, Andréia R. Schneider Nunes. Limites e aferição do controle judicial de políticas públicas. Tese (Doutorado em Direito Político e Econômico) - Universidade Presbiteriana Mackenzie, São Paulo, 2018, p.42.

317 BUCCI, M. P. D. O conceito de política pública em direito. *In*: BUCCI, M. P. D. Políticas Públicas: Reflexões sobre o Conceito Jurídico. São Paulo: Saraiva, 2006, p. 14.

proteção de dados pessoais e sensíveis como política pública, foi o caminho natural para materializar os preceitos da Constituição Federal e da LGPD.

Apesar de existirem dispositivos legais no Brasil que abordam a questão da privacidade e da proteção de dados, as regras eram esparsas e se mostravam superficiais para o momento tecnológico vivenciado no país. A ausência de uma legislação específica para proteção dos dados pessoais e, em especial, dos dados sensíveis, configurou o ponto de partida para a elaboração das políticas públicas atuais.

Aos poucos a utilização de dados se popularizou no país, sendo conduzida tanto por agentes públicos, como por agentes privados. Consequentemente, riscos e incidentes que feriam a liberdade, dignidade e privacidade dos usuários de sistemas digitais começaram a ser identificados com mais profundidade e frequência, resultando na necessidade de formação de uma agenda para discutir a matéria[318]. A proteção de dados, passou a ser tratada como prioridade por todo o Poder Público, que compreendeu a necessidade de regulamentação através de um marco legal.

Enquanto formulação de alternativas, o Poder Executivo, elaborou um anteprojeto de lei para tratar da proteção de dados pessoais, que convergiu no PL no 5.276/2016[319]. Outros projetos de lei que dispunham sobre o tema também chegaram a ser propostos pelo Poder Legislativo, como o PL no 4.060/2012[320] e o PLS no 330/2013[321], afiançando a necessidade da regulação do tema. Com as crescentes demandas oriundas dos avanços das tecnologias e da ampliação das redes e sistemas a serviço da população brasileira, foi atingido o estágio chamado de "tomada de decisão", marcado pelo

318 Se um problema é identificado por algum ator político, e esse ator tem interesse na resolução de tal problema, este poderá então lutar para que tal problema entre na lista de prioridades de atuação. Essa lista de prioridades é conhecida como agenda. SECCHI, L. Políticas Públicas: conceitos, esquemas de análise, casos práticos. São Paulo: Cengage Learning, 2012, p. 36.

319 PL no 5.276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. BRASIL. **Projeto de Lei nº 5.276, de 2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília, DF: Câmara dos Deputados, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0q1d5lxsv6vat1f4w8rhsnjs9u9 626721.node0?codteor=1457459&filename=PL+5276/2016. Acesso em: 24 mar. 2023.

320 PL no 4.060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. BRASIL. Projeto de Lei nº 4.060 de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Presidência da República, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 24 mar. 2023.

321 PLS no 330/2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. BRASIL. Projeto de Lei do Senado n° 330, de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Brasília: Senado, 2013. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947. Acesso em: 24 mar. 2023.

equacionamento de interesses e intenções. Esta foi uma fase abalizada por estudos, debates e consultas públicas em meio digital, para discutir o anteprojeto de lei.[322]

Em 2018 com a aprovação da LGPD se iniciou a implementação das novas regras, inicialmente com os procedimentos de planejamento e preparação para as políticas de proteção de dados. Conforme abordado no capítulo anterior, a entrada em vigor da LGPD exigiu a revisão de planejamentos, programas e estratégias propostas anteriormente, bem como demandou a atualização de protocolos e ações do poder público e de empresas privadas.

A título de conhecimento, a cronologia descrita na tabela abaixo demonstra o processo gradual de construção da LGPD, desde sua concepção até sua implementação e regulamentação. A legislação é resultado de um conjunto de esforços de diversos atores, visando à proteção dos direitos dos titulares de dados pessoais e à garantia da segurança e privacidade em meio a presença cada vez mais marcante das tecnologias na sociedade brasileira e no mundo.

Quadro 1 – Processo de construção da LGPD

Ano	Evento/Lei
2010	Criação do Marco Civil da Internet
2012	Realização da Conferência NETMundial
2013	Veto presidencial ao projeto de lei de dados pessoais
2014	Marco Civil da Internet entra em vigor
2015	Projeto de lei de dados pessoais é reapresentado no Congresso
2018	Sanção da Lei Geral de Proteção de Dados (LGPD)
2020	Início da Vigência da LGPD
2021	Criação da Autoridade Nacional de Proteção de Dados (ANPD)
2021	Início das decisões administrativas pela ANPD

Fonte: Elaborado pela autora.

A LGPD se destacou ao estabelecer diretrizes claras para o tratamento de dados pessoais, contribuindo para a adoção de medidas de segurança cibernética e prevenção de violação, minimizando riscos de acesso não autorizado, vazamento e uso indevido de informações[323]. Além disso, configura um meio de promover a transparência no

322 Neste período, situações externas acabaram por acelerar o processo de elaboração da política pública brasileira quanto à proteção de dados. No ano de 2018, o tema ganhou visibilidade por ser um ano eleitoral no Brasil e terem sido divulgadas informações acerca da utilização de dados de usuários do Facebook obtidos de forma não consentida, que acabaram por influenciar a campanha eleitoral de Donald Trump, nos Estados Unidos. Além disso, a entrada em vigor das novas regras estabelecidas pelo Regulamento Geral de Proteção de Dados da União Europeia, em maio de 2018 exigiu um posicionamento do Brasil quanto aos requisitos do manuseio de dados e consentimento para sua exploração.

323 A título de exemplo, em janeiro de 2021, a Serasa Experian foi notificada pelo Procon-SP que solicitou esclarecimentos sobre um suposto vazamento, envolvendo 220 milhões de dados pessoais de cidadãos brasileiros. A empresa negou o incidente e afirmou não haver nada indicações de que ocorreu vazamento de suas bases,

tratamento dos dados pessoais, informando aos titulares quais informações estão sendo coletadas, como serão utilizadas e permitindo o controle sobre o compartilhamento e exclusão desses dados.

Transcorridos pouco mais de três anos do início da vigência da LGPD[324], avanços e vulnerabilidades foram identificados quando se confronta teoria com a prática. A dimensão da base legal de execução de políticas públicas somada a amplitude de autorização do tratamento de dados por governos abre uma inquietante preocupação quanto a possibilidade de abusos[325]. Há que se primar pelo desenvolvimento social e tecnológico, mas sem olvidar os direitos à privacidade, intimidade e proteção de dados do cidadão. Trata-se de um delicado conflito que será aprofundo nos tópicos seguintes deste capítulo.

5.2 A amplitude das normas como obstáculos para proteger e administrar os dados pessoais e sensíveis

A inserção dos mais diversos tipos de tecnologias no cenário da saúde é tida como a grande solução para o enfrentamento de grandes desafios do setor, uma vez que viabiliza ao aumento da eficiência dos procedimentos e amplia o acesso às pessoas desassistidas aos serviços de saúde. Como já mencionado no capítulo anterior a oferta de tecnologias relacionadas à saúde que vinha em uma crescente nas últimas décadas, foi intensificada de forma expressiva durante o período pandêmico. Serviços como telesaúde, dispositivos móveis, análise de big data e inteligência artificial passaram

e afirmou continuar conduzindo uma investigação para apurar o incidente. Apesar da Serasa apresentar Parecer Técnico de empresa especializada segundo o qual os sistemas da empresa seriam seguros, o Procon-SP entende que, não foram implementadas medidas para cumprimento do Código de Defesa do Consumidor - CDC e da Lei Geral de Proteção de Dados - LGPD. Conforme as notícias, dados como nome, CPF, fotografia, salário, renda, nível de escolaridade, estado civil, score de crédito, endereço teriam sido violados e estariam sendo divulgados e comercializados na Internet. Notícia disponível em: https://www.procon.sp.gov.br/serasa-complementa-resposta-sobre-vazamento-de-dados/

324 O ciclo das Políticas Públicas abrange sete etapas interdependentes: 1) identificação do problema, 2) formação da agenda, 3) formulação de alternativas, 4) tomada de decisão, 5) implementação, 6) avaliação e 7) extinção. SECCHI, op. cit., p. 36.

325 O Relatório da Relatoria Especial da ONU sobre Pobreza Extrema e Direitos Humanos de 2019, ao analisar a digitalização de programas de bem-estar social, afirma que a ausência de regras claras sobre o tratamento de dados pessoais por governos permite que informações sobre esses indivíduos sejam utilizadas para "vigiar, mirar, intimidar e punir beneficiários de programas sociais, especialmente aqueles dentre as populações mais vulneráveis. ODS – OFFICIAL DOCUMENTS SYSTEM OF THE UNITED STATE. Un Human Rights Council. ODS, 2019. Disponível em:
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/197/47/PDF/N2119747.pdf?OpenElement. Acesso em: 2 jun 2023.

a integrar o cotidiano de instituições, profissionais e usuários dos sistemas de saúde público e privado.

Em consequência, o aumento vertiginoso de dados sensíveis de saúde lançados em rede todos os dias, com a consequente necessidade de proteção e justificativa para seu uso. Enquanto instrumento direto para responder a tal demanda, o Estado se vale da LGPD. Como visto nos capítulos iniciais deste trabalho, a é uma legislação abrangente que estabelece princípios, direitos e obrigações relacionados à proteção de dados pessoais no Brasil. No entanto, é de certa forma esperado que uma norma de tamanha amplitude acabe por apresentar pontos obscuros e venha a ser considerada falha em certos aspectos por não ser suficientemente específica para abordar todas as nuances e contextos específicos relacionados à proteção de dados pessoais e sensíveis. Em fato, atingir tal precisão parece uma tarefa impossível, diante da natureza da matéria.

Em seu texto, a LGPD abrange uma ampla gama de dados pessoais e sensíveis, incluindo informações de identificação, elementos de saúde, informações financeiras, dados genéticos, entre outros. Essa amplitude cria desafios para as organizações quanto a proteção e administração adequada desses dados, considerando a verificação de diferentes categorias e níveis de sensibilidade.

Ao definir dados pessoais como informações relacionadas a uma pessoa natural identificada ou detectável, a LGPD se utilizou desta perigosa amplitude. Afinal, a identificação de uma pessoa pode ocorrer de várias maneiras, incluindo informações indiretas ou combinando dados de diferentes fontes. A interpretação dos limites dessa definição pode ser complicada em casos complexos ou de dados agregados. Mas esta é apenas uma das situações que podem ser identificadas no artigo 5º da norma.

A ausência de uma definição detalhada para dados sensíveis [326] é uma questão abordada previamente, mas que se destaca neste contexto, como um exemplo de lacuna que acaba por dificultar que a norma atinja seus propósitos. Ao se pensar em dados sensíveis[327], fica a carência de uma especificação detalhada para cada tipo de dado sensível. É plausível assumir que determinados dados apresentem maior potencial discriminatório e potencial lesivo do que outros, revelando diretamente fragilidades e

326 Art. 5º, LGPD: 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; BRASIL, op. cit., 2018.

327 Dados sensíveis são uma espécie de dados pessoais que "compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação" BIONI, B. R. Proteção de Dados Pessoais: a função e os limites do consentimento. São Paulo: Forense, 2018, p. 8.

limitações. Assim, a indefinição de espécies de dados sensíveis e pode gerar discussões, debates e até decisões divergentes sobre como aplicar a lei em casos específicos.

É preciso atentar ainda, ao fato de que existem dados que embora não sejam inicialmente qualificados como sensíveis podem atingir essa condição, uma vez submetidos a um determinado tratamento, revelando aspectos da personalidade de uma pessoa, que, por sua vez, o que poderia culminar em práticas discriminatórias. É válido recordar que a capacidade de tratamento de dados pessoais foi consideravelmente ampliada com os recentes avanços das tecnologias, especialmente a popularização da inteligência artificial, mapeamento de algoritmos e por meio da possibilidade da *machine learning*[328].

Se um dado pessoal pode ser transmutado em sensível, o conceito de dados sensíveis deve ser pensado através do princípio da funcionalidade e considerar diretamente as formas de tratamento as quais é submetido. Deste modo, os dados sensíveis deverão ser assim considerados, não apenas por sua natureza personalíssima, mas também conforme o uso, a finalidade atribuída e a verificação da existência de potencial discriminação[329].

Outra situação que merece reflexão é anonimização de dados. A definição de anonimização contida na LGPD pode ser interpretada de maneiras diferentes, levando a diferentes abordagens na prática[330]. Embora a LGPD forneça diretrizes básicas para a anonimização, não há uma definição precisa e detalhada no texto da lei. Essa falta de especificidade também abre margem para interpretações diversas e desafios na aplicação prática do conceito.

---

328 O Machine Learning é um ramo da Inteligência Artificial, podendo dessa forma, ser classificado como uma subcategoria das Tecnologias Cognitivas. Este emprega uma variedade de técnicas estatísticas, probabilísticas e de otimização que permitem computadores a aprender a detectar padrões difíceis de discernir a partir de dados passados dos parâmetros analisados. MATEUS, F. M. Q.; MENDONÇA, M. C. Machine learning na melhoria de processos internos: estudos de caso na indústria de varejo brasileira. 2020. 106 fl. Projeto de Graduação (Bacharel em Engenharia) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020, p.36.

329 "Um dado, em si, não é perigoso ou discriminatório - mas o uso que dele se faz, pode sê-lo". DONEDA, 2021, p.162.

330 Art. 12, LGPD. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais. BRASIL, op. cit., 2018.

A anonimização envolve a remoção ou alteração de informações que permitem uma identificação direta ou indireta de um indivíduo[331]. No entanto, o grau de identificação que precisa ser removido para que um dado seja considerado anonimizado pode apresentar variações conforme a situação. Há uma clara divergência quanto a forma de condução do processo de anonimização de dados pessoais. Enquanto uma corrente afirma que a remoção de identificadores diretos é suficiente, outra defende que informações adicionais devem ser modificadas ou removidas para garantir a não identificabilidade[332].

A definição de anonimização está diretamente relacionada ao risco de reidentificação dos dados. O processo para ser bem-sucedido, deve ser capaz de reduzir o risco de reidentificar um indivíduo, mesmo combinando dados com outras fontes. No entanto, não há uma definição específica do nível de risco aceitável ou das técnicas que devem ser aplicadas para alcançar esse objetivo, o que pode levar a interpretações divergentes. Ocorre que na prática, o contexto e os dados agregados podem alterar a visão quanto a anonimização. Neste caso, é importante mencionar o exemplo dos dados pessoais sensíveis, que por suas características também pode afetar a abordagem de anonimização, considerando a sensibilidade das informações envolvidas.

As possibilidades de interpretações divergentes no texto da LGPD também alcançam a definição de consentimento, levando a interpretações variadas na prática. Embora a LGPD forneça uma definição geral de consentimento[333], sua aplicação específica em diferentes contextos pode ser influenciada por aspectos como o requisito de informação, segundo o qual informações claras e compreensíveis sobre o tratamento de seus dados deverão ser repassadas para seus titulares. Porém, imediatamente emerge o questionamento acerca de quais informações poderiam ser consideradas suficientes e claras para o cidadão comum.

---

331 A anonimização de dados é o processo que permite tornar o dado pessoal em anônimo. O procedimento tem por objeto não ser possível a reversão da identificação do titular dos dados pessoais tendo como base as informações anonimizadas. O esforço é realizado para que haja a quebra do vínculo entre o dado e seu titular. DONEDA, op. cit., 2021, p. 44.

332 Com variações de intensidade tem-se um método cujo objetivo é gerenciar a identificabilidade de uma base de dados. Conforme as características de cada dado e a percepção de eles estarem inseridos em uma gama de informações a análise deve ser orientada. Logo, não há um método ou uma combinação perfeita que parametrize o processo de anonimização. Isso posto, é preciso analisar especificamente como este procedimento deve ser empreendido para que os titulares dos dados anonimizados não sejam reidentificados. BIONI, B. R. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos–Direito digital e proteção de dados pessoais, São Paulo, ano 21, n. 53, 2020, p. 71. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimiza%C3%A7%C3%A3o_e_dado.pdf. Acesso em: 12 jul. 2023.

333 Art. 5º, XII, LGPD - Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. BRASIL, op. cit, 2018.

Outro ponto a considerar, é a forma pela qual o consentimento para tratamento de dados deve ser efetivado. A LGPD não especifica se o consentimento deve ser expresso, por meio de declaração verbal ou escrita, ou se o consentimento implícito será suficiente, remetendo apenas ao fato de que este deve ser inequívoco[334]. Logo, sua interpretação pode apresentar variações. Em alguns casos, o consentimento explícito pode ser considerado necessário, enquanto em outros, o consentimento tácito pode ser aceito, desde que cumpra os requisitos de informação. Além disso, as finalidades específicas do tratamento de dados podem afetar a forma como o consentimento é interpretado e implementado.

Ainda que a intenção tenha sido propor definições abrangentes, o resultado acabou por criar linhas genéricas, que não abordam especificamente determinados contextos ou setores. A falta de especificidade e detalhamento em certas áreas da lei, bem como à complexidade e diversidade dos cenários de aplicação da LGPD, pode resultar em interpretações divergentes por parte das organizações, profissionais da área jurídica e até mesmo das autoridades reguladoras, enfraquecendo assim, a consistência e a eficácia da proteção de dados.

Aclarar estes pontos obscuros e apresentar uma interpretação mais consistente destes conceitos e regras para concretizar a proteção de dados no Brasil, é apenas um dos desafios enfrentados pelo Poder Público no cenário da LGPD. Os primeiros anos da lei trouxeram avanços expressivos, mas também, a visão de vulnerabilidades que se destacam especialmente quando oriundas da utilização de novas tecnologias nos serviços públicos e privados de saúde. Uma matéria que merece especial atenção em virtude do tipo de informação compartilhada, que objeto de reflexão no tópico a seguir.

5.3 Vulnerabilidades da utilização de novas tecnologias nos serviços público e privado de saúde face a necessidade da proteção de dados pessoais

O compartilhamento de informações se tornou um processo comum para o cidadão, que constantemente é chamado a declarar seus hábitos, preferências e características, tornando seus dados pessoais públicos e facilmente acessíveis. No setor de saúde

334 Art. 7º, LGPD - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular. Idem.

onde as tecnologias ganham cada vez mais espaço, a questão se agrava considerando a especificidade das informações e seus impactos sociais.

A vulnerabilidade das informações transmitidas entre os diferentes entes do processo de atendimento, apresentam um caráter pessoal e privado, contendo pontos chaves da vida íntima do indivíduo. São dados que revelam condições de saúde física e mental, detalhando pré-disposições, sintomas, ou enfermidades, e por isso, tem um considerável potencial lesivo para a vida de seus titulares e familiares mais próximos.

Ao tempo em que beneficiou diretamente a área da saúde, ao estabelecer a necessidade de consentimento dos usuários, proteção dos dados por terceiros por meio de criptografia, indicação de instrumentos de segurança e transparência para usuários, e a prerrogativa de corrigir, atualizar ou modificar os dados, a LGPD firmou importantes pontos de segurança para esta modalidade de dados sensíveis.

A segurança de dados, é sem dúvidas um grande desafio para as instituições de saúde. O receio de vazamentos de dados pessoais é uma preocupação legítima, mediante as inúmeras possibilidades de prejuízo ao titular das informações. A utilização para fins indevidos como comercialização, construção de perfis comportamentais[335], distorção de pesquisas e opinião pública, além de outras práticas ilícitas, são cada vez mais comuns.

Outra preocupação é a questão da vigilância. Na sociedade da informação é presente o receio do controle em massa dos cidadãos por parte do Poder Público, que sem dúvidas, possui o maior acervo de dados e informação de seus cidadãos. Trata-se de dados oriundos dos mais diversos órgãos e departamentos públicos, dentre os quais se destaca a base de dados do SUS[336].

---

335 Com o surgimento do *Big Data*, tornou-se possível coletar, armazenar e analisar grandes quantidades de dados de forma rápida e eficiente. A prática da análise comportamental pessoal (também conhecida como criação de perfil) é valorizada por seus 3 Vs (volume, velocidade e variedade). Volume: O grande volume de dados de saúde gerados diariamente permite a identificação de padrões comportamentais e de saúde, mas também aumenta o risco de privacidade e abuso. Rapidez: A coleta e processamento de dados ocorre em tempo real, permitindo que comportamentos comportamentais sejam criados em tempo hábil. Essa velocidade abre oportunidades de customização e agilidade na tomada de decisões. Diversidade: diversas fontes permitem informações detalhadas sobre os perfis individuais, fornecendo informações sobre seu comportamento, estilo de vida e saúde. No entanto, a combinação desses diferentes tipos de dados aumenta os desafios em termos de integração, qualidade e interpretação adequada, além de apresentar questões éticas sobre consentimento informado e anonimização adequada. OLIVEIRA, C. E. G. Credit scoring e big data no regime jurídico brasileiro. *In*: FERNANDES, R. V. C.; COSTA, H. A.; CARVALHO, A. G. P. (coord.). Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia – 2017. Belo Horizonte: Fórum, 2018, p. 223-240, p. 224.

336 Entre 2018 e 2019 surgiram diversas notícias de que informações pessoais de servidores públicos (contracheques, CPF e comprovantes de residência, por exemplo) eram acessadas por terceiros para fraudar empréstimos de até R$500 mil. Para isso, utilizavam dados do Sistema de Gestão de Pessoas (Sigepe), administrado pelo atual Ministério da Economia (antigo MPDG). A investigação está em curso pela Polícia Civil do Distrito Federal revelou grupo que fraudava empréstimos de até R$ 500 mil com dados de servidores federais no DF;

Os dados trabalhados em ferramentas digitais são em fato, preciosos aliados para otimizar processos, gerar ações mais assertivas e auxiliar a tomada de decisões, tanto no setor público quanto privado. Porém, os instrumentos tecnológicos são passíveis de gerar erros, bem como reproduzir falhas históricas. Algoritmos ou modelos podem ser alimentados com dados históricos que contêm desigualdades sistemáticas[337], resultando na chamada "discriminação estatística[338]" na elaboração de ações afirmativas pelo Poder Público ou influenciando comportamentos através das mídias privadas.

Como consequência da discriminação estatística, certos grupos receberiam tratamentos diferenciados em razão de determinados atributos, podendo gerar riscos de discriminação e estigmatização unicamente em razão de um resultado probabilístico[339]. Este seria o caso se por exemplo, um algoritmo de processamento de máquina realizasse a análise de dados de empréstimos bancários e viesse a identificar que pessoas de uma determinada faixa etária apresentam uma taxa de inadimplência mais alta quando comparadas as outras faixas previstas, e viesse a concluir erroneamente que todos os indivíduos nessa faixa etária são de alto risco de crédito.

Assim, a estatística ocorre quando um indivíduo é tratado com base em características estatísticas associadas a um grupo, independentemente de suas características ou circunstâncias individuais. Isso pode levar a violação de princípios éticos, decisões injustas e desiguais, perpetuando desigualdades[340] existentes na sociedade. Logo, é

três foram presos. MARQUES, M. Grupo fraudava empréstimos de até R$ 500 mil com dados de servidores federais no DF; três foram presos. G1, São Paulo, 2019. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/01/09/grupo-fraudava-emprestimos-de-ate-r-500-mil-com-dados-de-servidores-federais-no-df-tres-foram-presos.ghtml. Acesso em: 29 mar. 2023.

337 Ocorre quando algoritmos ou modelos estatísticos usados em processos de tomada de decisão tratam indivíduos de forma desigual com base em características estatísticas associadas a um determinado grupo. REQUIÃO, M.; COSTA, D. C. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, Rio de Janeiro, a. 11, n. 3, 2022. Disponível em: http://civilistica.com/discriminacaoalgoritmica/. Acesso em: 19 maio 2023.

338 A disponibilidade de big data, que nos permite aprender muito mais sobre correlações – embora não necessariamente sobre causalidade – cria oportunidades para discriminação estatística e novos perigos de seu uso. Questões relacionadas surgem do desenvolvimento do aprendizado de máquina – computadores treinados em dados históricos desenvolverão algoritmos que refletem padrões passados de seleção que podem não ser mais apropriados ou aceitáveis. Mesmo que o uso explícito de informações como gênero ou raça seja proibido, os algoritmos podem ter essa consequência – sem intenção consciente de tal discriminação por parte de qualquer pessoa. KAY, J.; KING, M. Radical Uncertainty. Decision-making beyond the numbers. New York: W.W. Norton & Company, 2020, p. 208.

339 A análise estatística busca obter a mesma informação por meio da coleta de dados de apenas uma fração relevante de toda a população. Com uma amostra representativa, metodologia adequada e análise pautada pelo constructo que se pretende descrever, os resultados podem ser considerados para o todo. FREEDMAN, D.; PISANI, R.; PURVES, R. Statistics. 4. ed. New York: W. W. Norton & Company, 2007, p. 223.

340 Logo, os dados pessoais em certas circunstâncias podem ocasionar discriminação ou mesmo controle, diminuindo as liberdades de escolha do indivíduo. DONEDA, D. Privacidade e transparência no acesso à informação pública. *In*: MEZZAROBA, O.; GALINDO, F. Democracia eletrônica. Zaragoza: Prensas Universitarias de Zaragoza, 2010. p.179-216, p. 191.

essencial adotar abordagens regulatórias, técnicas e éticas para minimizar a estatística e garantir que as decisões sejam tomadas com base em estimativas individuais, considerando as características e necessidades únicas de cada indivíduo.

Neste quadro, é necessário retomar a preocupação com os dados de saúde. Devido a sua natureza pessoal e extremamente íntima, os dados sensíveis de saúde apresentam alto potencial discriminatório e podem ser instrumento de diversas formas de violação de direitos. Tendo por características organização, alto quantitativo e ao mesmo tempo defesa permeável, ferramentas de segurança menos efetivas e equipes despreparadas para identificar ameaças, não por acaso os dados de saúde tem sido alvos preferenciais para ataques cibernéticos.

Conforme relatório da *International Business Machines* - IBM intitulado "*Cost of a Data Breach Report 2021*", considerado referência em cibersegurança, houve um aumento do custo médio total por violação de dados no setor da saúde de US$ 7,13 milhões no ano de 2020 para US$ 9,23 milhões no ano de 2021, o que configura um aumento de 29,5%. Mediante um número tão expressivo, o setor de saúde desponta como o segmento com maior índice de ataques digitais. Segundo o relatório dentre os fatores que contribuem para o aumento dos custos de segurança, se destacam as falhas de conformidade[341].

No cenário brasileiro, pesquisas apontam para o aumento em 37% das violações envolvendo dados de saúde no terceiro trimestre de 2022, em relação ao mesmo período do ano anterior[342]. O relatório gerado pela empesa *Check Point Software* especializada em cibersegurança, revela ainda um tipo preferencial de ataque, por meio de *ransomware*[343], nas invasões em sistemas de organizações do setor de saúde. Segundo a pesquisa, 1 em cada 42 instituições foi afetada por esse método, resultando em um aumento de 5% em relação a 2021.

Esses dados preocupantes alertam para o fato de que as indicações de segurança dispostas na LGPD, bem como nas demais políticas públicas de saúde digital não estão se concretizando conforme o planejado. A implementação dos processos de proteção de dados afeta diferentes momentos do ciclo de atendimento e tratamento

341 Para aprofundamento de dados técnicos, recomenda a leitura do relatório disponível em: https://www.ibm.com/downloads/cas/OJDVQGRY#:~:text=The%20average%20per%20record%20(per,per%20record%20cost%20was%20%24141.

342 Relatório anual. UNITED STATES. Annual report pursuant to section 13 or 15(d) of the securities exchange act of 1934. Washington D.C.: Securities and Exchange Commission, 2022. Disponível em: https://www.checkpoint.com/downloads/investor/2021-CHKP-form-20F.pdf. Acesso em: 15 jun. 2022.

343 O *ransomware* é uma forma de *malware* que tem como objetivo bloquear o acesso a um sistema ou arquivos do usuário e requer um pagamento, geralmente em criptomoedas, para restaurar o acesso.

do paciente usuário dos sistemas de saúde. Para uma prover uma efetiva segurança aos dados sensíveis de saúde é necessária uma adequação global de todos os agentes envolvidos, sejam estes da rede pública ou privada, ao compliance exigido pela LGPD.

Contudo, uma adequação satisfatória exige a solução para problemas de segurança que se estendem desde a falta de criptografia até senhas fracas ou desatualizadas. Além disso, a falta de treinamento dos profissionais de saúde em segurança cibernética e ausência de atualizações de software, bem como a falta de protocolos claros e seguros para o compartilhamento de dados entre as partes interessadas pode comprometer a privacidade e a confidencialidade dos pacientes, são exemplos de vulnerabilidades enfrentadas nos serviços públicos e privados de saúde.

Tais dificuldades precisam ser consideradas quando da formulação de políticas públicas. Uma vez que se avança a largos passos nas tecnologias aplicadas aos serviços de saúde, resta clara a necessidade de uma regulamentação explícita quanto ao uso ético dos dados, informações e ferramentas tecnológicas no setor.

A LGPD é uma norma de caráter geral que se aplica a todos os setores, mas a prática comprova que a área da saúde tem características e desafios específicos que exigem abordagens regulatórias especiais. Assim, a elaboração de regulamentos específicos para a proteção de dados pessoais na área da saúde é essencial para nortear questões específicas e mitigar vulnerabilidades dos sistemas de saúde público e privado.

Outro ponto importante é o reconhecimento da possibilidade do surgimento de novas problemáticas e desdobramentos para as questões saúde digital no Brasil. Em um cenário em constante evolução de novas tecnologias, é necessário revisar regularmente os requisitos técnicos e medidas de segurança para a proteção dos dados pessoais sensíveis de saúde para assegurar que eles sejam adequados para enfrentar as vulnerabilidades emergentes.

Merece destaque neste caso, a ampla necessidade de conscientização e treinamento dos profissionais de saúde e organizações. Cabe aos agentes do setor a conhecer as instituições da LGPD, bem como seu direcionamento para lidar com os dados pessoais dos pacientes. Neste sentido, é fundamental a realização de ações educativas e programas de conscientização para contribuir para a adoção de boas práticas e redução de vulnerabilidades, conforme proposto na ESD28.

Enquanto um caminho mais ágil para neutralizar os mencionados pontos vulneráveis dos sistemas de saúde, tem-se o já mencionado processo de integração de dados, traduzido na capacidade que os sistemas apresentam para operar de maneira integrada.

A criação de padrões e concentração de informações[344] pode ser um grande aliado no fortalecimento da segurança das bases de dados de saúde. Um bom exemplo é o que tem sido praticado com os prontuários eletrônicos, que hoje centralizam exames laboratoriais, históricos dos pacientes, entre outros, em uma única plataforma, dando acesso em tempo real aos médicos, profissionais de saúde e pacientes.

Da mesma forma, acelerar o processo de integração nos sistemas de gestão conduzirá a uma maior organização financeira, fiscal e técnica. A intenção é investir na otimização de processos administrativos como a automação da emissão de documentos, notas fiscais, a produção de relatórios gerenciais para apoiar a tomada de decisão das instituições, entre outros benefícios.

Assim, a integração efetiva dos sistemas de saúde, amplamente discutida na ESD28 é apontada como um passo importante para que se amplie as proteções de dados sensíveis na saúde. Acredita-se que ao padronizar e otimizar a comunicação das informações, haveria meio de estabelecer uma maior segurança para todos os envolvidos nos sistemas de saúde. Contudo, antes de se falar em soluções definitivas para as vulnerabilidades verificadas a partir da utilização de novas tecnologias nos serviços público e privado de saúde, é importante considerar onde residem as principais deficiências na gestão de dados no setor.

5.4 Deficiências na gestão de dados no setor de saúde

A gestão de dados de saúde é uma área crucial para garantir a qualidade dos serviços prestados à população e promover a tomada de decisões embasadas em evidências. No entanto, é importante destacar que existem diversas deficiências nesse processo, que comprometem a segurança, a confidencialidade e a integridade dos dados. Contudo, antes de buscar identificar os principais obstáculos práticos presentes na gestão de dados na saúde, é importante considerar certos pontos no contexto do setor face o processo de implementação das diretrizes propostas pela LGPD e demais políticas de saúde digital.

Enquanto países da União Europeia, como a própria UE, e nações mais próximas ao Brasil, como Uruguai e Argentina, já avançam em suas discussões e implementações

344 Outro benefício da interoperabilidade de dados é que as informações estarão no padrão internacional HL7 FHIR (Fast Healthcare Interoperability Resource), utilizado para transferência de dados administrativos e clínicos do setor de saúde, que não são vulneráveis segundo o relatório "Hacking FHIR: Hacking and Securing FHIR APIs". Bruno Toldo, Diretor de Informações Médicas, Infor.

de regulamentações de proteção de dados[345], o Brasil enfrenta desafios próprios para atingir níveis de conformidade e proteção adequados e consolidar sua normativa. Características geográficas, sociais e políticas do Brasil têm exercido uma influência significativa e, em muitos casos, chegam a dificultar o processo de adequação à LGPD.

Conforme o dispõe o artigo 3º da LGPD, a Lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional. Além disso, a norma também deixa explícito seu caráter extraterritorial, segundo o qual pode gerar efeitos âmbito internacional, em dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduo no território nacional, ou que se encontrassem no Brasil.[346]

A vasta extensão territorial do Brasil é um fator que certamente impacta na implementação da LGPD, tornando a tarefa ainda mais complexa[347]. As dimensões continentais implicam em uma grande diversidade de realidades regionais e dificultam o monitoramento das práticas de tratamento de dados em todo o país, exigindo uma coordenação e investimentos logísticos adicionais. Assim, o cumprimento das disposições referentes à vigilância e monitoramento das práticas de tratamento de dados se torna uma empreitada complexa na qual as autoridades responsáveis pela aplicação da lei precisam coordenar esforços em diferentes regiões do país, o que exige logística, recursos e planejamento estratégico adequado.

No mesmo sentido, é preciso observar a questão das disparidades socioeconômicas verificadas na sociedade brasileira. Enquanto empresas de grande porte e multinacionais dispõem de recursos materiais e intelectuais para se adequarem à LGPD nos prazos

345 Conforme a orientação da Diretiva 95/46/EC, a Argentina adequou-se às regras europeias em 30/6/03 e o Uruguai em 21/8/12. Ambos os países fazem parte da convenção 108, assim como México. EUROPA, op. cit., 1995

346 LGPD, artigo 3: Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional. II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. BRASIL, op. cit., 2018.

347 O Brasil tem dimensão continental. É um país onde "cabe" a cidade de Altamira/PA, com seus cerca de 159 mil Km², "cabe" Santa Cruz de Minas/MG, com seus poucos 3,5 mil km², e "cabe" mais 5.568 municípios e o Distrito Federal. Se por um lado se tem muita riqueza e diversidade cultural, social, econômica, ambiental, de outro restam muitas diferenças e desafios para aplicar regras limitadas.

previstos, a realidade de um significativo contingente de pequenas e médias empresas é oposta.

Os setores de finanças, seguros e serviços correlatos são os pioneiros na adequação à LGPD, com 37,5% das empresas do setor considerando o atendimento entre 81% e 100% das exigências legais. Dois fatores parecem ter sido determinantes para tal pioneirismo: o espírito de inovação alimentado com as *fintechs*[348], bem como ao aumento de casos de golpes no setor no Brasil, que medidas de segurança e privacidade mais sólidas para garantir a fidelização de seus clientes. Por outro lado, as empresas do setor de serviços têm ficado para trás em termos de adequação à LGPD, com apenas 45% das empresas desse setor atendendo apenas de 0 a 20% dos requisitos legais[349].

Estes dados fazem sentido, quando se observa quantidade expressiva de empresas de pequeno e médio porte no setor de prestação de serviços no Brasil. Empresários que se encontram dentro desta classificação enfrentam dificuldades financeiras e técnicas para implementar as medidas necessárias de proteção de dados, arriscando a segurança dos dados que manuseiam e se expondo ao enquadramento das sanções previstas pela LGPD[350]. Para estas organizações, além da problemática do fluxo de caixa necessário para realizar os procedimentos de adequação à LGPD, se verificam ainda celeumas como ausência de mão-de-obra especializada, resistência cultural, o desconhecimento dos conceitos legais e insegurança quanto as sanções.

Como um caminho para evitar que essas empresas viessem a sucumbir as penalidades da Lei, a Autoridade Nacional de Proteção de Dados – ANPD publicou a Resolução

348 *FinTech* é um termo que surgiu da união das palavras em inglês financial e technology e refere-se ao uso da tecnologia para entregar soluções financeiras. ARNER, D. W.; BARBERIS, J.; BUCKLEY, R. P. The evolution of Fintech: a new post-crisis paradigm. Georgetown Journal of International Law, [*S.l.*], v. 47, p. 1271, 2015, p. 1271. Disponível em:
https://www.researchgate.net/publication/313365410_The_Evolution_of_Fintech_A_New_Post-Crisis_Paradigm. Acesso em: 22 jul.

349 A Pesquisa Serasa da *Experian* constatou que 326.290 brasileiros foram alvo de tentativas de golpe somente em fevereiro deste ano. Os setores mais visados pelos golpistas são o setor bancário e de cartões e o setor financeiro. A cada 7 segundos, uma tentativa de fraude é registrada no Brasil; saiba se proteger. JULIÃO, F. A cada 7 segundos, uma tentativa de fraude é registrada no Brasil; saiba se proteger. **CNN Brasil**, São Paulo, 2022. Disponível em: https://www.cnnbrasil.com.br/economia/a-cada-7-segundos-uma-tentativa-de-fraude-e-registrada-no-brasil-saiba-seproteger/#:~:text=Um%20levantamento%20da%20Serasa%20Experian,4%2C9%25%20nos%20casos. Acesso em: 22 jul. 2022.

350 Os dados da pesquisa Capterra mostram que apenas três em cada 10 empresas se consideram totalmente aderentes à LGPD. Como seria de esperar, a porcentagem de empresas que se definem como "plenamente aptas" foi maior entre as grandes empresas (46% nos grupos de 51 a 100 trabalhadores e 40% nos grupos de 101 a 250 trabalhadores) e mais baixa nas PME com menos de 50 trabalhadores. Para este estudo da Capterra, foram entrevistados 305 profissionais envolvidos na coordenação ou gestão de PMEs entre 16 e 23 de junho de 2021. GAVA, M. LGPD para PME: minoria está totalmente adequada à legislação. Capterra, 2021. Disponível em: https://www.capterra.com.br/blog/2153/lgpd-pme. Acesso em: 22 dez. 2022.

CD/ANPD N° 2/2022[351], concedendo flexibilizações à aplicação da LGPD para agentes de tratamento de pequeno porte, como startups e microempresas. O texto da Resolução deixa claro que as organizações que ali se enquadram seguem vinculadas ao cumprimento da LGPD, contudo, contam com benefícios, como a concessão de prazo dobrado para atendimentos de solicitações dos titulares dos dados e a não necessidade de indicar um encarregado pelo tratamento de dados pessoais, mediante a disponibilização de um canal de comunicação alternativo com os titulares dos dados. Esta flexibilização se mostra acertada, repercutindo no sentido de ampliar a conscientização quanto a relevância da questão da proteção dos dados pessoais e ao tempo que evita efeitos negativo que uma postura meramente sancionatória poderia gerar para a economia do país.

Em fato, o Brasil ainda está em processo de desenvolvimento de uma cultura de proteção de dados e privacidade. A educação e conscientização da população e dos profissionais envolvidos no tratamento de dados são essenciais para a compreensão dos princípios e diretrizes da LGPD. Da mesma forma, espera-se que empresas e organizações do setor público e privado conheçam e incorporem os mencionados procedimentos de proteção. Mesmo com o decurso de três anos da vigência da LGPD, muitas organizações não se encontram totalmente cientes das obrigações impostas pela lei, o que resulta em atrasos e inadequações no processo de adaptação.

É preciso investir na criação de uma cultura nacional de gerenciamento de dados, de modo a assegurar o cumprimento de todas as medidas de segurança informativa e operacional exigidas. No Brasil a proteção de dados pessoais ainda não atingiu o status esperado como prioridade nas organizações, demandando um trabalho constante que vai desde exemplos e boas práticas a partir da gestão, até cursos, capacitações e outras ações que tenham por objetivo de envolver todos os funcionários e prestadores que de alguma forma lidam com informações pessoais.

Outra peculiaridade brasileira diz respeito ao fato de que uma parcela significativa da população não estar conectada à internet. Enquanto em áreas urbanas e desenvolvidas, a infraestrutura de tecnologia e acesso à internet pode ser robusta, em áreas rurais e comunidades menos favorecidas, a conectividade e o acesso a recursos tecnológicos são limitados. Há áreas rurais e comunidades carentes sem acesso à tecnologia e à rede.[352]

---

351 BRASIL. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília: Presidência da República, 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 27 jul. 2022.

352 Mais de 33 milhões de brasileiros não têm acesso à internet, diz pesquisa. Segundo estudo do Instituto Locomotiva e da consultoria PwC, 71% da população com mais de 16 anos não consegue usar a internet todos

Logo, não há como assegurar o conhecimento e o exercício dos direitos de privacidade por parte desses cidadãos. O Brasil ainda está caminhando para a construção de uma cultura sólida de proteção de dados e privacidade, que perpassa pela necessidade de educação e conscientização, não apenas de profissionais e empresas diretamente envolvidos no tratamento de dados, mas também da população como um todo para a compreensão dos princípios e diretrizes da LGPD.

Diante desse cenário, é previsível que o setor de saúde demonstre dificuldades em materializar o planejamento de saúde digital, bem como apresentar uma adequação satisfatória à LGPD. Caracterizado pela necessidade de lidar com informações extremamente sensíveis e complexas, a esfera da saúde, apresenta demandas que incluem uma ampla gama de informações, com o manuseio de históricos médicos, diagnósticos, resultados de exames, tratamentos realizados, medicamentos prescritos, informações genéticas, entre outros dados que se relacionam intimamente com a vida privada e a identidade do indivíduo. Por isso, a necessidade urgente de um planejamento adequado e o fomento de uma cultura de proteção de dados.

5.4.1 Do baixo índice de planejamento, do enfraquecimento da ANPD e da ausência de uma cultura de proteção de dados

A complexidade dos dados de saúde por si só, apresenta desafios diferenciados para as instituições do sistema, que além de prestar serviços de qualidade aos usuários, lida com a difícil tarefa de implementar a visão de saúde digital apresentada pelo Poder Público e garantir a conformidade de seus processos com a LGPD. Como por exemplo dessas demandas, observa-se o exemplo da necessidade de consentimento específico para a coleta e tratamento de dados de saúde.

Conforme discutido nos capítulos iniciais, a LGPD exige que o tratamento de dados pessoais sensíveis de saúde seja realizado com base no consentimento livre, informado e inequívoco de seu titular. O obter o consentimento adequado pode ser mais desafiador devido à natureza sensível das informações e à necessidade de explicar claramente como esses dados serão utilizados. É preciso atentar que em muitos casos, por falta de conhecimento, nem profissionais, nem a população se mostram devidamente preparados para lidar com as informações e seus desdobramentos.

os dias. Grupo é formado principalmente por pessoas negras, que estão nas classes C, D e E, e que são menos escolarizadas. MAIS DE 33 MILHÕES de brasileiros não têm acesso à internet, diz pesquisa. G1 Portal, São Paulo, 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/03/21/mais-de-33-milhoes-de-brasileiros-nao-tem-acesso-a-internet-diz-pesquisa.ghtml. Acesso em: 14 fev. 2023.

Além disso, é preciso observar que quanto maior for a pessoalidade da informação, maior deverá ser a preocupação quanto a justificativa para sua utilização por parte da gestão de saúde pública. Conforme a LGPD, cabe aos profissionais de saúde o dever de informar o paciente sobre a necessidade de usar, compartilhar informações e buscar consentimento explícito[353]. Tal previsão, ao tempo em que representa uma importante linha de segurança para as organizações de saúde, na prática pode representar problemas de eficiência e flexibilidade na gestão[354].

Muito já se falou na definição de dados pessoais sensíveis disposta na LGPD[355], enquanto informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, dados genéticos, dados biométricos, entre outros. Muitas dessas categorias estão intimamente relacionadas à saúde e, portanto, medidas adicionais de proteção e cuidado no seu tratamento.

Neste sentido, é pertinente aprofundar na classificação dos dados, considerando dados relativos à saúde como dados pessoais relacionados associados a saúde física ou a saúde mental de uma pessoa, bem como aqueles oriundos da prestação de serviços médicos, que revelam informações sobre o seu estado de saúde. Já os dados genéticos são informações pessoais relativas a características genéticas herdadas ou adquiridas de uma pessoa que fornecem informações exclusivas sobre a fisiologia ou a saúde do paciente e que resultam, em particular, de uma análise de uma amostra biológica da pessoa física em questão. Por fim, tem-se os dados biométricos, enquanto dados pessoais resultantes de processamento técnico específico relacionados às características físicas, fisiológicas ou comportamentais de uma pessoa, que permitem ou confirmam a identificação única dessa pessoa física, como imagens faciais ou informações dactiloscópicas[356].

353 Artigo 7º, § 3º, LGPD: O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. BRASIL, op. cit, 2018.

354 "As razões de coleta, principalmente quando se tratarem de "dados sensíveis", devem ser objetivas e limitadas". MORAES, op. cit., 2008, p. 9.

355 Para os fins da LGPD, dados pessoais incluem informações sobre Pessoas singulares identificadas ou identificáveis (artigo 5.º I) e dados pessoais Sensibilidade refere-se a "origem racial ou étnica, crenças religiosas, opiniões filiação política, sindical ou organizacional de natureza religiosa, Filosofia ou política, dados sobre saúde ou sexo, dados genéticos ou biométricos, quando relativos a pessoa física" (art. 1º). art. 5º, II, LGPD. BRASIL, op. cit, 2018.

356 O RGPD destaca uma categoria especial de dados pessoais, que são mais conhecidos como "dados sensíveis", conforme indica o artigo 9.1: É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. Estes conceitos aparecem ainda no artigo 4.º, nº 13, 14 e 15 e considerandos 51 a 56 do RGPD. BRASIL, op. cit, 2018.

Ao tratar dados médicos de um paciente, a gestão de saúde lida com uma carga adicional para manter dados com informações de saúde, genéticas e biométricas em um padrão de proteção que atenda aos requisitos definidos pela LGPD. A condução correta do manuseio e tratamento desses dados demanda, antes de tudo, um bom planejamento. Mas na prática, o baixo índice de planejamento é uma fragilidade constante na gestão de dados de saúde, que dificulta a identificação e a correção de falhas e acaba por abrir espaço para ataques e acesso indevido aos dados.

Em muitos casos, se perde a oportunidade de otimizar processos e serviços, aproveitando o benefício efetivo das tecnologias disponíveis para o setor, frente a má utilização das estratégias e diretrizes para coleta, armazenamento, processamento e compartilhamento de dados. A ausência de um plano estratégico bem definido acaba por gerar lacunas na atribuição de responsabilidades, falta e desperdício de recursos e atrasos na implementação de medidas de segurança, ampliando vulnerabilidades que as Políticas de Saúde buscam corrigir[357].

Um bom planejamento é ponto crucial para promover a padronização nos sistemas de saúde e eliminar obstáculos para a concretização da integração ou interoperabilidade, compreendida como o compartilhamento seguro de informações entre diferentes entidades de saúde[358]. Uma linguagem homogênea, com a padronização, as informações podem ser lidas, interpretadas e utilizadas por diferentes sistemas sem perda de integridade, pode facilitar consideravelmente a implementação de tecnologias de saúde digital e ampliar resultados.

Formulários e protocolos de comunicação em um único padrão permitiriam uma integração mais fluida entre sistemas de saúde. Isso significa que diferentes entidades poderiam compartilhar dados de forma mais rápida e segura, facilitando a colaboração e a prestação de cuidados coordenados aos pacientes. Além disso, seria possível simplificar a migração de dados entre sistemas, facilitando a transição de uma entidade

357 Observe-se a denúncia de vazamento de dados da Unimed, noticiada em 2019 pelo site "Olhar Digital", baseado em informações passadas pelo grupo WhiteHat Brasil, que afirma que o banco de dados da companhia possui não apenas uma, mas várias falhas de segurança em inúmeras unidades da Unimed de todo o país. Os dados vazados incluem fichas cadastrais completas de pacientes (nome completo, CPF, nome da mãe, código beneficiário, e-mail e dados de dependentes), acessos a logins médicos, e-mails internos, imagens de problemas internos de centros de saúde, planilhas financeiras; além de dados sensíveis, como exames de pacientes, certidões de óbito e imagens de raio-x. Além desses dados, o WhiteHat Brasil ainda informou que o acesso completo ao banco de dados garante que qualquer um tenha possibilidade de alterá-los, incluindo ou excluindo qualquer informação que conste em documentos de pacientes. DADOS DE PACIENTES da Unimed é exposto na Internet. Allus, São Paulo, 2022. Disponível em: https://alus.com.br/dados-de-pacientes-da-unimed-e-exposto-na-internet/. Acesso em: 12 jan. 2023.

358 Um exemplo de padronização e cruzamento de base de dados que atingiu o objetivo de promover a melhoria da qualidade dos serviços públicos, facilitando o exercício de direitos fundamentais foi o "e-Social" - Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas.

de saúde para outra ou a adoção de novas tecnologias, o que reduziria esforços técnicos e financeiros. Sem mencionar que os profissionais de saúde passariam a ter acesso a um histórico mais completo e atualizado do paciente, o que permitiria a melhora da tomada de decisão clínica e auxilia no diagnóstico e tratamento mais eficaz.

As tecnologias aplicadas à saúde viabilizaram entre outros relevantes progressos a possibilidade de colaboração de profissionais da área, independente do fator geográfico. Porém, a transferência internacional de dados requer medidas adicionais de proteção, conforme estabelecido pela LGPD. O setor de saúde, por suas peculiaridades precisa de meios hábeis para assegurar que essas transferências sejam realizadas conforme as exigências legais.

A transferência internacional de dados pessoais é caracterizada pela existência de um fluxo de dados pessoais entre o Brasil e países terceiros. Conforme o artigo 5º, inciso XV da LGPD, trata-se da "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro". Nestes casos, é exigido que o país receptor desses dados forneça a garantia de segurança aos titulares dos dados pessoais no mesmo nível das suas legislações nacionais.

Este conceito é complementado pelo artigo nº 33 da Lei que indica as situações de autorização de transferência internacional de dados pessoais, destacando em seu inciso I a possibilidade de tráfego de dados entre os países ou organismos internacionais que proporcionem grau de proteção adequado ao previsto na legislação nacional, conforme avaliação exclusiva realizada pela Autoridade Nacional de Proteção de Dados - ANPD.[359] Adotando posicionamento similar ao que se encontra do RGPD,

359 Artigo 33, LGPD. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais ;c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

considera-se que só será legal a transferência internacional quando o país terceiro for adequado conforme os fins de garantia de proteção e segurança dos dados pessoais.

O RGPD, em seu artigo nº 45, permite sem autorização específica a realização de uma transferência internacional de dados para um país terceiro quando este puder assegurar um nível de proteção de dados compatível com o oferecido pela legislação europeia[360]. O nível de proteção de dados deve considerar, entre outros fatores, o respeito pelos direitos humanos e às liberdades fundamentais, a legislação em vigor, tanto em segurança pública, defesa, segurança nacional e direito penal, e as regras de proteção de dados pessoais, e ainda existência de uma Autoridade de Proteção de Dados efetivamente independente.

Sobre o tema, a já mencionada decisão no contexto europeu que tratou da questão da licitude da transferência internacional de dados pessoais, oriunda do Tribunal Nacional da Alemanha, na cidade de Colônia, que considerou ilegal a transferência internacional de dados para os EUA, via *Google Analytics*[361]. Na ocasião, o tribunal reconheceu a violação da legislação europeia de proteção de dados por meio de transferências de dados pessoais para fins de análise e marketing, uma vez que os titulares tinham os seus dados pessoais, como o endereço de IP e informações sobre navegador, transmitidos aos servidores do Google em território americano. O caso ganhou notoriedade por apresentar uma decisão pioneira na qual se declarou a ilegalidade de uma transferência internacional de dados aos Estados Unidos.

Situação mais recente foi verificada em maio de 2023, quando o *European Data Protection Board* - EDPB, autoridade europeia independente e responsável por promover a cooperação entre as demais autoridades dos Estados Membros da UE, determinou uma multa de 1,2 bilhão de euros e a suspensão de todas as transferências futuras a ser realizadas pelo Grupo aos EUA. A postura das autoridades europeias quanto a matéria deixa clara a necessidade de garantia de proteção de dados pessoais aos seus cidadãos.

No Brasil, cabe a ANPD a responsabilidade de definir diretrizes e regulamentações relacionadas às transferências internacionais. E seguindo a tendência, deve se espelhar em decisões judiciais emitidas pelas autoridades de proteção de dados da UE para

360 A Comissão da UE considera um país, região ou setor de um país terceiro adequado se puder ser demonstrado que a segurança jurídica e a uniformidade da proteção de dados são garantidas, tendo em conta o nível de proteção esperado da União Europeia. RGPD, op. cit., nº 45.

361 O *Google Analytics* é uma ferramenta de marketing digital bastante utilizada ao redor do mundo, por meio da qual é possível, através da identificação de códigos de rastreamento, a obtenção de relatórios de padrões de consumo de usuários de sites e aplicativos.

efetivar a regulamentação dos artigos da LGPD que versam sobre o grau de proteção exigido aos países e organismos internacionais como condicionante para serem considerados aptos a receberem dados pessoais provenientes do Brasil.[362]

A ANPD desempenha um papel central na efetivação da proteção de dados, e sua atuação é descrita em diversos artigos da LGPD. Contudo, a ideia de uma ANPD independente e autônoma, atuante no sistema de proteção de dados não se concretizou conforme o esperado, restando paralisada por entraves técnicos e jurídicos, situação que afeta diretamente suas características e aplicação. A tabela abaixo facilita a compreensão do percurso realizado na efetivação da ANPD.

Quadro 3 - Panorama da efetivação da ANPD

Base Jurídica da ANPD	ano	Normas Principais
Lei nº 13.709	2018	Lei que estabelece as regras gerais para o tratamento de dados pessoais e cria a ANPD.
Medida Provisória nº 869	2018	Cria a Autoridade Nacional de Proteção de Dados
Lei nº 13.853	2019	Altera dispositivos da LGPD e define uma estrutura da ANPD.
Decreto nº 10.474	2020	Regulamenta a composição, competências e funcionamento da ANPD.
Lei nº 14.010/2020 (Em decorrência da pandemia de COVID-19)	2020	Dispõe sobre o regime jurídico
Decreto nº 10.975	2022	Altera o Decreto nº 10.474, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e papéis de confiança.
Decreto nº 11.202	2022	Altera o Decreto nº 10.474, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados, e remaneja e transforma cargos em comissão e funções de confiança, e altera o Decreto nº 9.660.

Fonte: Elaborado pela autora.

A ausência de independência e autonomia, neste caso, abre margem para perigosas intervenções da gestão. A ANPD foi criada pela Medida Provisória nº 869, de 2018, convertida na Lei nº 13.853, de 08 de julho de 2019, que alterou a Lei Geral de Proteção de Dados – LGPD e passou a funcionar efetivamente em de novembro de 2020. Porém, no ano de 2022, a Medida Provisória nº 1.124, de 13 de junho de 2022, posteriormente convertida na Lei nº 14.460, de 25 de outubro de 2022, converteu a ANPD em autarquia de natureza especial[363].

362 Os artigos mencionados são 33, 34 e 35 da LGPD. BRASIL, op. cit., 2018.

363 BRASIL. lei nº 14.460, de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nº s 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Art. 9º Ficam revogados: I - os §§ 1º, 2º e 3º do art. 55-A, o art. 55-B e o inciso V do caput do art. 55-C da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as

Contrariando a proposta no projeto de lei aprovado por unanimidade no Congresso Nacional, a ANPD passou a pertencer à Administração Pública direta e está subordinada à presidência da República, perdendo muito de sua independência institucional, funcional e financeira à ANPD.[364] Recentemente, em janeiro de 2023, foi publicado o Decreto nº 11.401, passando a vincular a ANPD ao Ministério da Justiça e Segurança Pública. Essa nova conjuntura, fortalece a possibilidade de interferência direta dos chefes do Poder Executivo, tais como o presidente da República e o ministro chefe da Casa Civil, enquanto a ANPD deveria ser livre e autônoma para no exercício de suas funções, poder agir face ao Poder Público, enquanto sua posição como agente de tratamento de dados.

É essencial que as regras da LGPD, bem como os preceitos contidos nas demais legislações sobre privacidade e proteção de dados pessoais venham a alcançar o Poder Público. Dentre todos os agentes de tratamento de dados pessoais, certamente é o que detém maior força, tanto pelos recursos tecnológicos como em razão da quantidade de dados diariamente coletados e tratados. Afinal, o conhecimento detalhado sobre a população é pressuposto para uma administração pública eficiente.[365]

Não há sentido em excluir o Poder Público das previsões da LGPD, impondo regras apenas a uma parcela dos agentes de tratamento de dados da esfera privada. A proteção de dados, especialmente dos dados sensíveis deve ser outorgada a todo cidadão, independente do tratamento ocorrer na esfera pública ou privada. Aceitar tal distinção, despertaria dúvidas e desconfiança quanto a real possibilidade de proteção ao direito à privacidade dos brasileiros.

Como visto não são poucos os desafios a serem enfrentados nos próximos anos no processo de consolidação da saúde digital. Para além das situações mencionadas neste tópico, ainda é preciso atentar tanto no setor público, quanto no setor privado, para a rápida defasagem da infraestrutura tecnológicas, bem como as deficiências no quadro técnico.

Muitas instituições de saúde possuem infraestruturas tecnológicas mais antigas, o que pode dificultar a implementação de soluções modernas e seguras em conformidade com a LGPD. Essa defasagem pode ser atribuída a diversos fatores, como a evolução acelerada da tecnologia, o aumento da demanda por serviços de saúde, questões

Leis nº s 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Diário Oficial da União, nº 3. Brasília: Presidência da República, 2022.

364 BIONI, op. cit., 2020b, p.83.

365 DONEDA, op. cit., 2021, p. 8.

orçamentárias e complexidade das regulamentações que envolvem o uso de dados pessoais no setor. Tanto a rede pública quanto a privada de saúde enfrentam dificuldades em acompanhar o ritmo das inovações tecnológicas no setor[366]. Na rede pública, os desafios são ainda mais acentuados devido à limitação de recursos e à complexidade de processos de aquisição e implementação de novas tecnologias.

A rápida evolução tecnológica torna necessário que as instituições de saúde se mantenham constantemente atualizadas para oferecer serviços de qualidade e competitivos. Mas a aquisição de novas tecnologias pode ser onerosa, especialmente para pequenas e médias clínicas e hospitais, demandando equipamentos, instalações especializadas e profissionais capacitados.

Conforme a ISO/IEC 27701:2019, controle 8.2.2[367], cabe a cada organização que opere enquanto agente de dados, assegurar que as pessoas sob o seu controle estejam cientes da definição de dados pessoais, estando aptas a reconhecê-los. Gestores e colaboradores devem ser informados quanto aos preceitos da LGPD e suas implicações na rotina da organização. Logo é preciso orientação expressa e incentivar o engajamento nas novas rotinas de trabalho.

A capacitação e atualização dos profissionais de saúde são cruciais para garantir que as tecnologias sejam utilizadas de forma eficaz e segura e acabam por configurar outra fragilidade do setor. Apenas profissionais qualificados são capazes de utilizar plenamente as ferramentas disponíveis, otimizando a prestação de cuidados e a experiência do paciente, de modo a atingir a utilização de forma segura e eficiente da tecnologia. Conforme as ESD28, a capacitação adequada pode reduzir os riscos de erros de interpretação e garantir que os dados de saúde sejam tratados de acordo

366 A portaria nº 2.510, de 19 de dezembro de 2005 instituiu a Comissão para Elaboração da Política de Gestão Tecnológica no âmbito do Sistema Único de Saúde - CPGT. Em seu artigo 3º, § 1º afirma que Considera-se tecnologias em saúde os medicamentos, equipamentos e procedimentos técnicos, os sistemas organizacionais, informacionais, educacionais e de suporte e os programas e protocolos assistenciais por meio dos quais a atenção e os cuidados com a saúde são prestados à população. BRASIL. Portaria nº 2.510, de 19 de dezembro de 2005. Institui Comissão para Elaboração da Política de Gestão Tecnológica no âmbito do Sistema Único de Saúde - CPGT. Brasília: Ministério da Saúde.

367 A ISO/IEC 27701:2019 – *Security techniques – Extension to* ISO/IEC 27001 *and* ISO/IEC 27002 *for privacy information management – Requirements and Guidelines* especifica os requisitos e fornece a orientação para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Informações sobre Privacidade (*Privacy Information Management System – PIMS*) na forma de uma extensão da ISO/IEC 27001 e ISO/IEC 27002 para gerenciamento de privacidade dentro do contexto da organização. ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019. Disponível em: https://dokumen.pub/abnt-nbr-iso-iec-277012019-tecnicas-de-segurana-extensao-da-abnt-nbr-iso-iec-27001-e-abnt-nbr-iso-iec-27002-para-gestao-da-privacidade-da-informaao-requisitos-e-diretrizes-abnt-nbr-iso-iec-277012019-1nbsped-9788507083559.html. Acesso em: 21 jun. 2023.

com as diretrizes da LGPD e outras regulamentações de proteção de dados. A falta de investimentos projetados em treinamentos pode resultar em uma lacuna de conhecimento entre os profissionais, tornando-os menos aptos a lidar com as novas tecnologias, situação que também é refletida na resistência à adoção de inovações das equipes de saúde.

A resistência à mudança é um desafio comum sempre que ocorre uma alteração consistente na rotina de trabalho de uma organização. Mudanças rápidas e profundas, como as que se verificou nos últimos cinco anos no setor de saúde[368], certamente trazem incertezas e desconfortos para parte dos envolvidos. Porém, passado o impacto no momento inicial da apresentação de novos recursos, processos e regras, é preciso estabelecer estratégias para familiarizar as equipes com a nova realidade, desconstruindo receios e desconfortos através de treinamentos e capacitações adequadas.

Para que se utilize com êxito as ferramentas tecnológicas em favor do usuário dos sistemas de saúde, sem comprometer sua segurança ou direitos individuais, é preciso observar o aspecto humano. Na era das máquinas e dos dados, é essencial posicionar o ser humano como o condutor dos processos que se utiliza das ferramentas providas pela tecnologia. Para tanto, há que se assegurar conhecimento, diálogo e visão interdisciplinar.

Toda e qualquer organização de saúde, enquanto agente de tratamento de dados, deve ser integrada também por profissionais da seara das tecnologias, num intercâmbio essencial para garantir o gerenciamento de dados de forma adequada.

A demanda por profissionais com conhecimento técnico especializado em segurança cibernética, gerenciamento de riscos, aptos a conduzir os bancos de dados em conformidade com a LGPD configura mais um ponto desafiador a ser mencionado[369]. Entidades públicas e privadas, já conscientes da necessidade de contar o apoio técnico de um setor de T.I., indicam a dificuldade de contratar profissionais especializados, gerando uma lacuna que acaba por resultar no aumento dos riscos de violações

368 O período pandêmico trouxe uma grande aceleração para os setores público e privado. Em geral, as pessoas responderam mais rápido aos estímulos em âmbito privado, todavia a pandemia exigiu de todas as instituições, incluindo as do setor público, respostas imediatas, com uma rápida alteração da ordem e dos processos vigentes até então. Tais mudanças, em que pese as dificuldades, também foram geraram resultados positivos, como por exemplo, a adoção de plataformas digitais de gerenciamento informacionais em substituição ao uso de documentos financeiros físicos. BACKES, D. A. P.; *et al*. Os efeitos da pandemia de COVID-19 sobre as organizações: um olhar para o futuro. Iberoamerican Journal of Strategic Management (IJSM), [*S.l.*], v. 19, n. 5, p. 1-10, 2020, p.3. Editorial. Disponível em:https://doi.org/10.5585/riae.v19i4.18987. Acesso em: 15 jun. 2023.

369 A complexidade envolvida nas organizações de saúde produz desafios, que de fato, a tecnologia pode ajudar a cumprir, porém requer recursos financeiros, humanos e técnicos de uma fonte escassa. STROME, T. Healthcare analytics for quality and performance improvement. Hobbken: John Wiley & Sons; 2013, p.34.

dos preceitos da LGPD. Cabe, portanto, a compressão de uma nova especialidade profissional como requisito para que se atinjam as propostas da visão de saúde digital para o Brasil.

Diante dessas questões é possível compreender que a mera adoção de ferramentas de tecnologia com objetivo de otimizar processos, integrar sistemas e facilitar o acesso à saúde, não pode ser considerada como solução para os problemas e questões do setor. As inúmeras vantagens da saúde digital, dependem da condução da utilização, com um emprego seguro e eficiente dos recursos disponíveis. De nada vale, acelerar o tempo de atendimento e possibilitar o intercâmbio de informações entre profissionais médicos, se ao fim o cidadão encontrar sua intimidade exposta e vier a sofrer prejuízos em seus direitos básicos.

5.5 Impactos da ausência de uma proteção efetiva dos dados de saúde para os usuários do sistema

A privacidade e segurança dos dados de saúde são fundamentais para garantir o respeito aos direitos individuais e a confiança no sistema de saúde, tanto na rede pública quanto privada. Ao buscar tratamentos ou orientações sobre sua saúde, geralmente vivencia um de vulnerabilidade física e emocional, de modo que assegurar a privacidade dos dados de saúde se torna ainda mais crucial. As informações de saúde, conforme já discutido anteriormente, apresentam caráter sensível, vez que podem revelar condições clínicas, histórias familiares, traumas, entre outros aspectos íntimos do usuário do sistema. A garantia de privacidade dos dados de saúde nesse contexto, deve proteger indivíduo de uma exposição indevida por suas condições de saúde, que pode resultar não apenas em constrangimento, mas torná-lo vítima de ações predatórias ilícitas.

Os dados pessoais, além de seu valor intrínseco, apresentam também valor econômico que pode ser obtido com o uso dos próprios dados, conforme sua combinação e tratamento. O interesse comercial sobre este tipo de informação reside especialmente na possibilidade de conhecer e identificar perfis, prevendo comportamentos, gostos e até intenção de consumo. A inteligência artificial, por meio do jogo dos algoritmos, não apenas identifica pessoas, mas também é utilizada em larga escala para ler e direcionar ações de venda e atração, gerando mais conversão para empresas num perigoso ciclo

no qual quanto maior o acúmulo de dados, melhores modelos, maior atração e maior lucro[370].

Conforme o conhecimento gerado, também é possível rejeitar perfis com características indesejáveis. Tem-se aqui uma potente ferramenta de filtragem e segregação aplicada em prol de interesses econômicos, permitindo perigosos processos discriminatórios, além de incontáveis possibilidades de fraudes. Informação é poder e na busca por este poder, os dados sensíveis são matérias-primas de alta qualidade e por tanto, de alto valor.

O interesse indevido quanto aos dados de saúde pode ser observado em números. No ano de 2021, o setor foi o terceiro em número de ataques digitais, conforme. o relatório anual da *Apura Cyber Intelligence*[371]. De acordo com o mapeamento realizado, a maior parte das informações roubadas em ataques cibernéticos é vendida na *dark web*[372] e apresentam maior valor do que informações bancárias. No Brasil, o setor de saúde foi indicado como terceiro mais vulnerável a ataques de *ransomware*, ficando atrás somente do governo e da indústria.

Tal interesse reside nas características dos dados de saúde. Com base nos dados pessoais de um paciente, é possível ter acesso a informações detalhadas que versam tanto sobre informações básicas como nome, CPF e endereço, como dados bancários, bem como histórico médico com informações de familiares. Considerados como um grupo de dados mais completos as informações de saúde chegam a valer 50 vezes mais do que dados bancários na *dark web*[373] e podem ser usados por criminosos para cometer fraudes e crimes de identidade. A título de exemplo, pode se mencionar fraudes que vão

370 DOMINGOS, P. O algoritmo mestre: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Novatec, 2017, p. 36.

371 APURA CYBER INTELLIGENCE. Relatório anual de Segurança Cibernética Apura Cybersecurity S/A, 2021 O ano em resumo. São Paulo: Apura, 2021. Disponível em: https://www.linkedin.com/posts/apura_relat%C3%B3rio-anual-de-seguran%C3%A7a-cibern%C3%A9tica-activity-6885285395324571648-4v74/. Acesso em: 15 jun. 2023.

372 O termo Internet obscura ou endereço sombrio refere-se a servidores de rede disponíveis na Internet, acessíveis somente através de ferramentas, configurações ou autorizações específicas que dão um elevado nível de anonimato tanto a quem publica os conteúdos como a quem os consulta. A *Dark Web* ou Web Escura teve início com a tese de doutorado intitulada *Distributed Decentralised Information Storage and Retrieval System*, de Ian Clarke, na Universidade de Edinburgo em 1995. A *Dark W*eb é aquela parte da web que se destina a ser anônima. BECKETT, A. The dark side of the internet: in the deep web, Freenet software allows users complete anonymity as they share viruses, criminal contacts and child pornography. The Gardian, London, 2009, p. 2. Disponível em: http://www. guardian.co.uk/technology/2009/nov/26/dark-side-internetfreenet. Acesso em: 23 abr. 2023.

373 Dados de saúde valem mais que informações financeiras na dark web. PACETE, L. G. Dados de saúde valem mais que informações financeiras na dark web. Forber, São Paulo, 2022. Disponível em: https://forbes.com.br/forbes-tech/2022/06/dados-de-saude-chegam-a-valer-mais-que-informacoes-financeiras-na-dark-web/. Acesso em: 22 jun. 2023.

desde a utilização de históricos médicos para a obtenção de medicamentos controlados ilegalmente ou realizar procedimentos médicos fraudulentos em nome do paciente afetado, até fraudes contratuais envolvendo repasses de dinheiro público.

Para além de fraudes envolvendo interesses financeiros, os dados de saúde desprotegidos refletem em outros aspectos igualmente relevantes, tendo alto poder de impacto na vida do cidadão. A exposição não autorizada de dados de saúde, ou mesmo a mera desconfiança deste risco ocasiona um grave problema de confiança que pode descreditar décadas de trabalho na construção do SUS e mesmo de redes privadas de saúde. Quando os pacientes não têm confiança de que seus dados estão sendo devidamente protegidos, pela insegurança instaurada podem adotar comportamentos indesejáveis, evitando compartilhar e declarar informações consideradas relevantes para seu tratamento ou até mesmo vindo a se esquivar do atendimento médico.

Como consequência de tal situação, surge a fragilidade ou erro de diagnósticos, problemas de saúde não controlados ou sem tratamento, resultando em riscos e danos para a saúde, o que seria um verdadeiro retrocesso. Além disso, abre-se via para ações de danos materiais e morais mediante prejuízos suportados pelo cidadão, e a perda de confiança e de credibilidade da população em geral em relação às instituições do setor.

Neste sentido, vale mencionar a condenação da prefeitura de Barueri/SP em julho de 2021, ao pagamento da importância de R$ 20 mil reais, a título de indenização por danos morais, a um paciente portador de HIV que teve seus dados médicos vazados no portal de saúde do município. A 5ª Câmara de Direito Público do Tribunal de Justiça do Estado de São Paulo, realizou a condenação por descumprimento da LGPD. A desembargadora relatora do caso, entendeu que o município faltou com as normas de proteção de dados e ao segredo de informação em saúde, visto que com a mera a inserção de um número de Cadastro de Pessoa Física - CPF e da data de nascimento se chegou ao acesso completo do prontuário médico do paciente, portador do vírus HIV, fato que ocasionou constrangimento e degradação no ambiente de trabalho[374].

374 Apelações cíveis. Danos morais. Danos materiais. Divulgação de prontuário médico. HIV. Dados médicos do autor disponibilizados ao público no site da prefeitura mediante a simples inserção de seu CPF e sua data de nascimento, informações essas de fácil acesso. Ausência de senha de acesso que torna a informação, na prática, pública. O vazamento do prontuário médico do requerente (fls. 31/35), ao indicar ser ele portador do vírus do HIV, gerou situação embaraçosa e degradante no ambiente de trabalho. A responsabilidade civil objetiva exige apenas a ocorrência do dano, a existência de nexo causal entre a conduta e este dano e a ausência de culpa excludente da vítima (art. 37, § 6º CF). O sigilo dos dados pessoais ganha contornos cada vez mais sensíveis, sendo matéria cada dia mais regulada na seara legislativa. Eventuais vazamentos de dados particulares são evidentes fatos geradores de danos, seja de ordem moral ou material, e o legislador tende a protegê-los, especialmente quando digam respeito aos direitos de personalidade. Art. 5º, X, Constituição Federal, art. 42 da Lei nº 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018. Danos morais configurados. Quantum indenizatório majorado. Danos materiais não configurados. Ausência de prova de nexo de causalidade entre a exposição dos

No caso, em questão o paciente se viu obrigado a publicizar a sua condição como portador do vírus HIV e alguns tempo depois acabou por ser desligado da empresa sob alegações técnicas.

Em maio de 2022, a oitava Turma Cível do TJ/DF confirmou decisão antecipatória de tutela que determinou a inclusão de sigilo em documentos e prontuários médicos que contenham dados pessoais de pacientes protegidos por Lei Geral de Proteção de Dados – LGPD, Constituição Federal e legislação esparsa[375]. Na ocasião, o relator

dados médicos e a efetiva demissão do autor. Honorários advocatícios readequados. Recurso do autor parcialmente provido. Recurso do réu desprovido. SÃO PAULO. Tribunal de Justiça de São Paulo. **Apelação Cível nº 1016844-03.2020.8.26.0068 - TJ/SP**. o, informações essas de fácil acesso. Ausência de senha de acesso que torna a informação, na prática, pública. O vazamento do prontuário médico do requerente (fls. 31/35), ao indicar ser ele portador do vírus do HIV, gerou situação embaraçosa e degradante no ambiente de trabalho. A responsabilidade civil objetiva exige apenas a ocorrência do dano, a existência de nexo causal entre a conduta e este dano e a ausência de culpa excludente da vítima (art. 37, § 6º CF). O sigilo dos dados pessoais ganha contornos cada vez mais sensíveis, sendo matéria cada dia mais regulada na seara legislativa. Eventuais vazamentos de dados particulares são evidentes fatos geradores de danos, seja de ordem moral ou material, e o legislador tende a protegê-los, especialmente quando digam respeito aos direitos de personalidade. Art. 5º, X, Constituição Federal, art. 42 da Lei nº 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018. Danos morais configurados. Quantum indenizatório majorado. Danos materiais não configurados. Ausência de prova de nexo de causalidade entre a exposição dos dados médicos e a efetiva demissão do autor. Honorários advocatícios readequados. Recurso do autor parcialmente provido. Recurso do réu desprovido. Relator(a): Heloísa Mimessi. São Paulo: Tribunal de Justiça de São Paulo. Disponível em: https://esaj.tjsp.jus.br/cjsg/resultadoSimples.do;jsessionid=AE02A84D72A777156E9E282400D39571.cjsg2?conversationId=&nuProcOrigem=+1016844-03.2020.8.26.0068.&nuRegistro=. Acesso em 12 de julho de 2023.

375 *In casu*, a empresa agravante requer a inclusão de sigilo na documentação anexada aos autos originários, na qual consta o nome completo, a idade e o procedimento médico-hospitalar resumido realizado nos beneficiários do plano de saúde agravado. Ao analisar o recurso, o Relator esclareceu que a Lei 13.709/2018 (LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, de pessoa natural ou jurídica, de direito público ou privado, com o intuito de proteger os direitos fundamentais de liberdade e privacidade. Salientou que a aludida lei tem como um de seus fundamentos (incisos I e IV do art. 2º) o fomento ao respeito à privacidade e à inviolabilidade da intimidade, da honra e da imagem. Destacou que o art. 7º, I, e o art. 14, § 1º, da mencionada norma exige o consentimento expresso do titular para o tratamento dos dados ou o consentimento de um dos pais ou representante legal, no caso de crianças e adolescentes. Ponderou ser prudente, até a realização de estudos e consolidação da jurisprudência sobre o tema, a preservação do sigilo anotado nos documentos dos pacientes, os quais não são parte na presente ação, como forma de proteção do direito à privacidade e à intimidade, bem como do sigilo profissional correspondente a teor do disposto nos arts. 2º, I e IV, c/c o art. 5º, I, da LGPD, e o art. 79 do Código de Ética Médica/Resolução CFM 1.931/2009. Afirmou que frequentemente decreta segredo de justiça em documentos com dados protegidos "especialmente os que contêm informações íntimas, como os prontuários médicos. O processo tem curso público, ficando os documentos sigilosos acessíveis apenas pelos advogados das partes, com obrigação de segredo transferida. Isso quer dizer que os advogados, se violarem esses segredos, responderão pela infração no âmbito criminal, civil e ético". Com isso, o Colegiado confirmou a decisão antecipatória de tutela e deu provimento ao agravo de instrumento para manter o sigilo vindicado. Acórdão 1414740, 07027023720228070000, Relator: Des. Diaulas Costa Ribeiro, Oitava Turma Cível, data de julgamento: 7/4/2022, publicado no PJe: 25/4/2022. BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. (8ª Turma Cível). Agravo de instrumento 0702702-37.2022.8.07.0000. Agravo de instrumento. Ação de obrigação de fazer. Contrato de prestação de serviços. Empresas. Hospital e plano de saúde. Auditoria. Contas. Provas. Juntada de documentos médico-hospitalares. Pacientes. Sigilo. Lei geral de proteção de dados. Informações pessoais. Intimidade. Privacidade. Dados sensíveis. Proteção. Necessidade. Agravante: Servicos Hospitalares Yuge S.A. Agravado(s): Santa Luzia Assistencia Medica S/A. Relator: Desembargador Diaulas Costa Ribeiro. Acórdão Nº 1414740. Brasília: Poder Judiciário da União, 2022. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&controladorId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.ControladorBuscaAcordao&visaoAnterior=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.

enfatizou a finalidade da LGPD ao regulamentar o tratamento de dados pessoais, inclusive em meio digital, de pessoas físicas ou jurídicas, de direito público ou privado, a fim de proteger os direitos fundamentais à liberdade e à privacidade e ressaltou que uma das principais funções da norma é assegurar o respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem[376].

A segurança do sistema de saúde é uma responsabilidade compartilhada entre instituições de saúde, governos, profissionais da área e órgãos reguladores. A cada falha, verificam-se consequências que comprometem não apenas a reputação e o discurso, mas também na violação de direitos fundamentais do cidadão. A autodeterminação e a liberdade são condições essenciais para a democracia. Portanto, é imperativo encontrar maneiras de lidar com os riscos e desafios do processamento de dados de saúde que por sua natureza, podem afetar a capacidade de um indivíduo realizar suas escolhas e determinar como deseja ser percebido pela sociedade.

A proteção de dados pessoais está diretamente associada a ideia de dignidade humana, que em termos práticos apresenta em seu conteúdo mínimo inclui três elementos: o valor intrínseco de cada pessoa, a autonomia individual e o valor comunitário, ao tempo que considera a pessoa como sujeito de direitos e não como um meio ou objeto[377]. O direito à privacidade se encontra conexo a um sentido de individualidade e autonomia. O ser humano vive uma constante busca por liberdade e é seu interesse evitar qualquer forma de domínio e manipulação[378].

A este ponto é importante retomar a questão dos direitos subjetivos do titular dos dados pessoais. Não é razoável que o indivíduo se veja completamente afastado do controle do fluxo de seus dados pessoais. A exceção de situações de incontestável interesse público, tal como se verificou no período pandêmico, a cada pessoa possui diretos subjetivos em face de seus dados pessoais, dentre os quais destacam-se o direito geral de informação; o direito de acesso e o direito de notificação; o direito de

VisaoBuscaAcordao&nomeDaPagina=resultado&comando=abrirDadosDoAcordao&enderecoDoServlet=sistj&historicoDePaginas=buscaLivre&quantidadeDeRegistros=20&baseSelecionada=BASE_ACORDAOS&numeroDaUltimaPagina=1&buscaIndexada=1&mostrarPaginaSelecaoTipoResultado=false&totalHits=1&internet=1&numeroDoDocumento=1414740. Acesso em: 11 ago. 2022.

376 LGPD, art. 2º, incisos I e IV. BRASIL, op. cit., 2023.

377 BARROSO, L. R. A dignidade da pessoa humana no direito constitucional contemporâneo: a construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016, p. 9.

378 "A necessidade humana de não compartilhar com outros - ou de restringir a pessoas mais próximas - alguns fatos, desejos e informações pessoais é tão patente que o senso comum considera a privacidade, ao contrário do que defendem os estudiosos, um valor em si mesmo". BESSA, L. R. O consumidor e os limites dos bancos de dados de proteção ao crédito. São Paulo: Revista dos Tribunais: 2003, p. 88.

retificação, cancelamento e bloqueio dos dados; o direito de não se ficar sujeito a uma decisão individual automatizada[379].

O direito geral de informação se refere ao direito que as pessoas possuem de conhecer sobre a existência dos bancos de dados, seus objetivos e conteúdo. Parte do pressuposto de que a transparência é essencial para se combaterem os abusos. E em atenção à necessidade de transparência, cabe à contrapartida a esse direito de bancos de dados o dever publicar suas informações gerais, tais como nome, sede e conteúdo, em registros públicos, diários oficiais ou meios de grande circulação. [380]

Conforme mencionado nos capítulos iniciais deste texto, o acesso à informação é um direito fundamental que se encontra previsto no artigo 5º inciso XXXIII, bem como no inciso II do § 3 do art. 37 e no § 2 do art. 216 da Constituição Federal de 1988 e está diretamente relacionado ao exercício da cidadania.

O segundo direito a ser mencionado é o de acesso. Conforme indicado no artigo 9º da LGPD, trata-se do direito de um indivíduo receber, mediante solicitação, informações sobre os dados registrados sobre ele. Esta faculdade inclui o conhecimento dos dados armazenados, considerando informações sobre sua origem, autoridades que recebem as informações transmitidas ou sua categoria; e finalidade do armazenamento[381]. O direito de acesso também inclui o direito de um indivíduo saber, no caso de uma rede de bancos de dados, em qual banco de dados suas informações estão armazenadas. Nesse caso, o cidadão pode procurar por qualquer um deles[382]. É o caso de um cliente de um banco que solicita a instituição que informe quais dados pessoais estão sendo armazenados e tratados, bem como os fins específicos desse tratamento.

Em sequência, tem-se o direito de notificação, que se relaciona diretamente aos direitos subjetivos mencionados anteriormente e que desponta sempre quando ocorrer

379 MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 65-66.

380 BENNETT, C. Regulating Privacy: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, p. 109.

381 LGPD, artigo nº 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. BRASIL, op. cit., 2018.

382 Neste sentido se posiciona o Código de Defesa do Consumidor, em seu artigo nº 43: rt. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. BRASIL, op. cit., 1990a.

uma coleta de dados sem o devido conhecimento de seu titular. Todo cidadão necessita ser informado sobre o armazenamento de dados, os objetivos de seu tratamento e ainda quanto a identidade do responsável pelo banco de dados. Também deve ser realizada notificação em casos de transferência de dados, com a indicação dos organismos receptores. É válido recordar que a notificação pode ser dispensada na hipótese de que indivíduo vier a ter conhecimento do armazenamento ou da transferência de dados por outros meios ou ainda, quando essas ações tiverem fundamento legal[383].

Os direitos de retificação, cancelamento e bloqueio tem por objetivo assegurar o princípio da qualidade dos dados pessoais. Ocorre que nem sempre a coleta de dados é realizada forma satisfatória, o que gera a necessidade de correções em caso de equívoco, e até cancelamento no caso se tornem obsoletos ou tenham sido indevidamente armazenados. Também pode haver situações de bloqueio nos casos em que por algum motivo, o cancelamento não é possível ou esbarre em uma proibição legal. [384]

Os dados pessoais serão bloqueados ainda, quando se verificar controvérsia sobre a sua veracidade, sem que haja provas para confirmá-la. Nas hipóteses de correção, bloqueio ou cancelamento dos dados, é direito do titular solicitar a notificação expressa de todos os organismos que receberam por transferência os seus dados, a fim de que estejam cientes do recebimento das informações e tomem providências.

O direito de não ser sujeito a uma decisão individual automatizada trata do direito do cidadão de não se submeter a decisões proferidas considerando apenas o tratamento automatizado de dados[385]. Nos termos do artigo 20 da LGPD, tem-se uma proibição geral referente a decisões automatizadas, assegurando a defesa do titular e sua mínima participação no processo de decisão que tenha como base em seus dados pessoais e que poderia afetar sua vida prática de modo permanente.[386]

383 LGPD, artigo nº 10: O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. BRASIL, op. cit., 2018.

384 LGPD, artigo nº 18: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: III - correção de dados incompletos, inexatos ou desatualizados. Idem.

385 Originalmente esse direito está previsto no art. 15 da Diretiva Europeia 95/46/CE. EUROPA, op. cit., 1995.

386 LGPD, artigo nº 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. BRASIL, op. cit., 2018.

O próximo direito a ser considerado é o de eliminação, também conhecido como "direito ao esquecimento". Nos termos do artigo 18, inciso IV da LGPD, o titular tem o direito de solicitar a exclusão de seus dados pessoais quando o tratamento não for mais necessário, quando o consentimento para revogado ou quando os dados foram tratados de forma ilegal. [387] Situação que pode ser exemplificada por um usuário de uma rede social pode solicitar que sua conta e todas as informações associadas a ela sejam permanentemente excluídas.

Quanto ao direito de oposição, compreende-se que o titular tem o direito de se opor ao tratamento de seus dados pessoais em determinadas situações, como por exemplo, para fins de marketing direto. É o que ocorre quando um cliente vem a optar por não receber mais e-mails e notificações promocionais de determinada loja. E por fim, chega-se ao direito de portabilidade, descrito no artigo nº 18, inciso V da LGPD. Neste caso o titular possui o direito de receber os dados pessoais que forneceu a um controlador em um formato protegido e de uso comum, e tem o direito de transmitir esses dados a outro controlador, se assim desejar.[388] Seria esta, a situação de um usuário de um serviço de streaming que solicita que seus dados de perfil sejam transferidos para outra plataforma similar. Para uma visão didática acerca dos direitos subjetivos dos titulares de dados pessoais, indica-se a leitura do resumo da matéria, traduzido na tabela abaixo.

Quadro 4 - Direitos subjetivos dos titulares de dados pessoais

Direitos Subjetivos do Titular dos Dados Pessoais	Definição
Direito Geral de Informação	O titular tem o direito de receber informações claras e completas sobre o tratamento de seus dados pessoais, incluindo finalidades, formas de tratamento e direitos.
Direito de Acesso	O titular tem o direito de obter do controlador a confirmação de que seus dados estão sendo tratados e, se sim, acessar os dados e informações sobre o tratamento.
Direito de Notificação	O titular tem o direito de ser avisado caso tenha causado alguma violação de segurança que possa afetar significativamente seus dados pessoais.
Direito de Retificação, Cancelamento e Bloqueio dos Dados	O titular tem o direito de solicitar a correção de dados imprecisos, a exclusão de dados necessários ou tratados ilegalmente e o bloqueio de dados contestados.
Direito de não ser sujeito a uma Decisão Individual Automatizada	O titular tem o direito de solicitar intervenção em decisões humanas automatizadas que afetem seus interesses, direitos ou liberdades.

387 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei. Idem.

388 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Ibid.

Direitos Subjetivos do Titular dos Dados Pessoais	Definição
Direito de Eliminação ou Direito ao Esquecimento	O titular tem o direito de solicitar a exclusão de seus dados pessoais quando o tratamento não for mais necessário, quando o consentimento para revogado ou quando os dados foram tratados de forma ilegal.
Direito de Oposição	O titular tem o direito de se opor ao tratamento de seus dados pessoais em determinadas situações, como por exemplo, para fins de marketing direto.
Direito de Portabilidade	o titular possui o direito de receber os dados pessoais que forneceu a um controlador em um formato protegido e de uso comum, e tem o direito de transmitir esses dados a outro controlador, se assim desejar.

A importância de assegurar que o titular dos dados tenha voz ativa em processos de decisão que afetem significativamente suas oportunidades de vida é um dos pilares da visão quanto à proteção de dados. A LGPD, a exemplo do que se encontra no texto do RGPD[389], preconiza a necessidade de consentimento e específico do titular para o tratamento de seus dados em diversas situações, inclusive em processos automatizados de tomada de decisão que tenham efeitos jurídicos ou que afetem significativamente o titular. Na norma europeia, o controle dos dados pelos cidadãos envolve o conhecimento específico dos nomes das empresas que tratam seus dados, as finalidades para as quais serão utilizados, a base legal utilizada para o tratamento dos dados pessoais, o período em que serão conservados, bem como o direito de retirar o consentimento.[390] Desta forma, tanto no Brasil, quanto na Europa, o titular dos dados emerge como figura central do processo, exercendo direitos que lhe conferem maior controle sobre suas informações pessoais.

Em fato, ambas as legislações se apoiaram na filosofia de proteção aos direitos e liberdades fundamentais dos titulares de dados, colocando o controle e a privacidade do indivíduo em primeiro plano. Para tanto, se exige que o controlador forneça informações claras e adequadas sobre o tratamento dos dados, garantindo ao titular o conhecimento necessário para tomar suas decisões. A ausência de uma proteção efetiva dos dados pessoais, atinge fortemente o cidadão nas mais diversas esferas de sua vida particular e civil.

389 Na Europa, a proteção de dados é entendida como um direito da personalidade, ou seja, interpretada sob o ponto de vista objetivo, é considerada como "um conjunto de características e atributos de uma pessoa, que é considerada objeto de proteção pelo ordenamento jurídico". SCHREIBER, A. Direitos da Personalidade. Rio de Janeiro: Atlas, 2011, p. 6.

390 Vale destacar que RGPD não se aplica ao tratamento de dados pessoais de pessoas falecidas ou de pessoas coletivas, bem como também não será aplicado ao tratamento de dados por motivos exclusivamente pessoais ou domésticos. Comissão Europeia. EUROPA. Para que serve o Regulamento Geral sobre a Proteção de Dados (RGPD)? Comissão Europeia, 2016. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pt#refer%C3%AAncia. Disponível em: 1 maio 2023.

A situação que se agrava quando se trata de dados sensíveis de saúde. O vazamento de informações médicas sensíveis pode ter consequências graves tanto do ponto de vista emocional quanto social, criando um contexto de vulnerabilidade para os indivíduos afetados. Além dos exemplos já mencionados, é preciso atentar ao fato de que a invasão de privacidade e a sensação de perda de controle sobre suas informações pessoais podem gerar sentimentos de ansiedade, medo, raiva e vulnerabilidade, que venha a se converter em um grave problema para o indivíduo. Tratando-se de dados extremamente complexos e permeados de informações íntimas, a exposição pública de detalhes médicos sensíveis pode causar constrangimento e angústia emocional ao ponto de afetar a saúde mental dos usuários dos sistemas de saúde[391].

Outra consequência da exposição indevida de dados de saúde que demanda reflexão cuidadosa é a possibilidade de discriminação e estigmatização dos pacientes. Informações sobre condições médicas específicas, histórico familiar ou orientação sexual podem ser utilizadas para discriminar ou excluir indivíduos em diferentes contextos sociais, profissionais e familiares. A estigmatização pode levar ao isolamento social, prejuízos na carreira e impactar a autoestima e a qualidade de vida do paciente afetado, assunto que será detalhado a seguir.

391 Neste sentido, o exemplo da decisão do TJDF de outubro de 2022: PRONTUÁRIO DE PACIENTE INTERNADO NO HOSPITAL. INFORMAÇÕES. ACESSO INDEVIDO. FRAUDE. DEVER DE GUARDA. FALHA NA PRESTAÇÃO DO SERVIÇO. DANO MATERIAL E DANO MORAL. CONFIGURAÇÃO. VALOR ARBITRADO. RAZOÁVEL E PROPORCIONAL. (...) Na espécie, é notória a pertinência subjetiva, se a parte autora alega falha na segurança dos procedimentos do hospital réu, que deixou vazar informações confidenciais da paciente (genitora da autora), que ali estava internada, possibilitando o golpe e a consequente reparação pelos danos suportados. 2. A responsabilidade objetiva pelo fato do serviço na relação de consumo, consoante o art. 14 do CDC, é oponível aos hospitais na parcela dos serviços relacionados ao estabelecimento empresarial, a exemplo da internação, alimentação, instalações e serviços auxiliares. No caso, presente a falha na prestação de seu serviço, porquanto terceiros tiveram acesso a dados confidenciais extraídos do prontuário da paciente que estavam sob a guarda do hospital, circunstância que possibilitou que a autora (filha da paciente) fosse vítima de estelionato. 3. Diante de evidente negligência do hospital na guarda das informações pessoais da paciente, possibilitando a manobra fraudulenta, impõe-se o ressarcimento da quantia desembolsada pela vítima da fraude. 4. Atingido o direito da personalidade diretamente, o dano moral (puro ou direto) estará vinculado à própria existência do fato (in re ipsa), cujos resultados são presumidos, ao contrário de quando é atingido o direito da personalidade mediante lesão a bens de natureza patrimonial (dano moral impuro ou indireto). 5. Na hipótese, é inegável que o agravamento considerável do estado de saúde da paciente atinge a personalidade jurídica da autora, que se encontrava em situação de fragilidade emocional em virtude da internação de sua genitora. Assim, sem olvidar as finalidades compensatória, punitiva ao ofensor, pedagógica e preventiva da condenação, bem assim às circunstâncias da causa, inclusive a capacidade das partes, afigura-se adequado o valor fixado na sentença. 6. Apelações conhecidas e não providas. BRASIL. Tribunal de Justiça do Distrito Federal (5ª Turma). Apelação Civel - Processo nº 0708698-23.2021.8.07.0009. Apelante(s): Elissandra de Melo e Silva e Hospital Santa Marta LTDA. Apelado(s) Hospital Santa Marta LTDA e Elissandra de Melo E Silva. Relator: Desembargador Fábio Eduardo Marques. Acórdão Nº 1616700. Diário do Jornal Eletrônico, Brasília: TJDF, 2022.

5.6 O tratamento de dados de saúde como matriz para o surgimento de novas formas de discriminação

A principal razão para que os dados de saúde sejam classificados como sensíveis, reside no seu alto potencial discriminatório. A divulgação indevida de informações associadas ao histórico médico e condições genéticas de um indivíduo pode resultar em diferentes formas de controle social e econômico[392]. São ações que não apenas adentram a esfera da discriminação, mas apresentam uma surpreendente amplitude de repercussões, ao tempo em que ferem direitos individuais e podem resultar em situações que vão desde o isolamento social, barreiras no mercado de trabalho e perseguições de políticas ou de gênero.

A ideia de discriminação aqui apresentada se refere a ação preconceituosa em relação a uma pessoa ou grupo de pessoas, configurando uma exclusão direcionada, que dificulta ou impossibilita o convívio em sociedade. Ocorre um ato discriminatório sempre que se verifica uma atitude baseada em ideias preconcebidas envolvendo questões raciais, de gênero, orientação sexual, nacionalidade, religião, situação econômica ou qualquer outro aspecto social, violando o disposto no artigo 7 da Declaração Universal dos Direitos Humanos de 1948[393].

O preconceito é a matriz da discriminação. Trata-se da opinião preconcebida acerca de algo ou alguém, baseada na ignorância ou em estereótipos. São ideias negativas construídas sobre uma pessoa ou grupo formadas previamente à interação direta com esta pessoa ou grupo.[394]

A leitura do artigo 5º, inciso II da LGPD e demais dispositivos sobre a questão dos dados sensíveis deixa nítida a preocupação do legislador em distingui-los em uma categoria especial de dados, com a finalidade de estabelecer maiores proteções jurídicas. Isto ocorre em razão do potencial discriminatório desta classe de dados e o reconhecimento de que seu uso indevido pode resultar em comportamentos e práticas

392 Coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como a proteção de escolhas de vida contra qualquer forma de controle público e estigma social. RODOTÀ, op. cit., p. 12.

393 Conforme já mencionado o texto do artigo 7 da Declaração Universal dos Direitos Humanos de 1948 afirma que "todos são iguais perante a lei e têm direito, sem qualquer distinção, a igual proteção da lei. Todos têm direito a igual proteção contra qualquer discriminação que viole a presente Declaração e contra qualquer incitamento a tal discriminação." ONU, op. cit., 1948.

394 OHL, N. G.; ANGELUCCI, C. B.; NICOLAU, A. M.; HONDA, C. Escolarização e preconceito: lembranças de jovens com e sem deficiência. Revista da Associação Brasileira de Psicologia Escolar e Educacional(ABRAPEE), São Paulo, v. 13, n. 2, p. 243-250, 2009, p. 243.

de segregação.[395] Os dados sensíveis são marcados pela presença de informações íntimas como raça, etnia ou orientação sexual e os dados de saúde, acrescem a esta lista, detalhes quanto a condições físicas, emocionais e genéticas de seus titulares. Desta forma, é esperado que os dados sensíveis de saúde acabem por ocupar um papel central em situações que refletem discriminação e estigmatização[396].

Dentre os princípios elencados na LGPD quanto ao tratamento de dados pessoais consta o de não discriminação, que indica a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.[397] Ao utilizar tal escolha de expressões, dissociando a ideia da ilicitude e da abusividade, o legislador indica a possibilidade de tratamentos diferenciados, desde que não se caracterize situação de ilicitude e abusividade.

Em outras palavras, seria aceitável realizar tratamentos de dados que levem a segregação, desde que no sentido de diferenciação, sem que se verifique consequências excludentes ilícitas, tal como se verifica na prática da cobrança de seguros com valores diferenciados para determinados perfis que supostamente oferecem menor risco de envolvimento em acidentes.[398] No entanto, o mesmo raciocínio não caberia nas situações envolvendo dados pessoais sensíveis, visto sua natureza personalíssima e os riscos potenciais envolvidos.

Retomando a visão específica da seara de saúde, objeto deste estudo, o tratamento irregular de dados sensíveis pode ocasionar problemas e prejuízos em face da sensibilidade das informações. Como já mencionado, o acesso à dados tão completos permite que cibercriminosos pratiquem uma série de fraudes e conduzam campanhas de *phishing* ou extorsão contra indivíduos com base nas informações pessoais aderidas, o que pode incluir ameaças discriminatórias ou intimidatórias. Porém, para além das situações reconhecidas e já tipificadas pelo Código Penal, restam casos que em sua maioria não encontram precedentes e nem mesmo clareza legal.

Ao longo de sua história, a humanidade lidou em diversos momentos com doenças de avanço rápido que ocasionaram graves crises sanitárias. Da lepra à peste negra, da

395 LGPD, artigo 5º: Para os fins desta Lei, considera-se: 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; BRASIL, op. cit., 2018.

396 Aqui se entende a ideia da utilização ampla e não consentida de dados pessoais que sejam caracterizados por sua capacidade discriminatória tanto pelo Estado, quanto pelo mercado e sociedade em geral.

397 LGPD, artigo 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; BRASIL, op. cit., 2018.

398 MULHOLLAND, op. cit., 2018, p. 159.

varíola ao vírus ebola, do HIV e mais recentemente o COVID-19, a medicina se aliou à pesquisa e as tecnologias para vencer epidemias e assegurar a saúde. Nestas ocasiões, medidas de segregação surgiram apoiadas em dados clínicos sob a alegação de proteção do bem-estar geral.

Contudo, a realidade tecnológica e o acesso aos bancos de dados clínicos, ampliam os alvos de discriminação, impactando negativamente da vida de milhares de usuários dos sistemas de saúde. Para se tornar vítima de ações discriminatórias, basta somente que o indivíduo, por qualquer razão, esteja enquadrado em um grupo do qual tenha sido traçado um perfil com conotações negativas.[399] A discriminação se opõe por completo a ideia de igualdade, ao tempo que se aproxima do conceito de exclusão, devendo por tanto, ter suas origens identificadas e combatidas pelo Estado[400].

As informações obtidas através dos dados pessoais de saúde utilizadas de forma seletiva, podem vir a destacar apenas aspectos negativos de um indivíduo ou grupo e ignorando informações positivas, gerando tratamento injusto, ou ainda serem utilizadas como base para crimes e ações de ódio. Tal como o já mencionado exemplo do funcionário portador do vírus HIV, que teve a sua condição de saúde divulgada indevidamente através do sistema da prefeitura e passou a sofrer discriminação dos colegas de trabalho.

Outra questão a ser considerada é a possibilidade da chamada discriminação algorítmica, fenômeno que perpetua nos algoritmos utilizados nos mais diversos sistemas, preconceitos enraizados na sociedade e afeta principalmente grupos considerados frágeis ou minoritários tais como mulheres, pessoas não brancas, homoafetivos e indivíduos de baixa renda[401]. Essa forma de discriminação se materializa por meio da tomada de decisão automatizada, quando o algoritmo ao gerar um resultado utiliza bases ou critérios que excluem certos indivíduos que foram submetidos aquele tratamento de dados, perpetuando preconceitos que já são debatidos em nossa sociedade, gerando um resultado injusto para os envolvidos.

---

399 A formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação […] seja porque dados pessoais, aparentemente não "sensíveis", podem se tornar sensíveis; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas". RODOTÀ, op. cit., p. 56.

400 FERREIRA, A. A. O Brasil e o preconceito: uma análise teórica e crítica da Lei 7.716/89 frente à realidade brasileira. Âmbito Jurídico, Rio Grande, v. XVIII, n. 134, 2015, p.1

401 MENDES, L. S.; MATIUZZO, M. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. RDU, Porto Alegre, v. 16, n. 90, p. 39-64, 2019, p. 41. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 17 jun. 2023.

A discriminação algorítmica ocorre em dois momentos: inicialmente na criação e design do algoritmo, quando se definem quais critérios deverão ser utilizados como embasamento para a decisão pretendida e o peso cada um deles refletirá na avaliação; e posteriormente, na formação da base de dados a ser utilizada para seu treinamento e execução[402]. É preciso deixar claro que em nenhum momento se questiona a presença de uma subjetividade por parte dos sistemas. O que ocorre é que nem sempre os dados são completamente confiáveis. Na maioria das situações, pelos mais diversos motivos, tem-se dados frequentemente imperfeitos, o que permite que o algoritmo venha a trabalhar com uma base de preconceitos preexistente.[403]

No ano de 2020, uma pesquisa realizada pelo *NIST - National Institute of Standards and Technology* revelou falhas em algoritmos de reconhecimento facial que apresentaram de 10 a 100 vezes mais probabilidade de identificar imprecisamente o rosto negro ou asiático em comparação com o branco, especialmente quando se trata de rostos femininos. [404] Esses dados vão de encontro a notícia reportada no ano anterior, quando uma mulher foi detida por engano no Rio de Janeiro após ter sido confundida pelo sistema de reconhecimento facial da Polícia Militar. Os policiais acreditavam estar prendendo uma foragida da Justiça, acusada pelos crimes de homicídio e ocultação de cadáver, mas ao verificar a identidade da suposta criminosa, reconheceram o engano.[405]

Outro exemplo de discriminação algorítmica pode ser verificado na situação do indivíduo que busca aprovação de crédito junto a uma instituição bancária e acaba por ter seu pedido rejeitado mediante a avalição realizada por algoritmo que partindo da análise de dados sensíveis considera sua origem racial historicamente um indicativo de baixa renda. Logo, a leitura realizada com base em critérios de alguma forma viciados não poderá ser considerada justa ou segura.

---

402 SHIPPERS, L. M. Algoritmos que discriminam: uma análise jurídica da discriminação no âmbito das decisões automatizadas e seus mitigadores. Monografia (Bacharel em Direito)- Fundação Getúlio Vargas, São Paulo. 2018, p. 21.

403 Como os seres humanos programam algoritmos preditivos, seus vieses e valores podem ser incorporados às instruções do software, conhecidas como código-fonte e algoritmos preditivos. CITRON, D. K.; PASQUALE, F. The scored society: Due process for automated predictions. Washington Law Review, v. 89, n. 1, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 12 jul. 2023, p. 4 - tradução nossa.

404 GUEDES, P. **Discriminação tecnológica**: desmistificando a neutralidade da Inteligência Artificial em meio à crise de inclusão e de diversidade nas tecnologias emergentes. ITS Rio - Grupo de Pesquisa de Direito do Instituto de Tecnologia e Sociedade, Rio de Janeiro, 2020, p. 3. Disponível em: https://itsrio.org/wp-content/uploads/2020/10/Discriminação-tecnológica_Paula_Guedes.pdf. Acesso em: 14 abr. 2023.

405 Recomenda-se a leitura completa da notícia. SISTEMA DE RECONHECIMENTO facial da PM do RJ falha, e mulher é detida por engano. G1, Rio de Janeiro, 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 23 jun. 2023.

Por estas situações, reta claro que os riscos do uso de informações para segmentação discriminatória são reais e permeiam o cotidiano do cidadão. Sendo o SUS considerado com o detentor de uma das principais bases de dados do país, é natural que se volte a atenção para os perigos oriundos de vazamentos, tal como noticiados em tempos recentes. Empresas e indivíduos mal-intencionados, buscam hoje os dados pessoais de saúde para segmentar grupos específicos com base em características como raça, gênero, histórico de doenças, orientação sexual e até informações genéticas, a fim de oferecer ou negar serviços, produtos ou oportunidades exercitando tipos de preconceito implícito.

A discriminação oriunda dos dados de saúde pode ocorrer dentro e fora da esfera de cuidados. Não é raro que sejam reportados incidentes dentro de instituições da rede de assistência pública e privada. Porém, antes de abordar diretamente a problemática das clínicas, hospitais, laboratórios e empresas de planos de saúde, é válido destacar que ações discriminatórias que tem por base dados de saúde podem ser verificadas em outros setores e em outros momentos da vida do cidadão.

Ao preencher um cadastro em um laboratório de exames, ou uma requisição de medicamentos, o usuário do sistema de saúde declara suas informações e especialmente seu estado. Este tipo de informação pode ser utilizado para fins criminosos, para indução de comportamento, para indicação de restrições de crédito ou mesmo como critério avaliativo em processos seletivos. Percebe-se um amplo raio de ação da informação, que utilizada indevidamente ocasionará não um, mas diversos prejuízos a pessoa que teve suas informações íntimas divulgadas.

Conforme uma visão subjetiva, o acesso a dados dessa natureza pode se tornar um instrumento para favorecer práticas discriminatórias, fortalecer preconceitos e até mesmo gerar pânico, tal como foi visto em diversas ocasiões durante o ápice da pandemia do vírus COVID-19[406]. Não se pode olvidar que certas enfermidades, além de mazelas físicas, geram repercussões sociais. É o caso de doenças infectocontagiosas, doenças sexualmente transmissíveis e transtornos mentais.

A estigmatização oriunda de dados de saúde é real e provoca sérios impactos pessoais e sociais. O estigma pode ser compreendido como uma discrepância entre a identidade

406 Como exemplo o caso noticiado em Foz do Iguaçu, quando uma paciente procurou foi diagnosticada com suspeita de COVID-19 e teve seu prontuário foi divulgado nas redes sociais. A situação gerou alarme em toda a cidade, que até então não tinha casos registrados da doença. Porém, o diagnóstico da paciente estava errado. FALSA SUSPEITA sobre coronavírus em Foz inunda as redes sociais. H2Foz, Foz do Iguaçu, 2020. Disponível em: https://www.h2foz.com.br/sem-categoria/falsa-suspeita-sobre-coronavirus-em-foz-inunda-as-redes-sociais/. Acesso em: 12 jul. 2023.

social real de alguém, aquilo que ele é, e a identidade social virtual, o caráter imputado ao indivíduo pelos outros, ou seja, uma caracterização com base nas expectativas de como ele deve ser. Reflete um processo de desqualificação e à marginalização social, baseado em uma crença equivocada acerca da identidade de uma pessoa, em que ela é considerada como menor, menos igual e pertencente a um grupo inferior.[407]

Em fato, os serviços de saúde, tanto públicos quanto privados, em muitos casos reproduzem ações e padrões discriminatórios, gerando e reforçando estigmas, em uma falta com o propósito de defender direitos humanos fundamentais e reduzir iniquidades em saúde. Neste sentido, uma série de denúncias revelam o tratamento potencialmente discriminatório a determinados usuários nos serviços de saúde no Brasil durante os últimos anos.[408]

Um exemplo notório deste tipo de situação dentro dos sistemas de saúde seria o menor o acesso ao exame para detecção de câncer de colo uterino entre mulheres não brancas, ainda que estas apresentarem frequência de consultas ginecológicas semelhante à das mulheres brancas.[409] Outra situação frequente é a recusa dos planos de saúde em custear tratamentos para doenças preexistentes.

Mesmo se trate de doenças declaradas na contratação do plano, as operadoras frequentemente alegam carência, negando ou limitando a assistência médica essencial. Tal prática é inaceitável e muitas vezes afeta diretamente pacientes com doenças crônicas e debilitantes, privando-os de tratamento e colocando sua saúde em risco.

Outro problema comum é a negativa de cobertura para procedimentos considerados de alto custo ou complexidade. Algumas operadoras podem alegar que determinados tratamentos não fazem parte do rol de procedimentos obrigatórios da Agência Nacional de Saúde Suplementar - ANS ou restringem o acesso a tratamentos introduzidos, causados em prejuízos sofridos para a saúde dos beneficiários.

A postura discriminatória dos planos de saúde também pode ser percebida quando as operadoras negam ou restringem o acesso a certos procedimentos médicos ou

407 GOFFMAN, E. Estigma: notas sobre a manipulação da identidade deteriorada. Rio de Janeiro: Zahar; 1982, p. 39.

408 MASSIGNAM, F. M.; BASTOS, J. L. D.; NEDEL, F. B. Discriminação e saúde: um problema de acesso. Epidemiologia e Serviço de Saúde, v. 24, n. 3, p. 544-541, 2015, p. 541. Disponível em: http://dx.doi.org/10.5123/S1679-49742015000300020. Acesso em: 7 jun. 2022.

409 A pesquisa intitulada *Coverage and focus of a cervical cancer prevention program in southern Brazil. Rev Panam Salud Publica*, de 2004 demonstrou ser menor o acesso ao exame para detecção de câncer de colo uterino entre mulheres não brancas, apesar de estas apresentarem frequência de consultas ginecológicas semelhante à das mulheres brancas. QUADROS, C. A. T.; VICTORA, C. G.; COSTA, J. S. D. Coverage and focus of a cervical cancer prevention program in southern Brazil. Revista Pan American Journal of Public Health, v. 16, n. 4, 2004. Disponível em: https://www.scielosp.org/pdf/rpsp/2004.v16n4/223-232. Acesso em: 30 ago. 2022.

tratamentos com base em características pessoais dos segurados, como idade, histórico médico, gênero. No ano de 2021, a 25ª Vara Cível da Comarca de Fortaleza/CE, nos autos de uma Ação de Obrigação de Fazer c/c Pedido de Tutela Antecipada, julgou procedente o pedido do autor para compelir a operadora de saúde a restabelecer o plano de saúde do promovente, e pagar danos morais arbitrados em R$ 10.000,00 (dez mil reais). Na ocasião, o autor alegou que por ser dependente químico e possuir histórico de internações por conta de sua doença, a operadora de saúde teria cancelado o seu plano de saúde, de forma imotivada e sem observância dos requisitos legais[410].

Não é surpresa que diante de situações como estas, milhares consumidores brasileiros tenham vindo a acionar o Poder Judiciário em busca de seus direitos. A jurisprudência revela que os tribunais brasileiros têm decidido na maioria dos casos, a favor dos beneficiários, reconhecendo o caráter abusivo da negativa de cobertura e determinando que os planos de saúde cobrem os tratamentos necessários.[411]

---

410 PROCESSO CIVIL. APELAÇÃO CÍVEL. PLANO DE SAÚDE COLETIVO. RESCISÃO DO CONTRATO UNILATERALMENTE PELA OPERADORA DE SAÚDE. AUSÊNCIA DE NOTIFICAÇÃO PRÉVIA DO BENEFICIÁRIO. IMPOSSIBILIDADE. CONTINUIDADE DE TRATAMENTO DO PACIENTE. DECISÃO DE PRIMEIRO GRAU QUE DETERMINOU A REATIVAÇÃO DO PLANO DE SAÚDE DO SEGURADO E FIXOU DANOS MORAIS. MANUTENÇÃO DA SENTENÇA. RECURSO CONHECIDO E NÃO PROVIDO. 1. Trata-se de Apelação Cível interposta por Central Nacional Unimed - Cooperativa Central, adversando sentença proferida no processo nº 0176041-44.2018.8.06.0001, em curso na 25ª Vara Cível da Comarca de Fortaleza/CE, que, nos autos da Ação de Obrigação de Fazer c/c Pedido de Tutela Antecipada, julgou procedente o pedido autoral para compelir a operadora de saúde demandada a restabelecer o plano de saúde do promovente, e para condenar a promovida em danos morais arbitrados em R$ 10.000,00 (dez mil reais). 2. Alega o promovente/Apelado que, por ser dependente químico (CID 10 – F19.2) e possuir histórico de internações por conta de sua doença, a operadora de saúde teria cancelado o seu plano de saúde, de forma imotivada e sem observância dos requisitos legais. Argumenta que não fora notificado previamente da rescisão unilateral pela Cooperativa Médica, o que ensejaria a reparação pelos danos morais experimentados, ante a negativa de cobertura para tratamento de enfermidade grave. 3. Recorrente sustenta que, por ser o beneficiário contratante de plano de saúde na modalidade coletivo empresarial, não se aplicariam as regras de cancelamento dos planos individuais, não havendo qualquer abusividade no cancelamento do contrato em decorrência da inadimplência, que perfez um atraso de 30 dias. 4. Entendimento do Superior Tribunal de Justiça no sentido de ser possível a rescisão unilateral do contrato coletivo, imotivadamente, após a vigência do período de 12 meses e mediante prévia notificação da outra parte. Precedentes do STJ favoráveis ao arbitramento do dano moral em razão do cancelamento indevido de plano de saúde. 5. Recurso Apelatório conhecido e negado provimento. ACÓRDÃO Vistos, relatados e discutidos estes autos de Apelação nº 0176041-44.2018.8.06.0001, em que é apelante Central Nacional Unimed - Cooperativa Central, e apelado Mario Fiais dos Santos. Acordam os Desembargadores integrantes da Primeira Câmara de Direito Privado do Tribunal de Justiça do Estado do Ceará, por unanimidade de votos, em conhecer do presente recurso, mas para negar-lhe provimento, nos termos do voto do Relator, parte integrante desta decisão. Fortaleza, 17 de fevereiro de 2021. Presidente do Órgão Julgador DESEMBARGADOR FRANCISCO MAURO FERREIRA LIBERATO Relator. TJ-CE - AC: 01760414420188060001 CE 0176041-44.2018.8.06.0001, Relator: FRANCISCO MAURO FERREIRA LIBERATO, Data de Julgamento: 17/02/2021, 1ª Câmara Direito Privado, Data de Publicação: 17/02/2021.

411 De acordo com Conselho Nacional de Justiça - CNJ, no ano de 2019 foram registrados 1,6 milhão de processos relacionados à saúde no Judiciário brasileiro. Destes, cerca de 70% se referiam a demandas contra planos de saúde. O levantamento também aponta que os processos relacionados à saúde suplementar cresceram 33,7% entre 2016 e 2019. BRASIL. Conselho Nacional de Justiça. Justiça em números. CNJ, Brasília, 2021. Disponível em: https://www.cnj.jus.br/programas-e-acoes/pj-justica-em-numeros/. Acesso em 20 de mai. 2023.

Em 2022, o TJDF se manifestou negando provimento ao recurso de uma operadora de saúde que negou a cobertura de uma cirurgia de emergência alegando má-fé do consumidor em relação a uma doença pré-existente. Entendeu o tribunal na ocasião que segundo o art. 11 da Lei n. 9.656/1999, é vedada a exclusão de cobertura às doenças e lesões preexistentes à data de contratação dos produtos após vinte e quatro meses de vigência do aludido instrumento contratual, cabendo à respectiva operadora o ônus da prova e da demonstração do conhecimento prévio do consumidor ou beneficiário. Conforme entendimento do relator a negativa do plano de saúde em custear tratamento médico indispensável à saúde do segurado inflige sofrimento muito maior que um mero descumprimento contratual, ensejando indenização por dano moral, cujo valor fixado deve atender ao bom senso, à proporcionalidade e à razoabilidade, mostrando-se satisfatório para representar um desestímulo à prática de novas condutas pelo agente causador do dano e suficiente para oferecer digna compensação ao autor[412].

Tais decisões têm um papel fundamental em garantir que os beneficiários sejam tratados de forma justa e que recebam os cuidados médicos recebidos, independentemente de suas condições de saúde[413]. A postura discriminatória de algumas operadoras representa um desafio significativo para o sistema de saúde suplementar no Brasil, demandando medidas regulatórias e de fiscalização mais rigorosas por parte da ANS para proteger os direitos dos consumidores. Contudo, as mudanças viabilizadas pelas tecnologias e bancos de dados trouxe novos fatores que adicionaram pesos significativos nas questões envolvendo planos de saúde.

---

412 Civil. Consumidor. Apelação cível. Plano de saúde. Lei n. 9.656/1998. Cirurgia. Emergência. Cobertura devida. Doença preexistente. Má-fé. Não comprovação. Danos morais. TJ-DF 07262883720218070001 1634188, Relator: Getúlio de Moraes Oliveira, Data de Julgamento: 26/10/2022, 7ª Turma Cível, Data de Publicação: 21/11/2022. BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. (2ª Turma Cível). **Apelação Cível n. Processo: 20151410079609APC (0008397-15.2015.8.07.0014**). Direito civil, do consumidor e processual civil. Ação de conhecimento com preceito cominatório. Reparação por danos morais. Plano de saúde. Súmula 469, stj. Recusa de cobertura de cirurgia bariátrica (gastroplastia redutora). Doença peexistente. Migração de plano de saúde. Carência. Cobertura parcial temporária. Não incidência. Danos morais. Cabimento. Recurso improvido. Apelante(s): Bradesco Saúde S/A Apelado(s) : Daise Rodrigues de Franca Relator: Desembargador João Egmont. Acórdão n.: 1080743. Brasília: Poder Judiciário da União, 2018. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&controladorId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.ControladorBuscaAcordao&visaoAnterior=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=resultado&comando=abrirDadosDoAcordao&enderecoDoServlet=sistj&historicoDePaginas=buscaLivre&quantidadeDeRegistros=20&baseSelecionada=BASE_ACORDAOS&numeroDaUltimaPagina=1&buscaIndexada=1&mostrarPaginaSelecaoTipoResultado=false&totalHits=1&internet=1&numeroDoDocumento=1080743. Acesso em: 11 ago. 2022.

413 Neste sentido, o posicionamento do STJ quanto ao tema: "A relação jurídica estabelecida entre o paciente e a operadora de plano de saúde é pautada por regras de ordem pública, cabendo ao Judiciário, em cada caso concreto, a análise e a aplicação das normas e princípios que regem a matéria". BRASIL. Superior Tribunal de Justiça. **REsp nº 1.533.019 – SP**. Relator: Ministro Paulo de Tarso Sanseverino, Julgamento em 08/08/2017. 2017.

Há anos, o Brasil lida com o problema da discriminação nos serviços de planos de saúde. Conforme interesses envolvidos, e as negativas vinham motivadas por questões econômicas ou de raça, porém, mais recentemente percebe-se a presença de questões e características identitárias mais aprofundadas e íntimas, o que abre questionamento quanto ao sigilo dos dados de saúde. Significa dizer, que as operadoras encontram na análise de dados sensíveis, parâmetros que condicionam sua oferta de cobertura e serviço, abrindo margem a uma série de negativas que por seu caráter prejudicam, não apenas o indivíduo já fragilizado por sua situação de saúde, mas famílias inteiras, que se veem obrigadas a arcar com despesas não previstas e enfrentar o desgaste da busca de amparo judicial para assegurar os direitos contratados.

Em que pese o forte exemplo das operadoras de planos de saúde, não se deve esquecer que uma problemática similar pode ser constatada nas empresas de seguro de vida, bem como em outros tipos de serviços. Informações sobre doenças genéticas influenciam diretamente nos contratos de seguro de vida, que por exemplo poderiam negar a cobertura ou aumentar as taxas para um indivíduo com base em suas informações genéticas, geradas em benefícios financeiros e dificuldades na garantia de proteção adequada.

Até mesmo nas práticas esportivas é possível encontrar exemplos de como os dados sensíveis de saúde podem suscitar ações discriminatórias. Basta recordar o tal caso de uma jogadora que foi excluída da seleção brasileira de vôlei em virtude de uma de suas características genéticas.[414] Discriminação genética é a expressão que surgiu e tem sido utilizada para descrever o fenômeno segundo o qual as pessoas são discriminadas em virtude de características individuais ou familiares presentes no genótipo[415].

Esses exemplos destacam como os dados de saúde podem afetar a vida prática dos titulares dessas informações, perpetuando desigualdades e violando seus direitos fundamentais. Deste modo, o papel da ANPD e de todo o arcabouço legal que versa

414 O teste para identificação de portadores do traço falciforme foi adotado pela Confederação Brasileira de Vôlei como um exame de rotina para os atletas. O exame foi adotado pela CBV em virtude dos supostos riscos que a presença do traço falciforme poderia ocasionar à saúde e ao desempenho das atletas. Em 2004, uma jogadora foi excluída da seleção oficial brasileira de vôlei em virtude de uma de suas características genéticas, trazem diferentes conceitos de discriminação genética, segundo os quais esse é um neologismo usado para descrever o novo fenômeno moral e sociológico provocado pela evolução dos diagnósticos genéticos: a discriminação da pessoa devido a características individuais ou familiares presentes em seu genótipo (em sua configuração genética), ou, em outras palavras, a opressão do indivíduo por causa do seu patrimônio genético. GUEDES, C.; DINIZ, D. Um caso de discriminação genética: o traço falciforme no Brasil. Physis: Revista de Saúde Coletiva, Rio de Janeiro, v. 17, n. 3, p. 501-520, 2007, p. 503. Disponível em: https://www.scielo.br/j/physis/a/HjmCfLJtKbMLBSdNZF3STSK/?format=pdf&lang=pt. Acesso em: 13 jan. 2023.

415 GELLER, L. Current developments in genetic discrimination. *In*: ALPER, J. *et al* (Eds.). The doubleedged helix: social implications of genetics in a diverse society. Baltimore: The Johns Hopkins University Press, 2002.

quanto a proteção de dados ganham ainda mais relevância. É essencial que as empresas e instituições que lidam com dados de saúde estejam em conformidade com a LGPD e demais medidas protetivas, para garantir a privacidade e segurança dessas informações pessoais, evitando o alargamento da via de exclusão no Brasil.

5.7 Desdobramentos e consequências da utilização indevida de dados sensíveis de saúde na esfera individual de seu titular

A proteção de dados pessoais configura requisito essencial para o Estado Democrático de Direito e necessita ser interpretado sob a luz da dignidade da pessoa humana e do direito à privacidade. Com a ampliação de recursos tecnológicos, com algoritmos cada vez mais sofisticado, multiplica-se diariamente a capacidade de tratamento de dados pessoais. Tal evolução é frequentemente festejada sob o prisma da otimização, velocidade e aumento da qualidade de certos processos, mantendo sob a sombra uma série de efeitos colaterais sob os quais a maior parcela da população brasileira desconhece.

Ao se falar em dados sensíveis de saúde, resta claro tratamento de grandes bases de dados por meio de *softwares* e algoritmos conduz a uma série de análises probabilísticas e resultados que podem reduzir ou mesmo retirar a capacidade de autonomia do indivíduo e o seu direito de acesso ao consumo de bens e serviços e a determinadas políticas públicas.[416] Mas pela peculiaridade do conteúdo envolvido que revela detalhes do quadro de saúde física ou mental de uma pessoa, é possível antever outros tipos de consequências e desdobramentos mediante a exposição indevida de dados sensíveis de saúde.

Embora os dados de saúde sejam prioritariamente associados a prontuários, exames, diagnósticos e tratamentos, eles também contemplam outros tipos de informação, que podem ser classificadas indiretas, embora igualmente contemplem informações pessoais. Conforme essa visão puramente didática, dados diretos de saúde são aqueles que são obtidos diretamente dos pacientes ou indivíduos e fornecem informações precisas e discriminadas sobre sua condição médica e histórico de saúde.

Enquanto os dados indiretos de saúde se referem a informações coletadas de fontes secundárias ou registradas de forma indireta, muitas vezes sem o conhecimento ou

416 MULHOLLAND, op. cit., 2018, p. 173.

consentimento explícito do indivíduo.[417] A junção destas duas linhas de dados forma um material detalhado considerado extremamente útil para fins de pesquisa, marketing e análise de tendências, mas com igual potencial para levantar questões de privacidade e ética quando não são devidamente protegidos ou usados de forma correta.

Quadro 5 - Dados Diretos e Indiretos na Esfera da Saúde

	Dados Diretos de Saúde	Dados Indiretos de Saúde
Definição	Dizem respeito às informações propriamente clínicas, registradas em prontuários médicos.	Os dados de saúde indiretos, por sua vez, não seriam originados necessariamente no ambiente clínico. Eles também informam sobre o quadro de saúde de determinada pessoa, mas de maneira indireta.
Exemplos	Exames laboratoriais; Imagens médicas (como radiografias); Anamnese (relatório de sintomas narrados pelos pacientes); Valores de pressão, peso e frequência cardíaca; Relatos clínicos; Prescrição de medicamentos; Diagnósticos.	Fotos; Dados de localização; Voz; Pesquisas na internet; Velocidade de digitação.

Fonte: Elaborado pela autora.

A esta altura, a classificação em dados diretos ou indiretos de saúde tem a função de auxiliar na compreensão da ideia de que quando informações como histórico médico, diagnósticos ou tratamentos, associadas a nome, endereço e fotos pessoais, são expostas sem consentimento, a pessoa diretamente atingida tende a sentir-se extremamente constrangida e vulnerável. Episódios de vazamento de dados de saúde, conforme já exemplificado nos capítulos anteriores, tem apresentado frequência assustadora. Em muitos casos os dados são vendidos e utilizados de forma silenciosa, mas em outras situações, ocorre a exposição na internet.

O vazamento dados pessoais de saúde reportado em abril de 2023 pelo site *Canaltech* divulgou nome completo, CPF e data de nascimento associados a registros relacionados à utilização de planos de saúde entre 2016 e 2020, com direito a informações de procedimentos e as datas em que foram realizados.[418] O sentimento de exposição e

417 MATSUMOTO, M. M. S. Seus dados médicos estão mais expostos do que você imagina: considerações sobre a questão da privacidade de dados de saúde, quem tem acesso a eles e quais os impactos para a saúde e inovação. IPEA - Centro de Pesquisa em Ciência, Tecnologia e Sociedade, Rio de Janeiro, 2020. Disponível em: https://www.ipea.gov.br/cts/pt/central-de-conteudo/artigos/artigos/105-seus-dados-medicos-estao-mais-expostos-do-que-voce-imagina Acesso em 24 maio 2023.

418 Neste sentido a notícia "Vazamento expõe quase 6 milhões de dados de saúde dos brasileiros" divulgada em 12 de abril de 2023 pelo site Canaltech. Um grande vazamento de dados expôs mais de 5,8 milhões de registros de saúde, com consultas, procedimentos, exames e outros realizados por uma importante seguradora brasileira. Disponível em https://canaltech.com.br/seguranca/vazamento-expoe-quase-6-milhoes-de-dados-de-saude-dos-brasileiros-246314/. Acesso em 24 de jun de 2023.

invasão de privacidade em um caso como este pode gerar, além de prejuízos materiais, grande angústia emocional, ansiedade e vergonha, levando a efeitos negativos na saúde mental do indivíduo.

A exposição de dados sensíveis de saúde em redes sociais também representa uma preocupação crescente. Com o uso generalizado das redes sociais, as informações pessoais podem ser compartilhadas de forma inadvertida ou intencional, expondo a intimidade dos indivíduos. Essa prática pode levar a situações de *bullying*, assédio ou relação, causando sérios danos psicológicos e sociais ao titular dos dados. Considere uma situação na qual uma pessoa que tem informações sensíveis sobre um tratamento psiquiátrico divulgado em uma rede social sem sua permissão. Essa exposição pode levar a um estigma social, afetando a imagem e acreditando da pessoa, bem como sua vida profissional e relações pessoais[419].

Além disso, a mostra ilimitada de dados sensíveis também pode representar um risco de chantagem. Os cibercriminosos podem se aproveitar dessas informações acessíveis para extorquir dinheiro ou obter favores sob a ameaça de revelar dados comprometedores publicamente. Embora não se tenha até o presente momento relatos deste tipo de ação no Brasil, um episódio ocorrido na Finlândia no qual informações de pacientes de uma grande rede de psicoterapia foram roubadas por um invasor, que passou a chantagear centenas de pessoas em busca de dinheiro, chama a atenção para mais uma possível consequência da exposição indevida, neste caso criminosa de dados sensíveis de saúde.[420]

A dor e a pressão emocional experimentada por um indivíduo ao sofrer a ameaça de ter informações de foro íntimo expostas na internet dificilmente pode ser mensurada. Os constantes ataques a bancos de dados de saúde, podem ocasionar lesões permanentes na esfera psicológica da vítima de vazamento de dados além de perpetuar um ciclo de vulnerabilidade e violação de privacidade.

---

419 Tome-se o exemplo do estigma aos transtornos mentais. O estigma contra a saúde mental está enraizado na história. Pacientes com transtornos mentais graves sempre foram tratados de forma isolada, isolados da sociedade e vistos como loucos, gerando inclusive resistência aos tratamentos psicológicos ou psiquiátricos em virtude de desconhecimento e preconceito. CASSIANO, A. P. C.; MARCOLAN, J. F.; SILVA, D. A. Atenção primária à saúde: estigma a indivíduos com transtornos mentais. Revista de enfermagem da UFPE on line, Pernambuco, v. 13, 2019, p. 5. Disponível em: https://periodicos.ufpe.br/revistas/revistaenfermagem/article/view/239668. Acesso em: 29 mar. 2023.

420 A notícia intitulada "O pesadelo dos pacientes chantageados após vazamento das sessões de terapia" repercutiu pelo mundo e no Brasil foi veiculada pelo portal G1 em outubro de 2020. O PESADELO DOS PACIENTES chantageados após vazamento das sessões de terapia. G1, São Paulo, 2020. Disponível em: https://g1.globo.com/mundo/noticia/2020/10/27/o-pesadelo-dos-pacientes-chantageados-apos-vazamento-das-sessoes-de-terapia.ghtml. Acesso em: 2 jun 2023.

Assim, há que se considerar que a exposição de dados sensíveis de saúde vai além das questões legais e de proteção de dados. A este ponto tem-se efeitos devastadores na vida dos indivíduos, que causam constrangimento, transtorno emocional, estigma social e até mesmo expondo-os a riscos de chantagem. Por isso, é possível que empresas, instituições e indivíduos adotem medidas rigorosas para garantir a segurança e a privacidade dos dados pessoais e proteger a privacidade dos titulares dessas informações.

Ao buscar uma compreensão das consequências da utilização indevida de dados sensíveis de saúde na esfera individual de seu titular, tem-se delicados efeitos pessoais e sociais. Mas uma observação cuidadosa da questão, permite que se vislumbre um viés pouco mencionado, mas de extrema relevância: a possibilidade de que tais repercussões atinjam terceiros juridicamente conectados aos titulares dos dados de saúde.

O conhecimento da herança genética, foi alcançado com os avanços da medicina que hoje disponibiliza testes genéticos cada vez mais acessíveis, que tem o importante papel de informar quanto a probabilidade de certas doenças ou condições de saúde, permitindo tratamento precoce ou medidas preventivas, conforme o caso. Porém, estas informações podem ser utilizadas como base para ações discriminatórias, como já discutido.[421]

Uma possível discriminação genética, perpassa a figura do titular dos dados e alcança também a terceiros como familiares e descendentes, podendo atingir um caráter múltiplo. São situações que poderão ser percebidas no momento de contratar um seguro de vida e de saúde, no campo das permissões ou autorizações oficiais ou nas relações creditícias, levando indivíduos a serem considerados defeituosos ou não aptos para participar de certas relações sociais[422]. Desta forma, conclui-se que dados genéticos, classificados como dados sensíveis de saúde podem criar uma dinâmica de estigma e exclusão que é transmitida de uma geração para outra, prejudicando continuamente os membros de uma família.

Em tempos de avanços tecnológicos e cientificação dos hábitos de vida, a visão da medicina foi transformada, alterando o foco do copo físico e abrindo espaço para

421 HAMMERSCHMIDT, D.; OLIVEIRA, J. S. Direito à Intimidade Genética: um contributo ao estudo dos direitos da personalidade. Revista Jurídica Cesumar, Maringá, v. 6. n. 1. p. 421-455, 2006, , p. 421. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/320. Acesso em: 29 jun. 2023.

422 A discriminação baseada no patrimônio genético prevê a existência de diferentes graus no reconhecimento dos direitos de grupos predispostos geneticamente a determinadas enfermidades ou limitações. LOCATELI, C. C.; PANDOLFO, A. C. A intimidade genética: direito à intimidade e à informação na proteção dos dados genéticos. Revista do CEJUR/TJSC: Prestação Jurisdicional, Florianópolis, v. 1, n. 2, p. 92-119, 2014, p. 3. Disponível em: https://doi.org/10.37497/revistacejur.v1i2.67. Acesso em: 13 abr. 2023.

discutir fatores de risco, em um movimento que aumenta consideravelmente os efeitos da autovigilância e do autocontrole na sociedade.[423] Assim, é necessário um olhar quanto aos dados genéticos, que compõe a esfera dos dados sensíveis de saúde. São estes considerados únicos, estruturais, probabilísticos e geracionais, permitindo por meio de sua análise diagnósticos apurados que revelam não somente a qual espécie aqueles genes pertencem, mas também a qual indivíduo e suas possibilidades de vir a de desenvolver alguma doença ou de transmitir suas doenças para seus descendentes.[424]

Ações discriminatórias, nestes casos, podem partir tanto do Estado, como de grupos empresariais ou sociais, que em um olhar reducionista, venham a considerar a pessoa humana enquanto objeto resultante do conjunto de genes que possui, os quais têm a probabilidade de causar doenças e determinar comportamentos que não são de interesse daqueles grupos ou entes estatais e por tanto, não apresentam valor.[425]

Não é razoável que apenas porque sua carga genética apresentar diferença ou uma pré-disposição que não se sabe se irá ou não ser concretizada, a pessoa venha a ser desconsiderada, ignorando o processo de construção da identidade por meio de elementos ambientais, educacionais e experiências pessoais e culturais, gerando discriminação, perda de oportunidades e danos emocionais decorrentes desse processo. Por isso, mais uma vez se reafirma que face aos inúmeros desdobramentos ocasionados pela exposição não consentida de dados sensíveis de saúde, é preciso caminhar com cautela por um terreno acidentado que ainda não permite a visualização da sua total extensão, e consequentemente da extensão dos danos ali observados.

Ainda no ano de 2003, a questão quanto a segurança da informação associada a dados genéticos ganhou atenção com a aprovação da Declaração Internacional sobre os Dados Genéticos Humanos, que tem por objetivo geral a proteção dos dados genéticos da pessoa, considerando procedimentos de coleta, utilização e conservação, a fim de assegurar os direitos fundamentais do indivíduo. Tal documento configura um importante avanço na discussão da questão e é utilizada em conjunto com legislações específicas e políticas públicas para reforçar o direito a privacidade, indicando expressamente restrições de acesso deste tipo de dados por terceiros, salvo

423 Considera-se fator de risco (FR) alguma exposição que aumente a probabilidade de ocorrência de uma doença ou agravo à saúde, podendo ocorrer em qualquer parte da cadeia causal. BARBOSA, L. M. M.; MACHADO, C. B. Glossário de Epidemiologia e Saúde. *In*: ROUQUAYROL, M. Z.; GURGEL, M. (eds.). Rouquayrol: Epidemiologia & Saúde. 7. ed. Rio de Janeiro: MedBook. 2013, p.663.

424 NAVES, B. T.O. Direitos de Personalidade e Dados Genéticos: Revisão crítico-discursiva dos direitos de personalidade à luz da natureza jurídica dos dados genéticos humanos. Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC. 2010, p. 53.

425 LIMA NETO, F. V. O direito de não sofrer discriminação genética: uma nova expressão dos direitos de personalidade. Rio de Janeiro: Lumen Juris, 2008, p.61,

quando verificada a hipótese de relevante motivo de interesse público restritivamente previsto pelo direito interno, em consonância com os direitos humanos do direito internacional; ou tendo havido prévio, livre, esclarecido (com informação acerca de riscos e consequências) e expresso consentimento da pessoa, que conforme disposto no artigo 9º da Declaração, pode ser retirado a qualquer momento.[426]

Merece destaque no texto, a indicação de que que deverão ser feitos todos os esforços a fim de impedir o uso de modo discriminatório dos dados genéticos. [427] Há um claro posicionamento contra a ideia do reducionismo genético[428], ao enfatizar que a identidade humana não deve ser limitada a seus traços genéticos, excluindo-se por completo a consideração da influência de fatores externos que permeiam a formação do indivíduo. O Brasil, não apenas se comprometeu a adotar os princípios dessa Declaração, mas expôs entre outras preocupações, a necessidade de gerir os riscos ligados à coleta, ao processamento e à estocagem de dados genéticos. Contudo, após o transcurso de quase duas décadas, as legislações e políticas públicas mais modernas ainda não respondem de forma satisfatória a questão.

---

426 Artigo 14 da Declaração internacional sobre os dados genéticos humanos: Os Estados deverão desenvolver esforços no sentido de proteger, nas condições previstas pelo direito interno em conformidade com o direito internacional relativo aos direitos humanos, a vida privada dos indivíduos e a confidencialidade dos dados genéticos humanos associados a uma pessoa, uma família ou, se for caso disso, um grupo identificável. Os dados genéticos humanos, os dados proteómicos humanos e as amostras biológicas associados a uma pessoa identificável não deverão ser comunicados nem tornados acessíveis a terceiros, em particular empregadores, companhias de seguros, estabelecimentos de ensino ou família, se não for por um motivo de interesse público importante nos casos restritivamente previstos pelo direito interno em conformidade com o direito internacional relativo aos direitos humanos, ou ainda sob reserva de consentimento prévio, livre, informado e expresso da pessoa em causa, na condição de tal consentimento estar em conformidade com o direito interno e com o direito internacional relativo aos direitos humanos. A vida privada de um indivíduo que participa num estudo em que são utilizados dados genéticos humanos, dados proteómicos humanos ou amostras biológicas deverá ser protegida e os dados tratados como confidenciais. UNESCO - ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, CIÊNCIA E CULTURA. **Declaração internacional sobre os dados genéticos humanos**. Portugal: Unesco, 2004. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_inter_dados_genericos.pdf. Acesso em Acesso em: 29 jun. 2023.

427 Artigo 7° da Declaração internacional sobre os dados genéticos humanos: (a) Deverão ser feitos todos os esforços no sentido de impedir que os dados genéticos e os dados proteómicos humanos sejam utilizados de um modo discriminatório que tenha por finalidade ou por efeito infringir os direitos humanos, as liberdades fundamentais ou a dignidade humana de um indivíduo, ou para fins que conduzam à estigmatização de um indivíduo, de uma família, de um grupo ou de comunidades. (b) A este respeito, será necessário prestar a devida atenção às conclusões dos estudos de genética de populações e dos estudos de genética do comportamento, bem como às respectivas interpretações. Organização das Nações Unidas para a Educação, Ciência e Cultura. Idem.

428 O reducionismo epistemológico orienta as pesquisas genéticas desde seu princípio e se posiciona no sentido de buscar reduções, ou seja, explicar os fenômenos dos níveis mais altos de organização com base em entidades de um domínio mais fundamental. Exemplos: explicar o fenótipo em termos do genótipo, ou reduzir a fisiologia em termos das interações bioquímicas do organismo. FERREIRA, L. R. G. Filosofia da Edição Genômica: reducionismo e experimentalismo em engenharia genética. 2022. Dissertação (Mestrado em Filosofia) - Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2022, p. 33. Disponível em: https://doi.org/10.11606/D.8.2022.tde-28072022-180905. Acesso em: 11 maio 2023.

A ciência moderna não apenas permite prever, mas tornou acessível exames que possibilitam prever a probabilidade da ocorrência de doenças de origem genética. A título de exemplo, podem ser mencionadas enfermidades como câncer de mama, síndrome de Patau, ELA - esclerose lateral amiotrófica, diabetes, transtornos mentais, entre outras. Por um lado, esses testes são essenciais para viabilizar diagnósticos precoces e indicar tratamentos com maior probabilidade de sucesso, mas em uma via secundária poderiam estes resultados serem utilizados como motivação para práticas discriminatórias[429].

Verifica-se um perigoso risco de que indivíduos ou que determinados grupos venham a ser estigmatizados como defeituosos e de "menor valor", gerando diferentes níveis de tratamento conforme uma situação que pode ainda não ter se concretizado.[430] A mera pré-disposição a determinada doença já seria suficiente para a exclusão, em um processo que pode ser automaticamente replicado não apenas para uma, mas para diversas pessoas com as quais se verifique conexão genética.

Contudo, é preciso recordar que mesmo que o indivíduo apresente em seu histórico genético uma predisposição a determinadas doenças estas podem, ou não, se desenvolver[431]. Existem inúmeros fatores tais como comportamento, valores, cultura, alimentação, recursos e ambiente social, que poderão influenciar o desenvolvimento ou não da enfermidade pré-disposta. Além disso, a identificação permitiria tratamento e intervenções precoces. Mas para muitos, tais argumentos pouco valem diante do risco de redução do potencial de lucro associado a uma pessoa.

Outra grande questão da discriminação genética é que suas consequências se estendem por um campo indefinido, do qual não é possível conhecer as dimensões e nem o tempo de alcance. São situações que vão desde a dispensa de um emprego, ter

429 A divulgação das informações genéticas de um indivíduo pode conduzir ao reducionismo, ao determinismo genético, à estigmatização, à discriminação genética e à perda ou diminuição da capacidade de autodeterminação. LOCATELI; PANDOLFO, op. cit., p. 7.

430 Conforme a Convenção de Oviedo de 1997 - Convênio Europeu sobre Direitos Humanos e Biomedicina: Art. 12: Não se poderá proceder a testes predictivos de doenças genéticas ou que permitam quer a identificação do indivíduo como portador de um gene responsável por uma doença quer a detecção de uma predisposição ou de uma susceptibilidade genética a uma doença, salvo para fins médicos ou de investigação médica e sem prejuízo de um aconselhamento genético apropriado. Gabinete de Documentação e Direito Comparado. Procuradoria Geral da República. Convenção para a Protecção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina. PORTUGAL. Convenção para a Protecção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina. Oviedo: Gabinete de Documentação e Direito Comparado. Procuradoria Geral da República, 1997.

431 MYSSIOR, B. A. P. A.; SILVA, L. E. G. Discriminação genética: uma questão jurídica ou biológica? Revista de Biodireito e Direito dos Animais, Curitiba, v. 2, n. 2, p. 159-174, 2016, p.172. Disponível em: https://www.indexlaw.org/index.php/revistarbda/article/download/1381/pdf. Acesso em: 17 maio 2023.

acesso negado a um plano de saúde, não conseguir adotar uma criança, ser estigmatizado na escola ou não conseguir se relacionar amorosamente.[432]

A possibilidade de que dados pessoais sensíveis de saúde venham a ultrapassar a esfera individual de seu titular e influenciem a vida prática de outras pessoas com as quais partilha conexão genética e até da sua futura descendência é algo que merece cuidadosa atenção. Doenças, síndromes, transtornos físicos e mentais vistos como fatores indesejáveis no mercado de trabalho e nas relações de consumo, denotam o surgimento de uma perigosa linha de segregação, na qual o indivíduo é desconsiderado, passando simplesmente a ser lido através de dados e códigos, em contradição direta aos direitos fundamentais e o propósito de construção de uma sociedade justa e solidária.

432 Idem, p.169.

6 Capítulo 5 - A responsabilidade civil em consequência do vazamento de dados de saúde

O capítulo final desta pesquisa é dedicado a analisar os desdobramentos dos vazamentos de dados de saúde face ao instituto da Responsabilidade Civil. Para tanto, se inicia discutindo os caminhos e fundamentos da conexão entre a proteção de dados sensíveis de saúde e as responsabilidades mediante sua utilização indevida, conforme a esfera civil. A este ponto serão abordados os elementos de configuram a caracterização do dano face ao vazamento de dados de saúde, a fim de que se possa compreender em quais situações emergirá a responsabilização com o consequente dever de reparo.

Além disso, serão apresentadas e discutidas as dificuldades inerentes as possibilidades de indenização em virtude de vazamento de dados sensíveis de saúde e as delicadas nuances do arbitramento de valores face ao potencial discriminatório e lesivo das informações de saúde. O cenário proposto será arrematado com a análise de julgados dos tribunais brasileiros quanto a matéria, por meio da qual será possível traçar um panorama indicando a linha de interpretação que tem sido adotada quanto a matéria e as possiblidades de ofertar uma real proteção aos dados sensíveis de saúde para os cidadãos brasileiros.

6.1 Responsabilidade mediante o compartilhamento indevido de dados de saúde

Dados de saúde são poderosos instrumentos. Quando utilizados na via ética e legal, proporcionam benefícios preciosos para o indivíduo, que vulnerabilizado, busca meios de reestabelecer sua saúde, bem como auxiliam na efetivação das propostas do Estado para a concretização do direito à saúde. Porém, a força das informações ali contidas, quando utilizadas de maneira escusa, partindo da violação da privacidade dos titulares, apresentam surpreendente força lesiva.

Uma infração ou incidente de segurança ocorre quando dados pessoais são acessados, divulgados, modificados ou destruídos de forma não autorizada. São situações decorrentes de ataques cibernéticos, falhas de segurança, fuga de informações ou até mesmo negligência no tratamento desses dados, que ferem não apenas um, mas

diversos direitos, podendo gerar danos severos tanto na esfera patrimonial quanto moral de seu titular.

Primeiramente, há o risco de exposição de informações pessoais sensíveis, o que pode levar ao roubo de identidade, fraudes financeiras e chantagens. Tal é notícia anteriormente discutida, segundo a qual já se tem o registro de casos em que hackers invadem bancos de dados médicos de hospitais e roubam informações de pacientes para extorquir dinheiro deles ou vender os dados a terceiros. Além disso, a violação de dados, especialmente dados sensíveis de saúde, pode impactar negativamente na percepção dos titulares envolvidos e até mesmo de seus familiares e descendentes, prejudicando suas carreiras, relacionamentos pessoais e a sua vivência no contexto social. Não resta dúvidas de que respostas são necessárias para estes e outros casos decorrente de vazamento de dados de saúde.

Embora não estejam abarcados por essa pesquisa, cabe um pequeno adendo para mencionar que na esfera criminal, a exposição indevida de dados de saúde pode incluir diversos tipos penais. Enquanto a LGPD trouxe em suas previsões somente sanções administrativas, é válido buscar amparo no Código Penal para imputar os respectivos crimes às condutas delituosas que envolvam acesso, tratamento e utilização indevida de dados pessoais.

Conforme as peculiaridades da situação e os impactos sofridos pelos titulares de dados que tiveram suas informações pessoais expostas, é possível caracterizar estelionatos, práticas de hackeamento de dados[433], crimes contra a honra e formação de organização criminosa. Uma vez comprovada a violação da liberdade individual e a privacidade da titular dos dados, cabe ao Código Penal, atualizado no ano de 2021 para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet[434], apresentar as sanções adequadas[435].

---

433 Cabe lembrar que o hackeamento de informações se refere a prática de identificar e explorar vulnerabilidades em um sistema de computador ou rede, visando obter acesso não autorizado a dados pessoais ou organizacionais. RAYMOND, E. S. The new hack's dictionary (the jargon file). 3. ed. Cambridge: The MIT Press, 1996.

434 A lei nº 14.155, de 27 de maio de 2021 alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diário Oficial da União, Brasília, n. 1, 2021. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=14155&ano=2021&ato=3a4cXUU5UMZpWT48d. Acesso em: 12 jul. 2022.

435 Foram criadas criminalizações específicas, com penas próprias, em figuras típicas já definidas no diploma

Na hipótese do agente que realizou o ato de invasão ao sistema ou dispositivo informático, tem-se a previsão artigo 154-A do Código Penal[436], que indica como crime "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita", resultando em pena de reclusão, de um a quatro anos, e multa.

A destruição, inutilização ou alteração de dados pessoais sensíveis sem autorização pode configurar crime de dano qualificado a sistema de informática, previsto no artigo 313-A do Código Penal. Seria o caso do funcionário autorizado que vem a realizar ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano. [437]

A visão quanto ao crime de furto também foi alterada para incluir por meio do Furto § 4º-B incluído no artigo nº 155 do CP, a possibilidade de o ato ilícito ser realizado mediante fraude, cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo[438].

Quando se fala em responsabilidade por situações que envolvem de vazamento de dados, tem-se o desafio de identificar os fatores que concorreram para a quebra do dever

---

Penal, respectivamente, no crime de furto (art. 155, § 4º-B, CP) e no de estelionato (art. 171, § 2º-A, CP). As penas foram especialmente aumentadas, de quatro a oito anos de reclusão além de multa. Idem.

436 Para melhor compreensão sugere-se a leitura do restante do texto do mencionado artigo 154-A: § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido. Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. Ibid.

437 Código Penal, artigo, 313-A: Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. BRASIL, op. cit., 2021.

438 Código Penal, artigo nº 155, § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. Incluído pela Lei nº 14.155, de 2021. Idem.

de sigilo. É necessário verificar se a motivação do ataque se deu por vulnerabilidades do sistema, conduta técnica indevida, falhas de segurança da rede empresarial ou ausência de proteção adequada no armazenamento[439]. Neste raciocínio, há igualmente a demanda de apontar os sujeitos diretamente envolvidos na situação.

Conforme o já mencionado artigo 5º da LGPD a questão dos dados pessoais perpassa por quatro possíveis sujeitos: a) o titular: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento; b) o controlador: aquele que compete as decisões relativas ao tratamento de dados; c) o operador: aquele que realiza o tratamento de dados em nome do controlador e d) o encarregado: pessoa indicada pelo controlador que atua como canal de comunicação entre o titular, o controlador e a autoridade nacional de proteção de dados[440]. A depender da conduta utilizada que tenha vindo resultar em um vazamento de dados pessoais, o agente identificado como autor poderá ser enquadrado desde crimes patrimoniais até crimes contra a honra.

O legislador optou por estabelecer na LGPD apenas procedimentos administrativos para o mau uso de dados pessoais, deixando que as penas criminais específicas fossem definidas pelo Código Penal. Desta forma, cabe às autoridades e aos tribunais interpretar e aplicar as normas penais de acordo com cada caso concreto, tendo em vista a gravidade da violação e outras circunstâncias relevantes, sem prejuízo das sanções administrativas previstas pela LGPD.

A entrada em vigor dos artigos nº 52, 53 e 54 da LGPD ocorreu de forma escalonada, seguindo o cronograma originalmente estabelecido pela própria legislação. Para registro, a LGPD foi sancionada em agosto de 2018, mas sua aplicação prática foi gradual, com diferentes fases de modo a permitir que empresas e órgãos públicos se adaptem e se adequem às novas exigências quanto a proteção de dados. Inicialmente, a LGPD a entrada em vigor desses artigos seria imediata após a sanção, no entanto, o Governo Federal promulgou a Lei nº 14.010/2020, que dispôs sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado durante a pandemia da COVID-19, que acabou por adiar a aplicação das sanções ajustadas na LGPD para agosto de 2021.

Foi gerada uma grande expectativa em relação à vigência dessas regras tanto por parte das empresas e entidades que tratam dados pessoais, quanto dos próprios

439 SANDRIN, P. J. P. B.; SILVA, J. X. R. Possíveis reflexos penais da Lei Geral de Proteção de Dados. Migalhas, São Paulo, 2020. Disponível em: https://www.migalhas.com.br/depeso/320959/possiveis-reflexos-penais-da-lei-geral-de-protecao-de-dados. Acesso em: 16 jun. 2023.

440 LGPD, artigo nº5. Brasil, op. cit., 2018.

titulares dos dados, que buscavam maior segurança e proteção de suas informações. Muitas empresas se viram desafiadas a revisar suas políticas de privacidade, controle de segurança e designar um encarregado pelo tratamento de dados[441], conforme determinado pela norma.

O artigo 52 da LGPD é de extrema importância para assegurar o cumprimento da legislação, pois dispõe expressamente sobre como as obrigações administrativas podem ser aplicadas em caso de descumprimento das regras de proteção de dados pessoais. O texto estabelece medidas coercitivas com o objetivo de incentivar as empresas e entidades a adotarem práticas de tratamento de dados mais seguras e transparentes, garantindo a proteção dos direitos dos titulares. Conforme seu caput, a ANPD enquanto órgão responsável por fiscalizar e zelar pelo cumprimento da LGPD, pode aplicar diversos procedimentos administrativos, devendo atuar dentro dos ditames dos princípios da proporcionalidade e da razoabilidade.

A primeira medida indicada é a advertência com indicação de prazo para adoção de medidas corretivas. Trata-se de um procedimento de caráter mais brando, que serve como um aviso à empresa infratora sobre as irregularidades encontradas em seu tratamento de dados. A ponderação tem o propósito de alertar sobre a necessidade de correção e provisão às previsões da lei[442]. A segunda sanção, é a multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.[443] Caso a empresa não adote as devidas medidas corretivas após a advertência, a ANPD pode aplicar uma multa, fixada em valor pecuniário a ser pago pela empresa infratora.

Em sequência, há a disposição sobre multa diária, observado o limite total imposto pelo inciso II do mesmo artigo. A aplicação de multa diária é prevista para as infrações continuadas[444]. Ou seja, se a empresa persistir em descumprir as normas de proteção de dados após a imposição da multa simples. Nestes casos a ANPD pode estabelecer uma multa diária até que a irregularidade seja corrigida.

Além das multas, o artigo 52 da LGPD prevê a publicização da infração após devidamente apurada e confirmada a sua ocorrência. informando a natureza da violação

441 Conforme o artigo nº5, inciso VII da LGPD, considera-se encarregado a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Idem.

442 LGPD, artigo nº 52, I. Ibid.

443 LGPD, artigo nº 52, II. Ibid.

444 LGPD, artigo nº 52, III. Ibid.

e os dados envolvidos[445], garantindo a transparência e o conhecimento público de práticas irregulares; O bloqueio dos dados pessoais a que se refere a infração até a sua regularização, de modo a impedir o acesso e a utilização dos dados até que a situação seja regularizada[446].

Em situações mais extremas nas quais a empresa não esteja apta a corrigir as falhas encontradas, a ANPD pode determinar a eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; a suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período. E por fim, a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.[447]

O artigo 53 da LGPD trata das multas que podem ser aplicadas em caso de infrações, prevendo valores que variam de acordo com a gravidade e a natureza das violações[448]. A preocupação com a definição de valores tem como objetivo garantir um ponto de convencimento para que as organizações venham a adotar medidas de proteção de dados, uma vez que o ônus financeiro das satisfações pode ser significativo para os negócios. Já o artigo 54 da Lei, indica que o valor da sanção de multa diária aplicável às infrações previstas na Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.[449]

Na prática, a implementação dos artigos 53 e 54 representa uma mudança significativa no cenário da proteção de dados no Brasil. Antes da LGPD, muitas empresas e entidades públicas operavam com restrições em relação ao tratamento de dados pessoais, o que aumentava os riscos de vazamento, uso indevido de informações e violação à privacidade dos cidadãos. Com a entrada em vigor desses dispositivos, as organizações são impelidas a adotar políticas e procedimentos mais rigorosos de

445 LGPD, artigo nº 52, IV. Ibid.

446 LGPD, artigo nº 52, IV. Ibid.

447 LGPD, artigo nº 52, V, VI, X, XI e XII. Ibid.

448 LGPD, artigo nº 52. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. Ibid.

449 LGPD, artigo nº 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional. Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. Ibid.

segurança e privacidade de dados, buscando evitar incidentes e aumentando a confiança do público.

É fundamental ressaltar que as garantias aplicadas pela ANPD devem ser proporcionais à gravidade e à natureza das infrações cometidas. A LGPD não pretende inviabilizar empresas, mas sim de estimular a conformidade e o respeito com os direitos dos titulares de dados. Conforme procedimento previsto, ao ser autuada a empresa infratora tem o direito de apresentar defesa administrativa contra as taxas impostas.

A leitura cuidadosa das sanções dispostas no texto da LGPD revela que o legislador não buscou apenas punir os infratores, mas principalmente, criar uma cultura de respeito à privacidade e à proteção de dados no Brasil, garantindo que as informações pessoais dos cidadãos sejam tratadas de forma responsável e segura. A entrada em vigor destes artigos, foi um chamado as organizações para investir em medidas de segurança da informação, revisar suas políticas de privacidade e estabelecer programas de treinamento para seus colaboradores a fim de garantir o cumprimento da LGPD.

Nesse contexto, a ANPD desempenha um papel fundamental, fiscalizando e aplicando a garantia de acordo com os critérios adotados pela lei. A atuação da ANPD, aliada à conscientização das empresas e da sociedade sobre a importância da proteção de dados, contribuirá para um ambiente mais seguro e responsável no tratamento das informações pessoais, fortalecendo assim a confiança e a confiança no ambiente digital do país.

6.2 Da responsabilidade dos envolvidos no processo de tratamento de dados conforme a LGPD

Coube ao artigo nº 5 da LGPD definir os envolvidos no processo de tratamento de dados, apresentando inicialmente as figuras do titular, conceituada pela norma enquanto a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; O controlador, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; E o operador, como a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.[450] O mesmo artigo, conforme já mencionado também define em seu inciso VIII a figura do encarregado, como sendo pessoa indicada pelo controlador e operador para atuar como canal de

450 LGPD, artigo nº 5, V, VI. Ibid.

comunicação entre o controlador, os titulares dos dados e a ANPD e apresenta as figuras do controlador e operador, dentro classificação de agentes de tratamento.[451]

Tais definições quanto aos envolvidos no tratamento de dados na LGPD são compatíveis com as definições do RGPD europeu, com algumas pequenas diferenças terminológicas e a adição da figura do "Encarregado" na legislação brasileira. Ambas as regulamentações têm como objetivo proteger os direitos dos titulares de dados pessoais e estabelecer obrigações claras para os controladores e operadores também chamados de processadores na norma europeia, visando garantir a privacidade e a segurança dos dados.[452]

Os agentes de tratamento de dados são atores fundamentais no cenário de proteção de dados no Brasil. A eles cabe na prática a função de realizar o tratamento de dados pessoais, assumindo responsabilidades e obrigações específicas para garantir a proteção e privacidade dos dados dos titulares, atendendo uma necessidade crescente da sociedade cada vez mais digitalizada. Quantidades expressivas de dados pessoais são coletados, armazenados e processados diariamente por diversas organizações com distintas finalidades, gerando preocupação quanto as questões de privacidade. Neste cenário, a LGPD propõe figuras diretamente responsáveis pelos procedimentos que envolvem o tratamento de dados pessoais.

Para melhor compreensão, vale a observação de um exemplo prático: considere um hospital que compõe um grande grupo médico, que utiliza um *software* de gestão de prontuários eletrônicos para armazenar os dados médicos de seus pacientes. Nesse caso, o hospital atua como agente de tratamento de dados em nome do controlador, que é uma instituição de saúde ao qual se encontra vinculado. A responsabilidade do hospital é garantir a confidencialidade e integridade dos dados dos pacientes, além de assegurar que apenas pessoas autorizadas tenham acesso a essas informações.

---

451 LGPD, artigo nº 5, IX. Ibid.

452 Segue breve comparação dos conceitos considerando a norma europeia. Controlador (Equivalente ao RGPD): Tanto a LGPD quanto o RGPD definem o Controlador como a entidade responsável por tomar as decisões sobre o tratamento de dados pessoais. Operador (Equivalente ao RGPD): Na LGPD, o termo utilizado é "Operador", enquanto no RGPD é conhecido como "Processador". Ambos se referem à pessoa ou organização que trata os dados em nome do Controlador. Encarregado (Diferente do RGPD): A LGPD apresenta o conceito de "Encarregado", que é responsável por ser o ponto de contato entre o Controlador, os titulares dos dados e a autoridade de proteção de dados (ANPD). No RGPD, há a figura do "*Data Protection Officer* (DPO)", que é um profissional encarregado de garantir o cumprimento da regulamentação em organizações específicas, especialmente quando envolve o processamento em grande escala de dados sensíveis. Titular (Equivalente ao RGPD): Tanto a LGPD quanto o RGPD se referem ao "Titular" como a pessoa natural a quem os dados pessoais se referem. Dado Pessoal (Equivalente ao RGPD): A definição de "Dado Pessoal" é semelhante na LGPD e no RGPD, referindo-se a qualquer informação relacionada a uma pessoa identificada ou rejeitada.

Por este exemplo é possível esclarecer que no desempenho dos papéis indicados pela LGPD, cabe ao controlador tomar as decisões referente ao tratamento de dados, enquanto o operador, deve obedecer e executar às instruções do controlador. Desta forma, se constrói uma relação jurídica bem delineada que deve ser materializada na via contratual. O contrato neste caso, é um relevante instrumento no qual se define quem atuará na condição de operador e de controlador e pelo qual se reforçam as responsabilidades previstas na LGPD.

Quanto as responsabilidades atribuídas aos agentes de tratamento de dados, é preciso considerar primeiramente as disposições gerais que informam as bases legais para o tratamento de dados e os princípios que devem regê-la.[453] Ou seja, é preciso conhecer as situações nas quais os agentes poderão agir, sendo permitido o tratamento de dados, observando requisitos como o consentimento do titular, o cumprimento de obrigação legal, a execução de políticas públicas, entre outros.

Ao se referir aos deveres do controlador e do operador, a norma estabelece que ambos devem adotar medidas de segurança, criar relatório de impacto à proteção de dados, sempre que se fizer necessário e notificar incidentes de segurança ao titular e à ANPD.[454] Cabe ao controlador, a pedido da ANPD elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações, explicitando a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas.[455] Já ao operador, é atribuído o dever de realizar o tratamento de dados segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.[456]

Desta forma, há uma distinção das obrigações e responsabilidades do controlador e do operador[457] pautadas pelas atividades exercidas por cada um no âmbito do

453 LGPD, artigo nº 5 e 6º. Brasil, op. cit., 2018.

454 LGPD, artigo nº 37: O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Idem.

455 LGPD, artigo nº 38: A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único: Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Ibid.

456 LGPD, artigo nº 39: O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. Ibid.

457 Comparando com o RGPD europeu, pode-se observar algumas semelhanças nas responsabilidades dos agentes de tratamento de dados. O RGPD também diferencia entre controladores e cobertos (equivalente aos operadores da LGPD), estabelecendo responsabilidades para ambos. No entanto, algumas diferenças podem ser apontadas. Por exemplo, o RGPD possui uma abordagem mais detalhada em relação ao consentimento do

tratamento de dados pessoais. Porém, resta perceptível que sob o controlador recaí a principal responsabilidade[458], visto que a ele cabe as decisões sobre o ciclo de vida dos dados pessoais, da coleta ao descarte. Enquanto o operador responde em nome do controlador, com quem partilha algumas obrigações impostas pela LGPD, inclusive em caráter solidário.[459]

Conforme o artigo nº 42 da LGPD, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Percebe-se aqui o viés da responsabilidade trabalhado de forma conjunta entre os dois agentes. Mas buscando mais especificidade, além de assegurar a efetiva indenização ao titular dos dados, o legislador determinou no inciso I que o operador responderá solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos de exclusão previstos em lei.[460]

Deste modo, tem-se uma exceção à regra da responsabilidade exclusiva do controlador[461], caracterizada pela solidariedade com o operador. Tal excepcionalidade deverá ser aplicada em situação de danos causados mediante tratamento irregular realizado por operador, como por exemplo, em caso de descumprimento das obrigações da legislação ou ainda, por faltar com as instruções do controlador.

Em sequência, é preciso observar a situação do encarregado[462], pessoa, jurídica ou física, contratada ou terceirizada indicada diretamente pelo controlador para liderar ações e atividades relacionadas ao tratamento de dados pessoais[463]. Embora a LGPD

---

titular dos dados, sem que o consentimento seja específico, informado e inequívoco. Além disso, o RGPD possui um foco maior na responsabilidade proativa dos agentes de tratamento de dados, aguardando a adoção de medidas técnicas e organizacionais para garantir a proteção dos dados desde a concepção do projeto.

458 A teoria da responsabilidade se relaciona à liberdade e à racionalidade humanas que impõem à pessoa o dever de assumir os ônus correspondentes a fatos a ela referentes. Nesse sentido, a responsabilidade é corolário da faculdade de escolha e de iniciativa que a pessoa possui no mundo fático, submetendo-a, ou o respectivo patrimônio, aos resultados de suas ações, que, quando contrários à ordem jurídica, geram-lhe, no campo civil, a obrigação de ressarcir o dano, ao atingir componentes pessoais, morais ou patrimoniais da esfera jurídica de outrem. MELO, A. N. Dano moral coletivo nas relações de consumo: aplicabilidade da função punitiva do dano. Rio de Janeiro: Lumen Juris, 2018, p. 21.

459 VAINZOF, R. Disposições preliminares. *In*: BLUM, R. O.; MALDONADO, V. N. (coord.). LGPD – Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p.106.

460 LGPD, artigo nº 42, § 1º, I. BRASIL, op. cit., 2018.

461 LGPD, artigo nº 42, § 1º, II: os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. Idem.

462 No inglês denominado *DPO - data protection officer.*

463 LGPD, artigo nº 41. BRASIL, op. cit., 2018.

tenha separado a figura do encarregado dos agentes de tratamento, este ocupa um lugar de fundamental importância na proteção dos direitos dos titulares de dados e no cumprimento das disposições da lei[464].

Um acerto do texto foi a previsão expressa de que a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. [465] Tal regra garante a transparência e o acesso dos titulares de dados a figura do encarregado, que é o responsável direto por intermediar a comunicação entre os titulares e o controlador dos dados. Cria-se uma importante abertura aos titulares de dados, que passam a ter meios de contato com o encarregado, facilitando o exercício de seus direitos em relação à proteção de seus dados pessoais.

Segundo o parágrafo § 2º do artigo 41 da LGP, encontram-se entre as atividades do encarregado aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, bem como receber comunicações da autoridade nacional e adotar providências. Assim, o responsável deve atuar como o ponto de contato entre a empresa e a autoridade nacional de proteção de dados em questões relacionadas ao tratamento de dados pessoais.

Por fim, cabe ao encarregado orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. Em uma análise mais apurada, fica visível a intenção do legislador em indicar o encarregado como responsável por difundir a cultura da privacidade dentro da organização, garantindo que todos os envolvidos estejam cientes das diretrizes e práticas relacionados à proteção de dados.

A princípio a responsabilidade indicada na LGPD incide diretamente nos agentes de tratamento de dados pessoais. Não obstante, não parece razoável desconsiderar a possibilidade de dano frente as atividades designadas para o encarregado. Em ocorrendo uma prática ilícita, o encarregado deve responder conforme as normas e princípios gerais previstos no Código Civil[466].

---

464 Curioso observar que em que pese o importante papel a ser desempenhado pelo encarregado, a LGPD não indicou qualquer tipo de requisito profissional ou de formação.

465 LGPD, artigo nº 41, § 1º. BRASIL, op. cit., 2018.

466 MULHOLLAND, C.; GOMES, R. Encarregado empregado: problemas de responsabilidade civil na LGPD. Migalhas de responsabilidade Civil, São Paulo, 2021, p. 9. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de responsabilidadecivil/347010/encarregado-empregado-problemas-de-responsabilidade-civil-na-lgpd. Acesso em: 17 maio 2023.

Considerando um dano a terceiros em decorrência da atuação ou em função da atividade do encarregado, a princípio a responsabilidade recairia sob o controlador. A LGPD prevê que os agentes de tratamento não serão responsabilizados se comprovarem que o dano foi decorrente de culpa exclusiva do titular dos dados ou de terceiros.[467] A este ponto surge a controvérsia quanto a possibilidade de se enquadrar o encarregado como "terceiro".

Na verdade, a expressão "terceiro" denota a situação de uma pessoa que se encontra fora do ciclo de tratamento de dados e alheia a influência do controlador. Mas se a LGPD não estabeleceu o de direito de regresso face ao encarregado, o Código Civil garante essa possibilidade, na esfera da responsabilidade civil do empregador pelos atos de empregado[468]. Seria então considerada a responsabilidade de natureza objetiva conforme o artigo 993, do Código Civil, sendo o controlador responsável por ato de terceiro, desde que seja comprovado o vínculo empregatício entre controlador e encarregado[469].

Desta forma, é possível compreender que o encarregado pelo tratamento de dados pessoais responderá apenas em casos nos quais for comprovado dolo ou culpa grave em sua conduta, ou ainda quando o agente de tratamento de dados acionar o direito de regresso em face de ato ilícito praticado no curso de suas atribuições. Nas demais situações, caberá a imputação da responsabilidade ao controlador, conforme indica a LGPD.

A atuação adequada dos agentes de tratamento é crucial para garantir a confiança dos titulares de dados e para evitar possíveis violações de privacidade que possam afetar a autoridade das organizações e causar danos aos indivíduos envolvidos. Por isso, a conscientização e a implementação efetiva da LGPD são de suma importância para a construção de um ambiente digital seguro e confiável no Brasil.

467 LGPD, artigo nº 43, III: Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. BRASIL, op. cit., 2018.

468 MULHOLLAND; GOMES, op. cit., p. 11.

469 Tecnicamente, há possibilidade do encarregado ser terceirizado. LGPD não especifica se o encarregado deve ser pessoa natural ou jurídica, assim como não trata da necessidade de ser contratado terceirizado ou funcionário do agente de tratamento de dados pessoais. Em fato, há um embate quanto a adoção da responsabilidade objetiva ou subjetiva nas situações de tratamentos de dados e os principais argumentos das duas correntes serão apresentados no tópico a seguir.

6.3 Considerações sobre o sistema de responsabilidade civil adotado pela LGPD

A Lei Geral de Proteção de Dados (LGPD) representa um marco regulatório fundamental no Brasil, que visa proteger os direitos fundamentais de privacidade e segurança das informações pessoais dos cidadãos. A responsabilidade civil é um aspecto crucial da LGPD, pois estabelece as consequências para a violação das normas de tratamento de dados por parte das organizações que lidam com informações pessoais.

A responsabilidade civil[470] é um instituto derivado do reconhecimento de direitos individuais e tem por objetivo a manutenção de uma boa convivência em sociedade, garantindo que, uma vez violado determinado direito, possa ser feita a reparação do dano causado. Assim, o ato ilícito gera obrigação de remediar e cria constrangimento jurídico, conferindo a uma das partes o direito de exigir da outra o cumprimento de determinado prazo[471]. Todo dano ou prejuízo que não encontra a devida reparação pode se converter em um fator de inquietação social. Neste sentido, emerge a responsabilidade civil como meio de restaurar o equilíbrio patrimonial e moral violados[472].

A LGPD prevê a responsabilização das empresas, órgãos governamentais e demais entidades que realizam o tratamento de dados pessoais, sempre que estejam envolvidos em operações que resultem em danos aos titulares dos dados, mas seus artigos estão longe de abarcar todas as situações e nuanças decorrentes da exposição indevida de dados, especialmente os de conteúdo sensível[473]. Embora haja esta previsão, é válido destacar que essas regras não serão necessariamente aplicadas a todos os casos que suscitem responsabilização. A depender da relação jurídica configurada é possível que a LGPD ceda lugar a outras normativas, tais como o Código Civil e o Código de Defesa do Consumidor[474].

---

470 O termo responsabilidade é utilizado em qualquer situação na qual alguma pessoa, natural ou jurídica, deva arcar com as consequências de um ato, fato ou negócio danoso. Sob essa noção, toda atividade humana, portanto, pode acarretar o dever de indenizar. Logo, o estudo da responsabilidade civil abrange todo o conjunto de princípios e normas que regem a obrigação de indenizar. VENOSA, S. S. Direito Civil: obrigações e responsabilidade civil. 21. ed., v. 2. São Paulo: Atlas, 2021, p. 357. E-book. Disponível em: http://primopmtna01.hosted.exlibrisgroup.com/PUC01:PUC01:sfx26800000000062317. Acesso em: 3 jun 2023.

471 GONÇALVES, C. R. Direito Civil Brasileiro: responsabilidade civil. 16. ed. São Paulo: Editora Saraiva, 2021, p. 87.

472 Idem, p. 89.

473 A responsabilidade civil na LGPD é abordada desde o seu artigo 42 até o seu artigo 45. BRASIL, op. cit., 2018.

474 Neste sentido dispõe o artigo nº 45 da LGPD: as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. Idem.

Para assegurar a efetividade do regime de proteção de dados proposto pela LGPD é essencial a aplicação de responsabilidade civil face aos agentes de tratamento que por alguma de suas condutas venha a violar direitos individuais dos titulares dos dados. Logo, é possível perceber a estreita ligação entre o instituto da responsabilidade civil e a disciplina da proteção de dados. Todavia, o legislador não esclareceu de pronto qual seria o sistema de responsabilidade civil a ser adotado para estes casos, gerando uma série de polêmicas quanto a matéria.

Para melhor esclarecer, sempre que se verifica um dano decorrente de ato ilícito há uma quebra do equilíbrio jurídico e econômico anteriormente estabelecido. Logo, a busca por uma reparação, costumeiramente resulta no dever de uma indenização [475]em favor da vítima, a ser fixada em proporção ao dano por ela sofrido.[476] No que se refere a este dever de indenizar, a responsabilidade civil subdivide-se em subjetiva, fundamentada na teoria da culpa e objetiva, fundamentada na teoria do risco, se desdobrando em dois sistemas distintos.

Na realidade, a controvérsia quanto ao sistema de responsabilidade civil a ser adotada pela LGPD nas questões de vazamento de dados é um tema de grande resistência e debate entre especialistas. Tal discussão está centrada nas peculiaridades dos sistemas de responsabilidade civil subjetiva e objetiva, e acaba ganhando mais argumentos à medida que surgem novos casos de vazamento de dados e se verificam as consequências na vida prática de seus titulares.

Em poucas linhas, a responsabilidade civil subjetiva está fundamentada na culpa ou negligência do agente que causou o dano[477]. A ideia da culpa contempla a visão da reprovação do agente causador do dano e de seu dever de reparação. Seria uma resposta ao anseio por segurança jurídica, enquanto define que a obrigação de reparar o dano caudado, sempre que este for originado em conduta reprovável, ou pelo menos de modo culposo.[478]

---

475 A CRFB/88 estabelece o dever de indenizar no artigo 5°, incisos V e X: é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; [...] São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. BRASIL, op. cit., 1988.

476 CAVALIERI FILHO, S. Programa de Responsabilidade Civil. 14. ed. São Paulo: Atlas, 2020. E-book. Disponível em: http://primo-pmtna01.hosted.exlibrisgroup.com/PUC01:PUC01:sfx26800000000061280. Acesso em: 04 mar. 2023. p. 21.

477 A responsabilidade civil subjetiva, fundada na culpa, constitui fundamento para todos os ordenamentos jurídicos e apresenta estreita conexão com os princípios da Revolução Francesa: igualdade, liberdade e fraternidade.

478 NAVEGA, L. Expansão da Responsabilidade Civil Objetiva: Análise da (In)Adequação da Inserção no Ordenamento Jurídico de uma Cláusula Geral de Responsabilidade Objetiva. **Revista do Ministério Público do Estado do Rio de Janeiro**, Rio de Janeiro, n. 66, p. 109-127, 2017, p.110. Disponível em: https://www.mprj.

Conforme essa visão a responsabilidade se encontra vinculada à culpa, abrangendo a culpa *stricto sensu* e o dolo. Tem-se, pois, a situação violação de dever objetivo de cuidado, que o agente podia conhecer e observar, ou ainda a omissão de conduta exigível, sem que haja vontade ou intenção direta de praticar um ato ilícito.[479] Ao tempo em que também considera a concepção clássica de culpa conforme uma conduta voluntária contrária ao dever de cuidado. A responsabilidade civil subjetiva pondera a vontade de agir e a previsibilidade do resultado na violação do dever preexistente[480].

Nos termos do Código Civil, a responsabilidade civil subjetiva se encontra disposta no artigo nº 186, segundo o qual "aquele que, por ação ou missão intencional, negligente ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito". Dessa forma, fica claro que a responsabilidade civil subjetiva está associada à conduta humana culposa ou dolosa que resulta em danos a terceiros, criando uma relação de causalidade entre ação ou omissão e prejuízo experimentado pela vítima.

O nexo de causalidade é indicado pela norma civil como um dos elementos essenciais para a caracterização da responsabilidade civil. Seria este uma conexão clara entre a conduta do agente e o resultado, que resultou em prejuízo e dano para a vítima. Portanto, a conduta humana, positiva ou negativa, deve estar associada ao dano ou prejuízo causado, de modo que a exclusão de tal nexo, acarretaria a quebra da conexão entre conduta e resultado, eliminando o dever de indenizar.

Do mesmo modo, a caracterização do dano é outro ponto essencial para a aplicação da responsabilidade civil. Não há que se falar em dever de reparação quando não houver comprovação de redução de diminuição patrimonial ou uma lesão a um interesse juridicamente protegido. Aqui se abrange tanto os danos materiais que envolvem perda financeira e destruição de bens, quanto os danos morais que versam sobre lesões à honra, à imagem, sofrimento psicológico, entre outros.

---

mp.br/documents/20184/1246489/Leandro_Navega.pdf. Acesso em: 15 mar. 2021.

479 CAVALIERI FILHO, op. cit., 2020, p. 43.

480 A considerar a sistematização havida no período pós-clássico do Direito Romano, separam-se as funções punitivas e reparatórias, da responsabilidade civil. Representadas pela pena e pela indenização, respectivamente, atenderiam a interesses diversos: de um lado o interesse público e de outro o interesse privado, com uma distinção nítida entre procedimento civil e procedimento penal. A função reparadora do dano por meio de uma pena pecuniária permite a restituição do status quo anterior. A noção de culpa como requisito indispensável para surgir o dever de reparar, estabelecendo estrita ligação com a concepção de punição. São essas duas premissas que se revelaram no CC de 1916, sob nítida influência do Código Civil Francês, de 1804, estabelecendo como regra a responsabilidade civil subjetiva, a qual tem como pressuposto indispensável a comprovação da culpa do agente causador do dano. MELO, op. cit., 2018, p. 16.

Nesse sistema, para que uma empresa ou entidade seja responsabilizada por um vazamento de dados, é necessário verificar que uma ação de cunho doloso ou a presença de culpa no tratamento falho dos dados pessoais. Em outras palavras, a vítima precisa demonstrar que a organização não tomou as atitudes adequadas para evitar o vazamento ou que agiu de forma intencional para causar o dano.

A culpa em seu sentido *lato*, que abrange o dolo, não chega a ocupar a posição de pressuposto geral da responsabilidade civil, considerando que o Código Civil aceita a existência de outra espécie de responsabilidade, que prescinde desse elemento subjetivo para a sua configuração, materializado no sistema da responsabilidade objetiva[481].

A responsabilidade civil objetiva é pautada na ideia de que certas atividades ou circunstâncias trazem consigo o risco inerente de causar danos a terceiros, e, portanto, aquele que se dedica a tais atividades assume a responsabilidade pelos prejuízos eventualmente gerados, independentemente de sua culpa no evento danoso.

O Código Civil brasileiro estabelece a responsabilidade objetiva em seu artigo 927, parágrafo único, ao afirmar que "haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei". Nesse sentido, a legislação brasileira traz determinadas hipóteses em que a responsabilidade é objetiva, e não subjetiva. Existe uma tendência a responsabilização objetiva quando se percebe um desequilíbrio nas posições jurídicas. Desta forma, será responsável quem exerce uma atividade perigosa, devendo assumir os riscos, assim como reparar os prejuízos provenientes dela.[482] Tal é o exemplo verificado nas relações de consumo, onde se considera a hipossuficiência do consumidor em relação ao fornecedor.

Dentro do sistema objetivo, não se demanda de forma obrigatória a presença do elemento culpa, de modo que ainda que não haja a verificação de conduta culposa por parte do agente, existirá o dever de indenizar em virtude do risco da atividade que o provocou[483]. Os elementos indispensáveis neste caso, seriam a atividade habitual com potencial risco de dano, o dano configurado e o nexo de causalidade, conforme parágrafo único do artigo 927 do Código Civil.[484]

---

481 GAGLIANO, P. S.; PAMPLONA FILHO, R. M. V. Novo curso de direito civil: responsabilidade civil. 20. ed. São Paulo: SaraivaJur, 2022, p. 70.

482 CAVALIERI FILHO, op. cit., p. 191.

483 TEPEDINO, G.; TERRA, A. M. V.; GUEDES, G. S. C. Fundamentos do direito civil: responsabilidade civil. 2. ed. Rio de Janeiro: Forense, 2021, p. 7. E-book. Disponível em: http://primopmtna01.hosted.exlibrisgroup.com/PUC01:PUC01:sfx26800000000062157. Acesso em: 6 mar. 2023.

484 Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Para os fins desta pesquisa é importante destacar que a norma contida no mencionado artigo nº 927 do Código Civil possui enunciado aberto. Esta amplitude foi intencional no sentido de permitir sua aplicação a um número indeterminado de situações diferentes.[485] O direito caminha a passos lentos quando comparado com as inovações tecnológicas e transformações sociais, por este motivo, o legislador civil optou em diversos momentos por trabalhar com regras que possibilitem certa discricionariedade ao julgador.

Além dos casos expressos na lei, a regra disposta indica que haverá a incidência de responsabilidade objetiva quando "a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem", deixando a via de abrangência preparada para abarcar inúmeras possibilidades de situações, incluindo-se aquelas que se originam a partir das novas tecnologias. Mas é importante observar que o risco mencionado reflete um tom de perigo, denotando algo até certo ponto provável de ocorrer.

Na visão da doutrina, o risco é compreendido como perigo ou probabilidade de dano[486]. Tal conceito acaba por se desdobrar em diversas teorias, dentre as quais se destacam a teoria do risco integral, segundo a qual o dever de indenizar pode ocorrer, mesmo nos casos em que não se verifique nexo de causalidade;[487] A teoria do risco proveito, que prevê a reparação do dano quando o agente vier a ter proveito ou vantagem de uma atividade danosa; E a teoria do risco criado, na qual "responde civilmente aquele que, por sua atividade ou por sua profissão, expõe alguém ao risco de sofrer um dano[488]", tendo sido esta última, adotada pelo Código Civil.

Desta forma, não há que se esperar a comprovação de culpa ou dolo do agente causador do dano, na responsabilidade objetiva. Considerando o panorama dos dados sensíveis de saúde, neste sistema bastaria que o dano tenha sido causado em decorrência do tratamento de dados para que a responsabilidade seja atribuída à organização, independentemente de sua conduta. O argumento seria que a atividade de tratamento de dados, por si só, apresenta riscos potenciais, e, portanto, a empresa deve ser responsabilizada pelos danos causados decorrentes dessa atividade.

Porém, os argumentos quanto ao sistema de responsabilidade a ser adotado frente as situações que envolvam tratamento de dados ainda não encontraram voz uníssona.

485 CAVALIERI FILHO, op. cit., p. 215.
486 Idem, p.191.
487 Ibid., p.193.
488 Ibid., p. 194.

Quando se trata da responsabilidade civil a ser imposta aos agentes e encarregados, a LGPD não se posiciona diretamente quanto ao regime a ser adotado, permitindo controvérsias quanto a aplicação da responsabilidade objetiva ou subjetiva em seu contexto. Em fato, a imprecisão do texto do artigo nº 42 abre espaço para a interpretação do aplicador da norma, que necessita buscar amparo não apenas na LGPD, mas na Constituição Federal, Código Civil, além de considerar legislações específicas, conforme o caso concreto.[489]

Na leitura do texto do artigo nº 42 da LGPD, não há qualquer menção a ideia de culpa, o que a princípio poderia ser interpretado como um direcionamento a adoção do sistema de responsabilidade objetiva. Contudo, o referido texto também não utiliza a indicação "independentemente de culpa", tal como o Código Civil e o Código de Defesa do Consumidor, em uma omissão que poderia ser interpretada como um direcionamento para a responsabilidade subjetiva.[490]

A tese pela aplicação da responsabilidade objetiva, parte da ideia de que há um risco intrínseco a toda ação de tratamento de dados, mediante a verificação de um considerável potencial danoso em caso de falha no tratamento ou vazamento, que podem prejudicar direitos fundamentais do titular de dados e se apoia nos princípios da LGPD.

A possibilidade disposta na norma de que o agente de tratamento de dados seja ente público traz como reflexo automático a obrigação de responder objetivamente pelo dano causado decorrente de vazamento de dados, o que seria um indicativo da aplicação do sistema de responsabilidade objetiva. A imposição de outro regime para um mesmo fato, resultaria em tratamento diferenciado conforme o agente envolvido e consequente insegurança jurídica[491].

Ademais, ao se considerar que a LGPD tem por fundamento a diminuição de riscos de dano face ao tratamento de dados e impõe em seus princípios a "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[492]", tem-se a ideia de da opção pela responsabilidade objetiva ao tempo que se considera a atividade de tratamento de dados pessoais vinculada a

489 SCHREIBER, A. Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais: Tratado de Proteção de Dados Pessoais. São Paulo: Editora Forense, 2020, p. 333.

490 Idem, p. 334.

491 NOVAKOSKI, A. L. M.; NASPOLINI, S. H. D. F. Responsabilidade civil na LGPD: problemas e soluções. Conpedi Law Review, Florianópolis, v. 6, n. 1, 2020, p. 170. Disponível em: https://indexlaw.org/index.php/conpedireview/article/view/7024. Acesso em: 18 fev. 2023.

492 LGPD, artigo 6º, III. BRASIL, op. cit., 2018.

um risco inerente, potencialmente lesivo a seus titulares. Além disso, pela leitura dos princípios elencados no artigo 6º da LGPD, tais como os princípios da segurança, da prevenção, da responsabilização e da prestação de contas, é possível fortalecer a visão de uma lei que protege o titular de dados, prevendo em favor deste, o direito a ser indenizado pelos danos sofridos conforme a teoria do risco[493].

Outro argumento favorável a tese da responsabilidade objetiva encontra amparo no texto do artigo nº 44 da LGPD, que se utiliza a expressão "tratamento irregular" [494] atrelando a responsabilidade civil a qualificação da irregularidade, o que é esclarecido no artigo nº46[495], que se refere às medidas de segurança e boas práticas a serem observadas pelo agente de tratamento de dados.

Há neste ponto a identificação de duas situações oriundas de incidentes de segurança: a obrigação de indenizar em razão do exercício de atividade de tratamento de dados pessoais, prevista no artigo nº 42 da LGPD e a obrigação de indenizar na hipótese de verificação de tratamento irregular de dados pessoais, com a violação da segurança dos dados prevista no artigo nº 44. Os dois casos apresentam como ponto comum o risco inerente ao desenvolvimento a atividade de tratamento de dados, que na via prática podem ser materializados como vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados e consequentemente chamam para a responsabilidade objetiva.[496]

Por esta interpretação, caberia ao agente de tratamento o dever de indenizar os danos causados aos titulares de dados, sem que eles necessitem comprovar a conduta culposa

493 A LGPD atribui ao agente diversos deveres ativos, tais como a obrigação de transparência a ser acerca dos procedimentos que são tomados para a segurança e prevenção no tratamento de dados e o dever de prestação de contas, o que fortalece a ideia de uma responsabilidade objetiva. MULHOLLAND, C. S. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? Migalhas, São Paulo, 2020, p. 2. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso: 11. mar. 2023.

494 LGPD, artigo n° 44: O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

495 LGPD, artigo n° 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. BRASIL, op. cit., 2018.

496 MULHOLLAND, op. cit., 2020, p. 3.

por parte do controlador ou operador em virtude do potencial risco da atividade. Nesse contexto, é preciso observar que os danos suportados pelos titulares ferem direitos fundamentais e atingem sua esfera pessoal, apresentando ainda a peculiaridade de não ser possível mensurar de forma exata a extensão e o tempo que estes prejuízos podem perdurar. Por este viés gravoso, é pertinente a aplicação da responsabilidade civil objetiva face ao tratamento de dados, de forma similar ao que se verifica nas relações de consumo e questões ambientais.

É certo que a LGPD não apresenta previsão expressa quanto ao elemento culpa, porém seu texto também não o excluí completamente[497]. Assim, encontra amparo a teoria de que a LGPD segue o regime que considera a conduta ilícita do agente para indicar o dever de indenizar. A identificação do elemento culpa como pressuposto do dever de indenizar, nesta visão, conduz ao sistema da responsabilidade subjetiva[498].

A responsabilidade civil subjetiva, conforme mencionado se estabelece a partir da demonstração de culpa ou dolo do agente responsável pelo ato danoso. Em outras palavras, para que haja obrigação de reparar o dano causado a outrem, é preciso provar que o agente agiu com negligência, imprudência, imperícia ou de forma intencional para prejudicar o patrimônio ou a integridade física de outra pessoa[499].

O artigo 186 do Código Civil brasileiro estabelece o direito da responsabilidade civil subjetiva ao afirmar que "aquele que, por ação ou missão intencional, negligente ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito". Já o artigo 187 reforça que também está sujeito a reparar o dano aquele que, por ato ilícito, causar prejuízo a outrem[500]. Dessa forma, fica claro que a responsabilidade civil subjetiva está associada à conduta humana culposa ou dolosa que resulta em danos a terceiros, criando uma relação de causalidade entre ação ou omissão e prejuízo causado.

Sob o prisma da LGPD, que elege como uma de suas principais bases o dever de cuidado e indica possibilidade de responsabilização mediante sua quebra, seria possível caracterizar o regime de responsabilidade subjetiva. O texto da LGPD se firma sob

497 TASSO, op. cit., p. 104.

498 As hipóteses normativas de responsabilidade civil subjetiva devem prever expressamente a culpa como requisito necessário para gerar o dever de indenizar. BESSA, L. R. **Código de Defesa do Consumidor Comentado**. 2. ed. rev., atual. e ampl. Rio de janeiro: Forense, 2022, p. 75.

499 GAGLIANO; PAMPLONA FILHO, op. cit., p. 82.

500 Código Civil, artigo nº 186: Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. Artigo nº 187: Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. BRASIL, op. cit., 2002.

uma série de regras que visam cuidado e proteção, cuja falta de observação implica em responsabilidade do agente[501]. Tais deveres, expressos em diversos dispositivos da norma, não teriam o mesmo peso no sistema objetivo que se pauta pela existência ou não da culpa.

Conforme a redação do artigo nº 42, I da LGPD: "o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador". Por esta leitura se entende que a responsabilização se encontra atrelada ao descumprimento da legislação, desconsiderando o elemento culposo. O caput do mencionado artigo apresenta a esfera de responsabilidade do controlador e do operador de dados, prevendo reparação de danos patrimoniais, morais, individuais ou coletivos, sempre que esses decorram de violação à legislação de proteção de dados pessoais.[502]

Na verdade, o Capítulo VI da LGPD delimita um padrão de conduta a ser observado pelos agentes de tratamento de dados, indicando uma série de deveres e boas práticas de governança[503], o que seria considerado um indicativo do regime subjetivo sob o argumento de que no objetivo, não faria sentido tal previsão, visto que o dever de indenizar seria inerente ao risco da atividade.[504]

Outro ponto a ser analisado é o conteúdo do artigo nº43 da LGPD [505]que apresenta excludentes de responsabilidade para o agente, fato que remete a responsabilidade subjetiva. O inciso II do mencionado artigo, exclui a responsabilidade do agente de tratamento mesmo que verificado o nexo de causalidade entre a conduta e o dano,

---

501 Cabe mencionar o Projeto de Lei que originou a LGPD sofreu alterações que resultaram na retirada, da referência expressa sobre a responsabilidade objetiva, e teve a inclusão da expressão "em violação à legislação de proteção de dados pessoais" no caput do artigo 42 da LGPD. BRASIL. Projeto de Lei nº 5.276, de 2016. BRASIL, op. cit., 2016.

502 LGPD, artigo nº 42: O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. BRASIL, op. cit., 2018.

503 Tais deveres, em conjunto com as regras dispostas na LGPD, como boas práticas de governança, não são meras recomendações para evitar incidentes de segurança, mas correspondem ao tratamento regular de dados considerado "uma obrigação de resultado e não de meio. TASSO, F. A. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 97-115, 2020, p. 108. Disponível em: http://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf? d=637250344175953621. Acesso em: 30 mar. 2023.

504 GUEDES, G. S. C.; MEIRELES, R. M. V. "Término do tratamento de dados". *In*: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoas. 2. ed. São Paulo: Editora RT, 2019, p. 231.

505 LGPD, artigo nº 43Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. BRASIL, op. cit., 2018.

desde que tenha agido conforme deveres impostos pela LGPD, adotando as medidas de segurança recomendadas.[506]

Para reforçar a tese subjetiva, tem-se ainda o disposto no parágrafo único do artigo nº 44 da LGPD, segundo o qual "responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano". Por sua vez, o artigo nº 46, afirma a obrigatoriedade da adoção de medidas de segurança, técnicas e administrativas, para a proteção dados pessoais, além de indicar padrões técnicos mínimos e que as regras ali dispostas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Logo, a menção do artigo nº 44 quanto a violação de deveres específicos, elencados no artigo nº 46, seria mais um indício da aplicação da responsabilidade subjetiva na LGPD.

Neste raciocínio, a noção de culpa implementada na LGPD exige a análise dos parâmetros de conduta socialmente aceitos para posterior verificação da culpabilidade do agente, o que poderia ser inteiramente suprido pelo sistema subjetivo, já tradicional.

Observa-se que a discussão quanto ao sistema de responsabilidade adotado pela LGPD apresenta argumentos relevantes para as duas linhas, o que suscitou entre a doutrina a ideia de um regime de responsabilidade na LGPD que se distancia da aplicação das regras da teoria clássica, indicando uma responsabilidade ativa ou proativa[507], o que configuraria uma terceira via. Segundo tal visão, não basta cumprir as regras especificadas na lei, cabendo ao agente comprovar que seus procedimentos atendem as orientações legais e que suas medidas são eficazes.[508]

Para uma melhor visualização dos principais pontos desta discussão, segue tabela indicando critérios a serem verificados em situação de configuração de dano no sistema de saúde pública e privada. Em que pese, a pesquisa ter adotado como foco a saúde brasileira considerando uma visão global, no que tange a dúvida quanto ao sistema de responsabilidade civil a ser adotado, é interessante observar as aproximações e distinções das esferas da saúde púbica e privada.

506 GUEDES; MEIRELES, op. cit., p. 219.

507 Tal ideia foi proposta por doutrinadores como proposição de Maria Celina Moraes e João Quinelato de Queiroz, entre outros.

508 MENDES, L. S.; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. São Paulo: Revista dos Tribunais, v. 120, 2018, p. 469-483, nov.-dez.2018, p. 469.

Quadro 6 - Comparativo entre as esferas da saúde púbica e privada quanto ao tratamento de dados

Critérios	Saúde Pública	Saúde Privada e Suplementar
Natureza da Instituição	Órgãos Governamentais, Hospitais Públicos, Centros de Saúde da Esfera Pública.	Empresas Privadas, Hospitais e Clínicas Particulares
Agente de Tratamento de Dados	Órgão Governamental ou Entidade Pública Responsável pelo Tratamento dos Dados	Empresa ou Instituição Privada Responsável pelo Tratamento dos Dados
Encarregado	Geralmente há um Encarregado de Proteção de Dados (EPD) designado nos órgãos públicos de saúde para garantir o cumprimento da LGPD.	A empresa privada ou instituição deve indicar um Encarregado de Proteção de Dados (EPD) para assegurar o cumprimento da LGPD.
Impactos da Indenização	Indenizações são custeadas pelos cofres públicos, podendo impactar o orçamento do órgão público de saúde.	As indenizações são normalmente pagas pela empresa ou instituição privada responsável pelo tratamento dos dados, podendo afetar suas finanças e reputação.
Normas Aplicáveis	Constituição Federal, Código Civil Brasileiro, Lei Geral de Proteção de Dados (LGPD), Lei nº 8.080/1990 (Lei Orgânica da Saúde), Lei nº 12.527/2011 (Lei de Acesso à Informação).	Constituição Federal, Código Civil Brasileiro, Lei Geral de Proteção de Dados (LGPD), Resolução Normativa nº 277/2011 da Agência Nacional de Saúde Suplementar (ANS), entre outras normativas da ANS. Código de Defesa do Consumidor.
Jurisprudência e Precedentes	A jurisprudência sobre vazamento de dados de saúde pública ainda está em desenvolvimento, havendo poucos casos que ainda não se encontram consolidados.	Na saúde privada e suplementar, já existem diversos precedentes judiciais sobre vazamento de dados sensíveis que podem influenciar novos julgamentos.

Fonte: Elaborado pela autora.

Em fato, conforme se extrai dos já mencionados artigos nº 42 e 43 da LGPD, a comprovação do ato ilícito no tratamento de dados não cabe a vítima, mas cabe ao agente demonstrar que as práticas de suas atividades se deram em conformidade com a lei. Pela leitura destes e de outros argumentos previamente expostos, é perceptível que o sistema subjetivo de responsabilidade emerge como ferramenta para facilitar a aplicação do dever de indenizar proposto pela LGPD.

Porém, de outro lado, tem-se as questões da presunção da culpa do agente, a possibilidade de inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil e as aberturas que permitem uma interpretação discricionária quanto a configuração de tratamento irregular, que dificulta o afastamento do elemento culpa. Tal situação parece direcionar a questão para um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade [509].

Por este pensamento, seria possível antever a presença ativa dos dois sistemas de responsabilidade presentes na norma, tendo sua aplicação definida conforme o caso concreto. Todavia, cabe verificar se a proposta de um sistema não binário de

509 BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com, Rio de Janeiro, a. 9, n. 3, 2020b, p. 22. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Acesso em: 24 mar. 2023.

responsabilidade seria de fato o caminho mais adequado para tratar da proteção de dados e ainda, sobre como seria possível chegar a critérios claros, a fim de assegurar a aplicação da norma, preservando a segurança jurídica do titular de dados. Tais questões serão objeto de estudo e reflexão ainda neste capítulo por meio a análise de julgados recentes quanto a matéria a ser apresentada nos tópicos a seguir.

6.4 Dificuldades inerentes ao arbitramento do valor do dano face ao potencial discriminatório e lesivo das informações de saúde

São inegáveis as mudanças na visão e na condução dos processos e relações econômicas, políticas, culturais, sociais e, inclusive pessoais que repentinamente foram agregadas às nossas vidas por meio das tecnologias. A rede mundial de computadores desconstruiu uma série de paradigmas, ultrapassando rapidamente a ideia de um repositório de informações e atingindo o status de um novo mundo, no qual se permitem diversos protocolos de transmissão de dados em altíssima velocidade e a utilização de ferramentas que se revelaram capazes de eliminar barreiras físicas de acesso, viabilizando mecanismos e ações anteriormente restritos por condições temporais e geográficas.

A internet simboliza, sem dúvidas, um campo aberto com infinitas possibilidades para aqueles que desejam se aventurar em suas ondas. Inúmeros casos de sucesso de empreendedorismo digital, avanços científicos e até relacionamentos pessoais podem ser encontrados no curto período dessa "revolução" da era contemporânea. Entretanto, não se pode olvidar que um espaço tão dinâmico e com tantas áreas inexploradas também abre caminho para uma série de problemáticas e questões, especialmente nos campos do direito e da ética, que nem sempre conseguem ser respondidas na velocidade ideal.

Cercado pela presença de sistemas e elementos tecnológicos, o cidadão comum em muitos casos, sequer percebe a extensão da abertura gerada pelas constantes solicitações de entregas de dados pessoais. A cada momento, da vida prática tem-se o preenchimento de cadastros, entrega de documentos, aceite em termos de uso e privacidade que na maioria das vezes sequer chegam a ser lidos pelo titular, abrindo uma via direta para a esfera íntima do indivíduo, que segue sua rotina sem avaliar os riscos que suporta por estes procedimentos.

Um vazamento de dados pessoais é um evento sério que tem ramificações abrangentes e por tanto, requer ações imediatas e efetivas para mitigar os danos e proteger a privacidade dos envolvidos. As normas da LGPD, fortalecidas pela Emenda Constitucional nº 115/2022[510], tem sido utilizada como ferramentas para coibir procedimentos que atentem contra o direito à privacidade e que resultam dano para os titulares de dados.

Mediante um vazamento de dados de saúde, seja por uma falha de segurança, um ataque cibernético ou qualquer outra circunstância, o controlador será o responsável por indenizar o indivíduo afetado pelos danos decorrentes do vazamento, conforme já discutido nos tópicos anteriores. Tal indenização pode abranger danos materiais, nas questões que envolvam prejuízos financeiros diretos, danos morais nos casos de sofrimento psicológico e constrangimento, além de outros tipos de danos previstos na legislação.

O conceito de dano indenizável decorrente de um vazamento de dados pessoais está intrinsecamente ligado aos prejuízos sofridos pelos titulares dessas informações sensíveis quando ocorre uma violação de segurança. Quando informações privadas, como nomes, endereços, números de documentos, dados de saúde, entre outros, são expostos, acessados ou divulgados sem autorização seus titulares acabam expostos a sérios ricos. Nesse contexto, tem-se a indicação de um dever de indenizar face as consequências adversas que o titular dos dados pode enfrentar devido à divulgação indevida de suas informações.

Como já explicado, a esfera da saúde pelo conteúdo detalhado dos dados que utiliza, se tornou um alvo preferencial para ataques e práticas de hackeamento de dados, configurando um cenário que inspira preocupação. A partir da verificação da exposição ilícita de informações sensíveis de saúde, surgem diversas possibilidades de dano indenizável.

De maneira direta a LGPD reconhece o dever de indenizar mediante dano patrimonial, moral, individual ou coletivo, verificado em violação à legislação de proteção de dados pessoais[511]. Porém, a situação de vazamento de dados de saúde requer a consideração de outras espécies de danos tais como o dano social e o dano existencial. Em que pese as ressalvas quanto a aceitação destes "novos danos", indicados cada vez

510 Conforme já mencionado, a Emenda Constitucional nº 115/2022 alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. BRASIL, op. cit., 2022.

511 LGPD, artigo nº42. BRASIL, op. cit., 2018.

com maior frequência pela literatura jurídica e pelos tribunais no Brasil e no exterior, para os fins desta pesquisa são válidos enquanto despontam como agravamentos do dano moral, apresentando lesões específicas que podem conduzir a uma melhor avaliação quanto a extensão dos prejuízos e consequentemente, a valoração apropriada em termos de indenização ou compensação.

Sem a pretensão de aprofundamento na matéria, apresenta-se a seguir um breve panorama quanto as possíveis modalidades de dano que podem vir a ser identificadas especificamente na situação do vazamento de dados de saúde. A esclarecer, as modalidades descritas foram selecionadas conforme a análise de julgados recentes dos tribunais brasileiros, que serão posteriormente detalhados neste texto.

O dano material se refere ao prejuízo patrimonial causado à parte lesada pelo ato, que se subdivide em danos emergentes, referentes ao que o indivíduo perdeu em virtude da conduta lesiva e lucros cessantes, caracterizados pelo que se deixou de lucrar. Já o dano moral trata de uma lesão a interesse não patrimonial, atingindo a esfera íntima e o estado psíquico do indivíduo e se estende a todos os bens personalíssimos.[512] Aqui deve ser considerado sofrimento psíquico, dor emocional, abalo moral, entre outros. O dano moral é subjetivo, variando de acordo com as circunstâncias do caso, mas em geral refere-se à lesão à honra, à imagem e aos sentimentos do indivíduo afetado. Trata-se de duas espécies de dano que encontram amparo direto no texto da LGPD.[513]

Em um viés mais subjetivo, emerge o dano existencial. Originada na Europa, esta modalidade de dano busca proteger a existência humana e o projeto de vida do indivíduo, caracterizando como dano indenizável a lesão que atinja a as perspectivas pessoais de vida da pessoa humana, frustrando expectativas e objetivos de vida[514]. O

512 O dano moral atinge o ofendido como pessoa e representa a lesão de bens que integram os 'direitos da personalidade, como a honra, a dignidade, intimidade, a imagem, o bom nome etc., conforme art. 1º, III, e 5º, V e X, da Constituição Federal, e que acarreta ao lesado dor, sofrimento, tristeza, vexame e humilhação". GONCALVES, op. cit., 2021, p. 359.

513 Dentre as bases legais dos danos materiais e morais é possível citar o artigo 5º, inciso V da Constituição Federal (CF), que garante o direito à indenização por dano material, bem como os artigos 186 e 927 do Código Civil, que estabelecem a responsabilidade civil por danos causados a outrem, incluindo os danos materiais.

514 No Brasil, a indenização por dano existencial vem sendo aplicado pelas cortes trabalhistas. A título de exemplo: RECURSO DE REVISTA. DANO MORAL. DANO EXISTENCIAL. SUBMISSÃO A JORNADA EXTENUANTE. PREJUÍZO NÃO COMPROVADO. O dano existencial é espécie de dano imaterial. No caso das relações de trabalho, o dano existencial ocorre quando o trabalhador sofre dano/limitações em relação à sua vida fora do ambiente de trabalho em razão de condutas ilícitas praticadas pelo empregador, impossibilitando-o de estabelecer a prática de um conjunto de atividades culturais, sociais, recreativas, esportivas, afetivas, familiares etc., ou de desenvolver seus projetos de vida nos âmbitos profissional, social e pessoal. Não é qualquer conduta isolada e de curta duração, por parte do empregador, que pode ser considerada como dano existencial. Para isso, a conduta deve perdurar no tempo, sendo capaz de alterar o objetivo de vida do trabalhador, trazendo-lhe um prejuízo no âmbito de suas relações sociais. TST - RR: 14439420125150010, Relator: Maria de Assis Calsing, Data de Julgamento: 15/04/2015, 4ª Turma, Data de Publicação: DEJT 17/04/2015.

dano existencial busca tutelar os caminhos do desenvolvimento da personalidade e a forma como a pessoa se relaciona em sociedade.[515]

Também merece a atenção o chamado dano social. Uma espécie decorrente de comportamentos reiterados que causam um mal-estar social, provocando um rebaixamento no nível de vida da coletividade.[516] O dano existencial atinge especialmente questões de segurança e diminuição na qualidade de vida de um grupo e se distinguem dos danos morais coletivos, posto que enquanto estes ferem direitos personalidade de pessoas determinadas ou determináveis, enquanto o dano social viola a sociedade como um todo.[517]

Por fim, vale mencionar ainda a ideia da perda de uma chance. Embora se imponha a caracterização do dano enquanto pessoal e certo para que se verifique o dever de indenizar, os tribunais pátrios reconhecem a possibilidade de indenizar um dano oriundo da frustração de uma oportunidade de ganho patrimonial ou da redução de vantagem ocasionada por uma conduta ilícita de um terceiro. A teoria da perda de uma chance está relacionada a rápida evolução das relações sociais e as inúmeras situações imprevisíveis percebidas a partir das condutas humanas, que eliminam uma possibilidade, ou probabilidade de a pessoa obter um uma vantagem ou de evitar a ocorrência de um evento danoso.[518]

Ao aprofundar a investigação quanto o dever de indenizar face ao vazamento de dados de saúde, estas espécies de dano não apenas precisam ser lembradas, mas verdadeiramente consideradas para avaliar de forma fidedigna os possíveis impactos da exposição indevida de informações sensíveis. Pelos ditames do princípio da proporcionalidade, espera-se que o valor da indenização seja correspondente ao dano experimentado pela vítima, mas esta valoração se torna extremamente complexa, face a subjetividade das lesões a serem avaliadas nos casos de dados sensíveis de saúde.

---

515 No conceito formulado pela doutrina italiana, o dano existencial resulta, portanto, de uma lesão às atividades realizadoras não produtoras de riqueza, ou seja, ligadas à dimensão existencial do indivíduo. GONZÁLES, C. A. A.; MAMANI, S. L. Q. O dano existencial como contribuição da cultura jurídica italiana. Tradução: Fabiano Coulon. Canoas: Redes: Revista Eletrônica Direito e Sociedade, v. 6, n. 1, 2018, p. 49.

516 Danos sociais "são lesões à sociedade, no seu nível de vida, tanto por rebaixamento de seu patrimônio moral – principalmente a respeito da segurança – quanto por diminuição na qualidade de vida". AZEVEDO, A. J. Por uma nova categoria de dano na responsabilidade civil: o dano social. *In*: FILOMENO, J.G. B.; WAGNER JÚNIOR, L. G. C.; GONÇALVES, R. A. (coord.). O Código Civil e sua interdisciplinaridade. Belo Horizonte: Del Rey, 2004, p. 376.

517 TREVIZAN, T. C.; SILVA, V. B. O dano social como reflexo das novas tendências da responsabilidade civil. Revista Científica-Faculdade Pio XII, Campo Grande, v. 6, 2007, p.21.

518 AMARAL, A. C. C. Z. M. **Responsabilidade civil pela perda da chance:** natureza jurídica e quantificação do dano. Curitiba: Juruá, 2015, p. 65.

A indenização tem função de restabelecer o equilíbrio que foi rompido pela conduta ilícita, buscando trazer ao ofendido uma compensação pelo que perdeu ou sofreu em virtude do ato danificado e ao mesmo tempo, punir o ofensor para que ele não venha reincidir[519]. É um mecanismo de justiça e reparação, de caráter compensatório, que oferece ao prejudicado uma forma de ser ressarcido por prejuízos tenha experimentado mediante ato ilícito praticado por terceiro. Seria uma forma de recompensa, que visa minimizar o sofrimento e o impacto negativo causado pela violação de direitos, buscando restaurar, ao menos em parte, uma situação anterior ao ato ilícito.[520]

Quando se trata de dano material, a apuração do valor é realizada conforme dados concretos, o que permite reparar com exatidão o prejuízo sofrido no patrimônio da vítima. Contudo, quando se trata de matérias da esfera do dano moral ou de uma de suas variações, cabe ao juiz analisar o pedido de reparação de dano e se utilizar de sua liberdade para arbitrar a indenização dentro dos parâmetros pretendidos pelas partes. Não há no ordenamento jurídico brasileiro, um critério legal objetivo, que preveja a fixação do *quantum* indenizatório para o dano moral e consequentemente para as espécies de dano que dele decorrem.

Nestes casos, a vítima se vê à mercê da sensibilidade do julgador, ao tempo que espera o arbitramento de um valor condizente com os efeitos que suportou frente a conduta ilícita de um terceiro. Embora existam parâmetros básicos, como o tipo de dano, padecimento para a vítima e seus familiares, gravidade da conduta ofensiva, prejuízo permanente, entre outros, não há como afastar o olhar subjetivo do juiz, que utiliza como balizador a regra segundo a qual a indenização não pode ser insignificante, de modo a impor nova humilhação a vítima, nem elevada a ponto de representar enriquecimento sem causa.[521]

Quanto a matéria de tratamento de dados ineficiente de dados, recente decisão unânime da 2ª Turma do Superior Tribunal de Justiça - STJ deixou claro que não cabe presunção quanto ao dano moral suportado pelo titular pela exposição das informações. O mencionado julgado reformou a decisão do Tribunal de Justiça de São Paulo, que originalmente condenou uma concessionária de distribuição de energia elétrica ao pagamento de danos morais para uma consumidora que teve seus dados pessoais vazados, independentemente da comprovação da ocorrência de dano efetivo.[522]

---

519 No âmbito da legislação brasileira, o Código Civil trata da responsabilidade civil e da indenização em seus artigos 186 a 954. BRASIL, op. cit., 2002.

520 GAGLIANO; PAMPLONA FILHO, op. cit., p. 103.

521 GAGLIANO; PAMPLONA FILHO, op. cit., p. 104.

522 PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZA-

O entendimento do tribunal, reconhece a falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, mas indica que esta, por si só, não caracteriza dano moral indenizável. Para que se verifique o dever de indenizar, é necessário comprovar não apenas o vazamento das informações, mas que deste fato tenha decorrido o suposto dano experimentado pelo titular dos dados.

Retomando a questão do dano verificado mediante ao vazamento de dados de saúde, é preciso observar que mais do que comprovar um dano, seria necessário demonstrar que este pode reverberar no tempo e apresentar diversos desdobramentos, visto que o potencial lesivo da informação exposta não pode ser facilmente neutralizado. Tem-se, portanto, uma questão que vai além da materialização, suscitando a demonstração da extensão do dano, situação que ainda não foi enfrentada de forma direta pela doutrina, pelos tribunais e nem pelo próprio Estado.

Neste sentido, é preciso destacar ainda, o desafio de valorar de forma justa a indenização devida à vítima da exposição não consentida de dados sensíveis de saúde, agravado por uma série de questões que foram apresentadas ao longo deste estudo, como a volatilidade da informação exposta na rede, a impossibilidade de determinar seu alcance e o tempo pelo qual estará ativa, o alto potencial discriminatório e lesivo do tipo de informação envolvida, e ainda a possibilidade de que o dano se estenda a familiares e até mesmo uma prole eventual.

Tarefa impossível é tentar mensurar um valor justo sem a real extensão do dano e é precisamente o que se vê face ao problema da exposição indevida de dados de saúde. A

MENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido. STJ. AGRAVO EM RECURSO ESPECIAL Nº 2.130.619 - SP (2022/0152262-2).

informação difundida por meio digital cria em poucos minutos centenas de milhares de rastros e cópias, de modo que se inviabiliza o seu retorno à esfera íntima do titular. Uma vez exposta a informação, se perde o controle a seu acesso, privando o titular da decisão de compartilhar ou não algo que diz respeito a sua vida privada.

Uma única situação de vazamento de dados pode desencadear não apenas um, mas inúmeros eventos danos ao mesmo titular. A invasão ao banco de dados de determinada clínica poderia em um primeiro momento possibilitar o crime de chantagem, tal como o exemplo já mencionado do caso que ocorreu na Finlândia e anos depois resultar da perda de uma chance durante uma seleção de emprego, forçando o titular a suportar dois prejuízos, ambos passíveis de reflexos psicológicos em tempos distintos.

Outra questão pertinente se eleva na extensão do dano a outras pessoas além de seu titular direto. Ao se tratar da possibilidade da discriminação genética, ficou claro que o vazamento de dados de saúde não apenas pode prejudicar mais de uma pessoa de um grupo familiar, como pode se estender para gerações futuras. Situação que até o momento não apresenta qualquer tipo de parâmetro para mensuração econômica.

Na realidade, a visão social quanto as questões de saúde ainda apresentam muitas crenças negativas. O preconceito para com aqueles que apresentam qualquer tipo de enfermidade, síndrome ou transtorno é uma realidade, em virtude da qual muitas pessoas evitam expor determinadas condições. Assim, mediante um vazamento de dados que contenham detalhes da condição de saúde, é possível que mesmo com o decurso de um tempo razoável, esse indivíduo continue sendo estigmatizado e consequentemente venha a demandar a desindexação das páginas que contenham seus dados pessoais, em um pleito que se apoia no direito ao esquecimento.[523] Caberia aqui, como fundamento, a previsão de retirada do consentimento[524]

Mas em que pese exemplos que demonstram o alto potencial lesivo e discriminatório dos danos envolvendo exposição de dados de saúde, muito pouco foi discutido sob medidas de reparação. Em fato, os tribunais brasileiros ao analisar a matéria têm se movido de forma extremamente tímida. Sob a justificativa da devida cautela, e sem um olhar apurado quanto as possíveis consequências do vazamento de dados sensíveis

523 MARTINS, A. Direito ao Esquecimento de Dados de Saúde. *In*: DALLARI, A.; MONACO, G. LGPD na Saúde. São Paulo: Editora Revista dos Tribunais, 2021, p.184.

524 LGPD, artigo nº 8, § 5º: O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei. BRASIL, op. cit., 2018.

de saúde, as sentenças adotam valores consideravelmente inferiores ao que se espera para a problemática. Tal pontuação pode ser constada a partir da análise de julgados recentes sobre a matéria que será apresentada no tópico a seguir.

A título ilustrativo, segue algumas informações sobre os principais incidentes envolvendo vazamento de dados de saúde no Brasil nos últimos entre os anos de 2019 e 2021:

Quadro 7 - Principais incidentes envolvendo vazamento de dados de saúde no Brasil

Ano	Situação do Vazamento de Dados	Natureza da Instituição Responsável	Número de Vítimas
2019	Grupo Fleury	Instituição de Saúde Privada	Cerca de 16 milhões
2020	Laboratório Dasa	Instituição de Saúde Privada	Mais de 5 milhões
2020	Ministério da Saúde (COVID-19)	Órgão Governamental	Mais de 200 mil
2021	Hospital Albert Einstein	Instituição de Saúde Privada	Não divulgado

Fonte: Elaborado pela autora.

Por esta visão, resta clara necessidade da implementação de uma tutela rigorosa para os dados sensíveis de saúde, de modo a assegurar a concretização dos princípios constitucionais da igualdade, liberdade, e da não discriminação. A exposição de informações desta natureza traz consequências graves aos titulares e ao Estado, vez que acarreta um desequilíbrio social. Por isso, não apenas se faz pertinente, mas necessário lançar mão de um olhar interdisciplinar na busca da identificação dos reais desdobramentos da informação coletada e tratada na esfera de saúde, alcançando as nuanças e buscando respostas que a LGPD, por seu caráter generalista não chega a responder.

Em que pesem todos os benefícios da informatização dos dados de saúde, não é possível ignorar os riscos de dano frente a situações de vazamento de dados. Mesmo com o *compliance* delineado pela LGPS e pelas políticas públicas de saúde, ainda não é possível afastar completamente o risco de uma exposição indevida. Incidentes de falha na proteção dos dados de saúde com maior e menor alcance tem sido reportados nos últimos anos, alguns tendo ascendido aos tribunais pátrios, que discutem como aplicar na via prática as indicações de responsabilidade face ao dano sofrido pelo titular dos dados, dispostas na LGPD. Este desafio será exemplificado a partir da análise de decisões recentes quanto a matéria, que se expõe a seguir.

6.5 Análise de decisões envolvendo dados sensíveis de saúde emanadas por tribunais brasileiros

Por meio da interpretação e mediação do texto normativo, se viabiliza a aplicação do direito na vida prática. Em que pese se tratar de uma matéria recente, cujas demandas ainda não ascenderam de forma expressiva aos tribunais superiores a ponto de consolidar jurisprudência, é importante verificar através de exemplos reais, a direção na qual caminha o judiciário brasileiro quanto a questão do dano no vazamento de dados sensíveis de saúde.

Conforme previamente exposto não se tem um entendimento pacífico quanto ao sistema de responsabilidade a ser aplicado na esfera civil mediante a situação de exposição não-autorizada de dados sensíveis. Apesar dos argumentos a favor de cada um dos sistemas, determinados posicionamentos do Poder Judiciário indicam uma terceira via, cuja viabilidade necessita ser ponderada. Ademais, ainda paira no ar a delicada questão do potencial discriminatório e lesivo dos dados de saúde que até o presente momento não encontrou a devida consideração na esfera jurídica.

Por esta pesquisa, foi apontando que no entendimento dos tribunais, a obrigação de indenizar está diretamente atrelada a configuração de um dano. Logo é preciso comprovar que a violação do direito à privacidade dos titulares de dados sensíveis de saúde acarretou efetivo prejuízo, afastando a hipótese de dano indenizável automático frente ao tratamento irregular de dados. Mas o se discutir o dano de base digital, é preciso considerar fatores específicos e trabalhar uma visão interdisciplinar, a fim de compreender seus reais impactos e alcances.

A proteção à saúde só pode ser concretizada a partir da efetivação da segurança jurídica disposta em sua esfera documental e informativa e neste sentido a LGPD representa um grande avanço. De posse de um arcabouço protetivo que trata tanto de indicativos de condutas e responsabilidades como de sanções, indivíduos que se sentem lesados pela exposição indevida de seus dados pessoais, passaram a buscar seus direitos e exigir reparação. O exame destes pedidos, tem gerado as primeiras respostas sobre como a LGPD pode repercutir na vida prática dos usuários dos sistemas de saúde.

Diante desse cenário, uma análise documental de decisões de tribunais brasileiros se mostra um importante caminho para a compreensão e interpretação da matéria jurídica face as adversidades verificadas na vida real. A técnica bibliográfica, neste

caso, se revela insuficiente para captar a dinamicidade e complexidade inerentes aos processos envolvendo transmissão de dados sensíveis de saúde, cabendo discutir os principais elementos que compõe a argumentação das partes, bem como interpretação do julgador na busca por reestabelecer um equilíbrio violado na dimensão informativa da saúde.

É importante ressaltar que esses documentos, embora substanciais, ainda não passaram por um tratamento analítico aprofundado. A análise documental representa um instrumento flexível e adaptável às diversas nuances e particularidades presentes nos casos de transmissão de dados sensíveis de saúde. Por este motivo, antes de adentrar no texto das decisões e na discussão quanto aos entendimentos apresentados nos julgados, é de suma importância destacar os critérios e bases de pesquisa utilizados para a seleção das decisões analisadas.

Para a análise documental, foi realizada pesquisa de decisões prolatadas entre os anos de 2020 e 2023 nos sítios eletrônicos oficiais dos principais tribunais brasileiros, a partir das palavras-chave: responsabilidade civil, dano moral, vazamento de dados sensíveis, dados de saúde e privacidade. Conforme o objetivo desta pesquisa, foram selecionados acórdãos do Superior Tribunal de Justiça, Tribunal de Justiça de Minas Gerais, Tribunal de Justiça do Rio de Janeiro e Tribunal de Justiça de São Paulo.

Cada uma das decisões analisadas apresenta informações específicas que auxiliam na compreensão das nuances jurídicas envolvidas do caso de vazamento de dados de saúde. Assim, os textos foram selecionados com base nos argumentos apresentados pelas partes e pelo Poder Judiciário[525], bem como por suas falhas e contribuições, permitindo embasar uma discussão que visa o aprimoramento do sistema jurídico no enfrentamento dos desafios relacionados à proteção de dados sensíveis na área da saúde.

Para concretizar a verificação dos textos, foram eleitos critérios aptos a destacar fundamentos e teorias aplicadas aos casos em análise. Para fins didáticos, a sequência adotada se inicia com a referência e histórico do caso, avaliação da presença dos elementos para configuração da responsabilidade civil, identificação do tipo de dano

525 O Judiciário tem um papel estratégico na sociedade. Tal poder não exerce apenas atividades burocráticas e legalistas, mas tem papel importante nas democracias contemporâneas. No sistema *common law* é comum que o Judiciário adentre na esfera das políticas públicas, pois as normas possuem conteúdo amplo e necessitam de uma complementação ou interpretação. FERNANDES, R. G.; OLIVEIRA, L. P. S. Notas Sobre o Papel Da Herança Histórica Brasileira Na "Expansão" Do Poder Judiciário No Domínio Das Políticas Públicas. **Revista Direitos Culturais**, Santo Ângelo, v. 15, n. 37, p. 123-143, 2020. Disponível em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/205. Acesso em: 23 abr. 2023.

e por fim, a avaliação de como se deu a indenização, tal como se infere do primeiro julgado apresentado a seguir.

A primeira decisão analisada é oriunda do Tribunal de Justiça do Estado de São Paulo, e versa frontalmente sobre um episódio de vazamento de dados sensíveis de saúde, que acarretou danos à titular que deveria ter sua identidade e informações preservados. Este julgado apresenta extrema relevância pois, na configuração do dano se encontram presentes elementos de ordem moral e emocional, que ultrapassam a figura da titular e atingem o grupo familiar.

Trata-se de acórdão proferido em sede de recurso de apelação (nº 1041607-35.2021.8.26.0100) proferido pela 1ª Câmara de Direito Privado e sentença oriunda da 10ª Vara Cível Central da Comarca de São Paulo, cujo apelante é Cryopraxis Criobiologia Ltda e a apelada: Larissa Ribeiro de Almeida Sales. Os desembargadores da Câmara negaram provimento ao recurso, votação unânime, de conformidade com o voto Relator integrante do acórdão[526].

Da análise do relatório, consta que o juízo de 1º proferiu sentença que julgou procedente ação cominatória e de indenização por danos morais movida pela autora da demanda em face de Cryopraxis Criobiologia Ltda- banco de células-tronco do sangue do cordão umbilical- condenando-a ao pagamento de indenização por danos morais no valor de R$ 10.000,00 (dez mil reais) com correção data da sentença e juros de mora a partir do trânsito em julgado. A sentença também determinou que a ré informasse "em 05 dias, quem divulgou os dados pessoais, quais os dados da autora que possui e para quem os dados foram repassados, além de providenciar a eliminação de tais dados". A ré foi condenada, ainda, ao pagamento das custas, despesas processuais e honorários advocatícios de 15% sobre o valor da condenação.

526 APELAÇÃO CÍVEL – IMPROBIDADE ADMINISTRATIVA – VIOLAÇÃO A PRINCÍPIOS – Prefeito e Secretário Municipal da Saúde que acessaram, sem autorização do titular, de familiares ou por ordem judicial, dados pessoais sensíveis de munícipe falecido, com o propósito de instruir ação obrigacional cumulada com pedido de danos morais contra a família do "de cujus", demanda proposta pelo Prefeito em razão de postagem realizada por um familiar nas redes sociais – INÉPCIA DA INICIAL – Inocorrência – ILEGITIMIDADE PASSIVA DO SECRETÁRIO MUNICIPAL – Inocorrência – Servidor que não agiu conforme dever legal, não sendo hipótese de subordinação hierárquica – CONDUTA ÍMPROBA - Lei Geral de Proteção de Dados que impõe sigilo a dados pessoais sensíveis e obsta o seu uso para fins pecuniários – Reforma da Lei de Improbidade Administrativa – Lei nº 14.230/2021 - Artigo 11, inciso III – Princípios da Administração Pública infringidos ao revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo, propiciando beneficiamento por informação privilegiada – Ato de improbidade caracterizado – SANÇÃO – Multa civil – Proporcionalidade da sanção aplicada, em observância aos parâmetros do artigo 17-C da Lei de Improbidade Administrativa – Sentença mantida – Recurso dos réus improvido. (TJ-SP - AC: 10081247220208260286 SP 1008124-72.2020.8.26.0286, Relator: Maria Laura Tavares, Data de Julgamento: 21/02/2022, 5ª Câmara de Direito Público, Data de Publicação: 23/02/2022)

Insatisfeita com a decisão, a empresa ré apelou ao Tribunal de segunda instância alegando que a sentença desvirtuou o disposto na LGPD e que teria obtido junto a terceiros dados cadastrais não sensíveis e não sigilosos. Sustentou que a demanda deveria se voltar contra o médico da autora ou a empresa que compartilhou os dados. Esclarece que os dados foram obtidos apenas para que fosse possível a divulgação de seus serviços, em regular ação lícita, prevista no art. 7º, inc. IX, da Lei nº 13.709, presente autorização da autora para utilização de seus dados.

A apelante negou ter conhecimento da gravidez da autora, e acresceu que instituiu programa de cuidado na preservação de dados de clientes e, por não ter atuado como controladora, não se justifica a imposição de obrigação atinente à identificação de pessoas que teriam recebido os dados da autora. Pugnou pela ausência de ato ilícito; inexistência da violação de dados pessoais, e, portanto, sem dano moral a ser reparado.

Contrarrazões devidamente apresentadas. O relator passou ao voto no qual aduziu ele, em suas considerações, que a autora da ação tomou conhecimento de que estava grávida através de exames ambulatoriais, em dezembro de 2020. Todavia, em fevereiro de 2021, foi constatada a perda gestacional. De acordo com o voto do relator, a autora afirmou que dias após o aborto sofrido, a empresa ré teria encaminhado mensagem, via *whatsapp*, com oferta a respeito do serviço por ela prestado de coleta e armazenamento de cordão umbilical.

Embora a ré afirme que se utilizou de dados não sensíveis e não sigilosos, referentes apenas ao nome e telefone celular da autora, não é o que se depreende dos fatos narrados. A autora estava grávida. Esta informação é um dado, que foi utilizado pela ré em sua atividade empresarial com o fito de angariar novos clientes. Para o MM relator, a gravidez da demandante é, notadamente, um dado sensível como dispõe o art. 5º, inc. II, da Lei nº 13.709/2018, *in verbis*: "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" (destaque contido no voto do relator).

Reiterou em seu voto que a própria ré confirma que a autora não buscou os serviços dela. Logo, a ré somente poderia ter conhecimento da gravidez da apelada a partir do compartilhamento por terceiros de dado sensível. A ré, embora tenha atuado em preponderância, como operadora, também atuou como agente de tratamento da informação recebida e, por isso, nos termos do art. 18, § 3º, da Lei nº 13.709/18, tem a obrigação de identificar o responsável pela coleta de dados da autora e apresentar esta

informação nos autos, o que ainda não foi cumprido pela ré, nos termos da decisão do juízo *a quo*.

Em seus fundamentos, o desembargador entendeu não haver verossimilhança na alegação da ré de que não tinha conhecimento da gravidez da autora. A própria empresa demandada confirmou que trabalha com coleta e armazenamento de cordão umbilical de bebês recém-nascidos. Dessa forma, acresceu o relator, natural seria que dirigisse sua atividade de prospecção de novos clientes a mulheres grávidas, razão pela qual não convence a argumentação da apelante de que não teria se utilizado de dado sensível pertencente à apelada.

Ao contrário do alegado nas razões recursais, não há demonstração, segundo os argumentos do magistrado ad quem, de que a autora tenha expressado seu consentimento a respeito do dado sensível coletado e armazenado, prova que incumbia à ré, nos termos do art. 8º, § 2º, da Lei nº 13.709/18. Nos termos do art. 42, do mesmo diploma legal, a ré responde, portanto, pela utilização indevida de dado sensível, que, seguramente, causou à autora dano moral, pois à ocasião do contato realizado pela ré, a requerente não mais apresentava estado gravídico. Dessa feita, a conduta da ré, certamente, além de representar violação ao direito de privacidade, fez a autora reviver sofrimento decorrente da perda gestacional.

Em sequência apresenta anotações de consagrados teóricos do Direito Civil Brasileiro, a exemplo de Cristiano Chaves de Faria, com a pretensão de melhor embasar os fundamentos por ele apresentados no voto, assim como apresentou decisão da mesma colenda câmara que integra, o qual se aqui se reproduz:

"AÇÃO INDENIZATÓRIA - pretensão à reparação de danos morais por comercialização de dados pessoais sigilosos, bem como à sua exclusão da plataforma da ré - Ré revel - Independentemente da presunção de veracidade dos fatos afirmados na inicial, decorrentes da revelia, no caso ficou provado que a ré oferece em seu site a quem pagar, vários tipos de acesso a dados pessoais de qualquer cidadão, ou empresa - Violação da LGPD que se revela evidente Indenização que se impõe com base no art. 42 dessa mesma lei. Sentença de improcedência. Apelo provido para julgar a ação procedente, com determinação" (Apelação nº 1013341-62.2021.8.26.0577, Rel. Des. Rui Cascaldi, j. 31.03.2022). (sic)

Finalizou seu voto, declarando adequado fundamente à sentença proferida no juízo de origem, devendo ser integralmente confirmada. Desprovido o recurso, eleva-se a verba honorária para 20% sobre o valor da condenação. Recurso improvido.

Na decisão ora apresentada, restou claro o entendimento do magistrado de 2º acerca dos danos causados à apelada no que toca ao desrespeito à manutenção da sua privacidade assegurada em lei, sobretudo no presente caso, dada à sutileza do tema envolver vazamento de dados relacionados à uma mulher que sofrera aborto, causando-lhe ainda mais incômodo e dissabores, em uma situação que já configuraria o dano moral.

No presente julgado verificou-se de forma cristalina a presença dos elementos caracterizadores da responsabilidade civil, a saber: primeiro a conduta do agente que agiu de forma ostensiva com o envio de mensagem de *WhatsApp* para lhe ofertar coleta e armazenamento do cordão umbilical. A conduta é própria prática da ação lesiva à autora da ação recém-saída de uma perda gestacional, o que agrava a situação abordada, vez que a gravidez se afigura como estado peculiar que produz diversas modificações no organismo da mãe e envolve todo um grupo familiar. O viés psicológico se torna impossível de ser ignorado dada a fragilidade física e emocional da vítima.

Desta forma, o elemento dano é o próprio prejuízo causado e, no caso em espécie, foi considerado em seu aspecto moral, que por sua própria natureza, torna-se insuscetível de avaliação pecuniária, assumindo a indenização caráter indenizatório. O prejuízo para a apelada foi relatado de forma expressa pelo magistrado ao entender que além da abordagem feita à apelada representar uma violação ao direito de privacidade, fez com que também revivesse sofrimento decorrente da perda gestacional. Esse tipo de dano é exteriorizado pela dor, angústia, tristeza, sentimentos que abalam a condição psicossocial da vítima, os quais parecem ter permeado a autora da demanda ao receber as mensagens ofertando a coleta das células.

Importante destacar que diferente do que alegou a empresa ré, a gravidez não é um mero dado cadastral/pessoal, e poderia até mesmo levar à responsabilização solidária do laboratório que informou à apelante o dado atinente à gravidez. Reitere-se ainda que ao revés do que assevera a apelante, não havia nos autos qualquer comprovação da autorização da titular dos direitos acerca de divulgação de informações, e se não havia consentimento, inclusive, para uso de fins específicos, como o uso de informações sobre a gravidez, houve violação à proteção dos dados

O nexo causal, por sua vez também é elemento caracterizador da responsabilidade que se revela na situação, tendo em vista que a relação de causa e efeito se faz presente entre a conduta do agente e o resultado provocado. Destaca-se ainda, o elemento culpa, dentre os caracterizadores da responsabilidade civil. A culpa parece o ponto central para a caracterização da natureza da responsabilidade civil, se objetiva ou subjetiva.

Se há necessidade de comprovação da culpa, seja ela por imperícia, imprudência ou negligência, a situação clama pela responsabilização subjetiva. De outra sorte, caso não seja necessária essa comprovação, afigura-se a modalidade objetiva de responsabilidade.

O acordão objeto deste enfrentamento discursivo, reiterou os termos da decisão do juiz de 1º que entendeu, de pronto, haver conduta lesiva à privacidade da apelada, responsabilizando a empresa pelo vazamento de dados sensíveis à empresa que enviou mensagens para a apelada. Tal situação abre margem para que se questione o critério adotado pelos julgadores do caso em tela.

Do bojo da decisão, resta perceptível que o entendimento do magistrado enveredou pela esteira da responsabilidade objetiva, pois não fez menção a ausência de elementos comprobatórios da culpa da empresa ré, ao contrário, reclamou não existirem nos autos, comprovação da autorização da autora para divulgação de dados, como alegado pela apelante. Não só o magistrado o relator entendeu que havia, de fato ocorrido vazamento de dados sensíveis, como determinou que fossem apresentados a origem deles, e a eliminação dos mesmos em poder de terceiros não autorizados.

Por fim, merece ressaltar a questão da mensuração da quantia arbitrada a título de indenização pelo dano moral sofrido pela apelada. Embora o desembargador não tenha adentrado no mérito do tema em apreço, tem sido recorrente em diversos julgados observados que os valores não costumam ultrapassar um teto mediano de R$ 5.000,00 (cinco mil reais), inclusive valor determinado em outro acórdão a ser apresentado nesta pesquisa.

Todavia, na condenação que ora se discute, este valor foi de R$ 10.000,00 (dez mil reais), o que leva a crer que a majoração do valor em relação à média das condenações, de modo geral, se deveu ao fato do estado gravídico da autora e a angústia por ela sentida em razão da importunação lhe ter causado mais dores pelo aborto sofrido, mesmo que o valor não pareça atender o critério da condição econômica da Cryopraxis Criobiologia Ltda. Um grande banco de células-tronco do sangue do cordão umbilical não deveria arcar com o ônus superior ao determinado na decisão, especialmente para gerar a consciência da necessidade de evitar reincidência? Há que se pensar na força econômica das empresas e instituições envolvidas nos casos de vazamento de dados sensíveis de saúde, ponto que seguirá sendo objeto de reflexão na próxima decisão a ser analisada.

Apresentando uma linha mais técnica, o segundo julgado a ser trabalhado é uma Apelação do Tribunal de Justiça do Rio de Janeiro que tramitou sob o número

0031396-89.2016.8.19.0208, abaixo apresentada[527]. O acórdão da referida apelação traz um caso de ação indenizatória baseada em golpe que requereu transferência bancária de valor por um suposto preposto do réu, qual seja um hospital particular do Rio de Janeiro, o Hospital Memorial Fuad Chidid, o que teria ocorrido mediante conhecimento de informações da família da vítima.

O juízo *a quo* proferiu sentença de procedência ao pedido indenizatório e o TJ -RJ manteve a decisão por entender que o Hospital em comento falhou na proteção de informações pessoais do paciente, as quais foram utilizadas por estelionatários. O Judiciário entendeu que prepostos do Hospital participaram do hackeamento do sistema informatizado daquela instituição de saúde, viabilizando informações ostentadas pelo criminoso, tais como nome do médico que atuava no tratamento e até o detalhe do box do CTI ocupado pelo paciente, autor da ação indenizatória.

Ainda integraram o acórdão, o entendimento dos magistrados quanto ao vazamento de informações pessoais de privacidade informacional, a teoria do risco do Empreendimento e a proteção do sigilo dos dados do paciente que integra o trabalho do prestador dos serviços. Nessa toada de pensamento, os desembargadores acordaram que ainda que perpetrada por terceiro, a fraude não constitui causa de exclusão de responsabilidade, referência essa baseada na inteligência do Enunciado 94 da Súmula TJRJ, que assim se posiciona: "Cuidando-se de fortuito interno, o fato de terceiro não exclui o dever do fornecedor de indenizar."

Os desembargadores da 21ª turma cível do TJRJ votaram pela obrigação do Hospital de indenizar o dano material, em conformidade com o Princípio da Reparação do Dano Integral, bem como pela configuração dos danos morais, preservando os princípios da Razoabilidade e Proporcionalidade. Também majoraram os honorários advocatícios em razão da reiteração da sucumbência, em sede recursal. A câmara, por unanimidade, negou provimento ao recurso, nos termos do voto da Relatora.

Antes da análise do julgado convém mencionar, de modo breve, uma síntese do que houvera em termos de fatos, os quais levaram o autor da ação indenizatória a pleitear a reparação na via judicial: o autor da ação indenizatória, aduziu em sua inicial que sua avó de 82 anos de idade, estava internada no HOSPITAL MEMORIAL FUAD CHIDID LTDA e recebeu telefonema, noticiando a gravidade do estado da paciente, não sendo permitida qualquer visitação naquele momento. Na mesma ocasião fora

527 RIO DE JANEIRO Tribunal de Justiça do Rio de Janeiro - TJ-RJ (21ª Câmara Cível). **Apelação - APL: 00313968920168190208**. Relator: Des(a). REGINA LUCIA PASSOS, Data de Julgamento: 09/07/2020, 2020.

solicitada a transferência de R$ 1.800,00 (hum mil e oitocentos reais) para a conta bancária da suposta Diretora do Hospital, a fim de realizar tomografias urgentes não autorizadas pelo plano de saúde.

De acordo com o apelado, na mesma ligação, lhe foram repassadas pelo golpista, várias informações acertadas, de acesso (teoricamente) exclusivo dos prepostos do réu, tais como: o box do CTI em que estava alocada a paciente, o nome de um dos médicos que assistiam a enferma, bem como o plano de saúde de sua avó. Alegou ainda que, após a realização da transferência bancária, lhe solicitaram mais uma, desta feita para a suposta dona da farmácia, no valor de R$ 1.500,00 (hum mil e quinhentos reais), referente a um antibiótico necessário, com cobertura também recusada pelo plano de saúde. Expôs que passou a desconfiar de fraude, visto que as contas bancárias indicadas eram de pessoas físicas.

Relatou que descobriu, por ligação telefônica ao hospital apelante que se tratava de um golpe já aplicado contra outras sete famílias, de acordo com informação de uma enfermeira do CTI. O número de vítimas do referido golpe ainda aumentou para dez, naquele mesmo dia, segundo uma fisioterapeuta. Aduziu que, foi frustrada a tentativa de bloqueio bancário da operação, pois o montante já havia sido movimentado pelo estelionatário e acrescentou que fez registro do ocorrido perante a autoridade policial, acarretando a identificação de dois dos beneficiários das contas bancárias destinatárias das transferências, mas o banco e o Hospital negaram o estorno do valor.

Aduziu que tentou resolver a questão junto ao Diretor do Hospital e com a chefia do jurídico do Hospital, sem êxito. Também acrescentou que o golpista ameaçou de morte uma das vítimas, que não teria caído no golpe. Disse que não havia controle para a o acesso ao hospital, nem segurança e, que o cadastro junto à recepção é facultativo, e ali não são registrados fotografia ou documento dos visitantes. Concluiu ter experimentado danos morais decorrentes dos fatos retro mencionados.

Em decorrência da narrativa e razões sustentadas, postulou: "… Condene a empresa Ré, A INDENIZAR O AUTOR À TÍTULOS DE DANOS MATERIAIS, o valor de R$ 1.800,00 (um mil e oitocentos reais), referente ao depósito em conta do suposto médico que respondia pelo Hospital (réu nessa demanda); Condene a empresa Ré, ainda, A INDENIZAR O AUTOR À TÍTULOS DE DANOS MORAIS, no equivalente a 35 (trinta e cinco) salários mínimos, que corresponde nessa data ao valor de R$ 30.800,00 (trinta mil e oitocentos reais), por todos os dissabores sofridos por ele, que deverá ser atualizado com juros e correção monetária;"

Na Sentença, indexador 121, publicada em 15/08/2019, constou o seguinte dispositivo: "isto posto, JULGO PROCEDENTE, em parte, a pretensão autoral para condenar o réu ao pagamento de indenização por danos materiais em R$ 1.800,00 (hum mil e oitocentos reais), corrigidos monetariamente desde a data do desembolso e acrescidos de juros de mora desde a citação, e ao pagamento de indenização por danos morais em R$ 5.000,00 (cinco mil reais), corrigidos desde a publicação da sentença e acrescidos de juros de mora de 1% ao mês desde a citação. CONDENO a parte ré nas despesas processuais e no pagamento de honorários advocatícios ao patrono da parte autora em 10% sobre o valor da condenação, com fulcro no art. 85, § 2º, do CPC."

Em sede de recurso o Hospital, apelou alegando que o prejuízo do autor foi produto de sua imprudência em não se certificar dos fatos antes de ceder à solicitação do estelionatário, fato que não guarda relação com nenhuma ação ou omissão do apelante, e sim com um problema de segurança pública. Acresceu que os clientes são orientados a somente realizar quaisquer pagamentos no caixa do Hospital e nunca por depósito bancário; e que presta serviços de excelência; aduziu também em outro julgado semelhante a decisão foi pela improcedência do dano e disse não se ter demonstrado que qualquer preposto do Hospital tenha ligado para solicitar quantias, não havendo ilícito a lhe ser imputado; alegou por fim, que o Hospital não tinha relação causal com os fatos em questão e não ocorreu dano moral e a indenização foi arbitrada sem razoabilidade, promovendo enriquecimento ilícito.

Mantida a sentença, a relatora trouxe suas fundamentações, as quais serão exploradas adiante, no intuito de demonstrar por meio de análise de alguns aspectos considerados cruciais para o desenvolvimento desta pesquisa, a problemática da mensuração do *quantum* indenizatórios e suas repercussões. A pretensão é apreciar as razões que levam os magistrados de modo geral, independente do grau de jurisdição em que atuam, a fixar os parâmetros indenizatórios e como estabelecem suas valorações a partir dos possíveis elementos da responsabilidade civil ali presentes.

Durante a trajetória desta pesquisa, percebeu-se a dificuldade em detectar, de forma mais precisa, como o Estado, especialmente o Poder Judiciário, tem se comportado no que toca às questões relativas à proteção, e, sobretudo, ao vazamento de dados sensíveis no âmbito da saúde. No que diz respeito à problemática de proteção dos dados sensíveis pelo Estado- atuação legislativa, tem-se o amparo de leis protetivas. No aspecto do Executivo, os diversos bancos de dados são direcionados a observar normas de proteção, ou deveriam fazê-lo, em respeito à sensibilidade do tema, porém, ainda se carece de fiscalização efetiva.

A problemática exposta, se amplia porque nem sempre esses parâmetros estabelecidos em lei são devidamente preservados, ocasionando prejuízos de proporções variadas às pessoas que porventura, tenham sido objeto desse descuido. Diante disso se questiona como poderia se ofertar a vítima uma verdadeira reparação, indagação pertinente que se busca responder com respaldo nas decisões aqui apresentadas.

O caso acima relatado traz alguns pontos que merecem destaque: primeiro, o pedido apresentado pelo autor da ação no que tange ao dano moral, aspecto grifado na narrativa do fato; e o outro a condenação nessa mesma instância jurisdicional. Em termos práticos, verifica-se uma significativa diferença entre o pedido e o concedido em termos de danos morais. Na perspectiva do dano material essa dificuldade não é sentida, posto que o valor despendido pela vítima do golpe é facilmente percebido por meio das transferências bancárias, devendo ser ressarcido no mesmo montante, como fora.

O demandante da ação requereu o valor de 35 (trinta e cinco) salários-mínimos, em decorrência dos dissabores sofridos; a condenação arbitrou os danos morais no montante de R$ 5.000,00 (cinco mil reais). Na oportunidade da decisão o valor solicitado seria, pois em torno de 30.000,00 (trinta mil reais). Não cabe nessa discussão fazer uma mensuração de juízo individual, mas tão somente analisar os parâmetros e as extensões do dano, buscando compreender a satisfação reparadora do referido dano.

Da leitura do voto da relatora, depreende-se que seus critérios de valoração de conduta transitam pelo direito do consumidor e assim estabelece ela que a responsabilidade do Hospital é objetiva, como preconizado pelo Código de Defesa do Consumidor, em seu art. 14§ 3º, II. Entretanto, a discussão parece ter maior alcance: a responsabilidade neste caso ganha contornos que perpassam a ideia da proteção do consumidor, esta certamente de grande importância. Os elementos da responsabilidade civil se fazem presentes no caso em espécie. Percebe-se a conduta do agente causador do dano: o hospital que agiu de forma omissiva ou pouco cautelosa ao não resguardar a contento os dados dos pacientes, facilitando destes. O dano, que no jugado em análise foi considerado em seus aspectos moral e material; a culpa, e esse, certamente, é o ponto crucial para a caracterização das duas modalidades de responsabilidade, e por fim o nexo causal que aponta a relação entre o efeito e a conduta, também presentes *in casu*.

Comporta maior atenção o elemento culpa. Na abordagem que ora se desenvolve, a culpa restou demonstrada na medida que o Hospital apelante admite que outros casos de mesma configuração ocorreram. Assim, infere-se que houve vazamento de dados pessoais sensíveis relacionadas ao tema saúde, previstos em lei (art. 5º, II).

Embora não dito em tom expresso no voto da ministra da 21 ª Câmara Cível do TJRJ, caracteriza-se na espécie, um dano de natureza subjetiva, dada a necessidade de comprovação da culpa. Frise-se que a culpa do Hospital apelante não é propriamente relacionada à solicitação de quantia em dinheiro, mas a falha na proteção dos dados da paciente hospitalizada.

Este elemento está ligado à intenção do agente durante o ato, podendo ser representada por um agir negligente, imprudente ou imperito. Ao que parece da narrativa do autor da ação indenizatória, a conduta do agente não manteve o cuidado e atenção devidos com os dados da paciente internada e dos demais pacientes vítimas do golpe naquela ocasião. Também poderia se vislumbrar uma conduta imperita, representada pela atuação sem o conhecimento ou habilidades técnicas necessárias dos dados armazenados, sem o devido treinamento ou preparo de quem a responsabilidade de os guardar.

Nesse sentido, o voto da desembargadora remete claramente por meio de citações doutrinárias, a necessidade de condutas cautelosas quanto à preservação dos dados, como se lê a seguir: "o direito à proteção de dados pessoais é um direito novo e ativo, que impõe o funcionamento de um sistema de segurança para proteger o indivíduo sempre que seus dados pessoais são coletados e utilizados". (sic)

Da referência utilizada pela relatora do julgado, percebe-se ela entende a necessidade de uma conduta segura e cauta do agente, caracterizando assim a noção de responsabilidade subjetiva, pois somente diante desse não agir cauteloso se vislumbraria a culpa. E esta por sua vez é condição necessária para a existência de responsabilidade subjetiva.

De outra sorte, na sequência de sua fundamentação, a magistrada retoma à tese da Teoria do Risco do Empreendimento e menciona que o fornecedor de bens e serviços tem o dever de responder pelas falhas e vícios resultantes do empreendimento, independente de culpa. O *decisum* pautou-se na responsabilidade objetiva como no princípio referido pela douta relatora? Ou na responsabilidade subjetiva que clama por culpa a ser provada pelo possível lesado em razão da conduta daquele que não agiu com as devidas cautelas?

Diversos precedentes e julgados foram colacionados como fundamentos da decisão, e em vários deles, surge outra vez a ideia de fraude perpetrada por terceiro, com base em caso fortuito interno, baseados na Teoria do Risco do Empreendimento, caracterizando assim, a responsabilidade objetiva. Tais argumentos utilizados na fundamentação do

voto são apoiados na Súmula 479 do STJ e Enunciado 94 do TJRJ, segundo a qual "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias." (grifo nosso). Bem como o Enunciado 94 do TJRJ: "Cuidando-se de fortuito interno, o fato de terceiro não exclui o dever do fornecedor de indenizar."

Em ambas as situações utilizadas como parâmetros, nota-se uma menção a casos relacionados a dados pessoais, de acordo com a previsão da LGPD, em seu art. 5º, I. Todavia, na presente decisão, objeto desta análise, o caso perpassa a fronteira dos dados pessoais; são dados pessoais sensíveis, em conformidade com o mesmo art. 5º da LGPD, agora em seu inciso II por tratar de vazamento de dados relacionados à saúde, como bem preconiza a referida Lei.

Portanto, o que seria um fundamento inicialmente alicerçado na ideia de responsabilidade objetiva, depois passa a ganhar contornos de reponsabilidade subjetiva, sendo necessária a apresentação de prova da culpa. A condição de provar essa culpa, pode, entretanto, em muitos casos, tornar-se inviável, uma vez que o existe uma grande dificuldade na apresentação dos elementos comprobatórios. Desse modo é possível até mesmo a configuração da prova diabólica[528], instituto vedado pelo ordenamento jurídico.

Ademais os dados pessoais sensíveis carecem de tratamento diferenciado, e própria lei assim já o fez. Resta a aplicabilidade dessa condição particular, via Poder Judiciário, quando da solução dos conflitos oriundos da falta de preservação destes dados. O porquê da necessidade dessa maior proteção se faz verificar nos efeitos possíveis para aquele que teve seus dados expostos, podendo, inclusive essa ação reverberar em terceiros, como filhos e cônjuges.

Ainda na perspectiva dos fundamentos do voto, a relatora menciona que a prova apresentada pelo autor da ação no juízo de piso, não se revela cabal, embora as tenha considerado preponderantes no cotejo com as alegações da ré. Senão leia-se a passagem retro mencionada: "Assim, conquanto não se revele cabal, a prova apresentada pelo autor preponderou no cotejo com as alegações da ré, baldias de comprovação." (sic)

Por fim, e não menos importante é a mensuração do dano. O primeiro deles, o material, fora consubstanciado pela transferência bancária, e confirmado pelas decisões

528 Compreende-se pela denominação "prova diabólica", a prova impossível ou excessivamente difícil de ser produzida. Mediante a impossibilidade de acesso ou meios de produção, a parte seria lançada em uma situação desigual, que se distancia da visão da razoabilidade, visto que se lhe atribui a missão de apresentar fato ou documento difícil ou impossível de se provar.

de ambas as instâncias jurisdicionais. Como corriqueiro na esfera do Poder Judiciário, os danos extrapatrimoniais costumam ser duramente enfrentados no sentido de que dissabores ou chateações não caracterizam danos; é necessário que sejam maculados direitos como a privacidade, honra, imagem, saúde, dentre outros.

No presente caso, a magistrada entendeu que os danos exorbitaram a seara do trivial, causando constrangimentos e angústias maiores que o normal. Delineou ainda que para a fixação do dano moral é necessário observar dos princípios da proporcionalidade e razoabilidade, em como observar a condição econômica do ofensor e ofendido, a gravidade da lesão e sua repercussão. Também ressaltou que não se pode olvidar da moderação para que não haja enriquecimento ilícito ou se possa desprestigiar o caráter pedagógico-punitivo da indenização. E por todos esses argumentos decidiu manter o valor da condenação já determinada pelo juiz *a quo.*

Diante do quantum apresentado como reparador do dano experimentado pelo autor, surgem questionamentos: o critério da condição econômica do Hospital apelante foi de fato levada em conta? Um hospital particular de grande porte do Rio de Janeiro não teria condições de pagar um valor para além do arbitrado? O valor da condenação satisfaz a realidade da conduta do Hospital?

No curso dessa pesquisa e com base nos julgados e prejuízos causados àqueles que deveriam ter seus dados pessoais sensíveis preservados, as condenações parecem não alcançar o propósito punitivo-pedagógico e reparador das sanções. Para grandes empresas, como o exemplo *in casu,* o poder econômico do Hospital é bem superior à condenação imposta. E os danos causados ao apelado não fazem jus aos prejuízos e constrangimentos, vez que os dados podem ser usados em outros contextos e situações que expõem de maneira invasiva a vida dos lesados pelo dano.

Outro caso que contém elementos importantes para a discussão aqui proposta é a Apelação do Tribunal de Justiça de Minas Gerais de número 5002051-68.2021.8.13.0148[529]. O acórdão em tela traz um recurso de apelação e reexame necessário interposto pelo município de Lagoa Santa-MG, em face de sentença de ordem proferida por um juiz da referida comarca. Em sede de 1º de jurisdição, fora impetrado um Mandado de Segurança por vereadores da Câmara Municipal daquela cidade contra ato praticado pelo prefeito.

A segurança foi concedida para determinar à autoridade impetrada - prefeito- que fornecesse todos os dados solicitados pelos vereadores, os quais estariam ali

529 MINAS GERAIS. Tribunal de Justiça e Minas Gerais - TJ-MG (5ª Câmara Cível). **AC: 10000230016917001 MG**. Relator: Áurea Brasil, Data de Julgamento: 02/03/2023, Câmaras Cíveis, 2023.

funcionando como agentes públicos legalmente autorizados ao acesso de dados particulares imprescindíveis à proteção do interesse público, cuja disponibilização independe do consentimento de seus titulares. O acesso encontra guarida na Lei nº 12.527/2011, em seu art. 31, § 1º, I, como se percebe na sua redação: "Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem;".

Ainda assim o prefeito municipal recusou-se a fornecer os dados, que uma vez em poder dos vereadores, teriam a obrigação de zelar pelo sigilo das informações, podendo até mesmo ser responsabilizados em caso de possíveis vazamentos. No caso, os desembargadores da 5ª Câmara Cível do Tribunal de Justiça de Minas Gerais acordaram em negar provimento ao recurso apelatório, prejudicado o reexame necessário, em consonância com o voto da relatora. Vale a seguir uma exposição contextualizada dos fatos oriundos do juízo de piso, que motivaram os vereadores a ingressar com demanda judicial para ver assegurado o direito líquido e certo que entendiam lhes caber.

Os vereadores do município de Lagoa Santa-MG, no uso de suas atribuições fiscalizadoras, solicitaram informações ao Chefe do Executivo Municipal com o propósito de obter dados sobre a campanha nacional de imunização contra o corona vírus que assolou a população mundial em 2020. Desejavam eles que lhes fossem repassados os dados sem anonimização.

Alegaram os vereadores que o pedido encontrava respaldo tanto na Lei Orgânica do Município, como na lei nº 12.527/201, no artigo anteriormente mencionado. Acresceram que a postulação tinha o condão de cumprir obrigação legal, o que lhes disponibilizaria as informações completas, sem anonimização, também em conformidade com a LGPD, em seu art. 7º, II.

Depois de negada a postulação administrativa dos integrantes do Legislativo de Lagoa Santa, estes impetraram Mandado de Segurança para satisfação do direito assegurado em lei. O magistrado concedeu a ordem e determinou que fossem repassadas as informações nos seguintes termos: Se servidores públicos: nome completo, RG, CPF, função, cargo/lotação detalhada, lote da vacina e data da vacinação; População em geral: nome completo, CPF, categoria, grupo de atendimento, lote, nome da vacina,

data da vacina; A quantidade de vacinas disponibilizadas pelo Ministério da Saúde ao município de Lagoa Santa e o quantitativo de pessoas imunizadas com a 1ª e 2ª doses, incluindo dados referente a maio de 2021 até a data do cumprimento da ordem judicial.

Em suas razões, o apelante aduziu que cumpriu todas as determinações do magistrado de primeira instância e que não seria possível fornecer esse tipo de informações sem ordem judicial, uma vez que poderia ser responsabilizado solidariamente em caso de divulgação inadequada. Acresceu que o Conselho das Secretarias de Saúde de Minas Gerais defendeu a preservação dos dados sensíveis dos vacinados ao fundamento de que a Lei de Acesso à Informação não pode conflitar com a LGPD; pontuou ainda que o órgão controlador é o Ministério da Saúde, responsável por disponibilizar os dados pessoais das pessoas vacinadas, sendo os municípios apenas os operadores, por essa razão alegou que as solicitações deveriam ser encaminhadas ao Ministério da Saúde e não ao Município.

Por fim requereu a reforma da sentença, visto que apresentou justificativa plausível para a entrega incompleta dos dados em observância ao sigilo das informações pessoais, bem como informou que entregou as informações no dia seguinte ao tempo do prazo, demonstrado não ter criado óbice ao poder fiscalizador do legislativo da cidade de Lagoa Santa. Os apelados pugnaram pelo desprovimento do recurso, e o Ministério Público manifestou-se pela manutenção da sentença em reexame necessário.

Em seu voto a desembargadora da 5ª Câmara Cível se manifestou no sentido de admitir o reexame necessário e a apelação, uma vez presentes os requisitos de admissibilidade. Entendeu ela que o writ impetrado pelos vereadores- apelados – em sede de juízo superior fora o remédio constitucional adequado, uma vez que o Prefeito teria se recusado a fornecer a lista com dados completos das pessoas imunizadas em Lagoa Santa com a vacina da COVID-19, limitando-se a apresentar listagem anonimizada dos vacinados.

Concordou com a decisão do MM juízo *a quo* que concedeu a segurança, entendendo caracterizada omissão ilegal da autoridade coatora no seu dever de prestar informações, decidindo pela manutenção integral da sentença primeva.

A magistrada do 2º entendeu que o objeto da demanda não fora perdido, como alegou o apelante, posto que a omissão ilegal só foi suprida depois do deferimento da ordem judicial liminar. Teceu suas considerações e fundamentos no que toca em específico à controvérsia em verificar se a disponibilização da lista dos vacinados com

dados anonimizados seria suficiente para a função fiscalizadora da Câmara Municipal de Vereadores. Complementou seu questionamento neste ponto, valendo-se da LGPD em seu art. 5º, III quanto ao conceito de dados anonimizados: "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

Com o fito de solucionar a controvérsia suscitada, socorreu-se de um juízo de ponderação baseado nos critérios da razoabilidade e proporcionalidade, entre o direito fundamental de acesso à informação e à proteção de dados pessoais e à intimidade, tudo com fulcro na análise das leis bases para essa análise: LGPD (13.709/2018) e Lei de Acesso à Informação. (Lei 12.527/2011)

Numa primeira observação justificou os parâmetros trazidos pela Lei 12.527/2011, e os cotejou com a Lei 13.709/2018, formando um juízo de que elas não são conflitantes entre si, como faz alega o apelante. Ao revés, elas se complementam com vistas a uma aplicação harmônica dos direitos fundamentais à proteção de dados, à vida privada, bem como ao interesse público.

No voto em comento, a relatora endossou que assiste razão aos impetrantes -apelados- ao requererem a lista de pessoas vacinadas, visto que são legitimados e detém competência fiscalizadora quanto aos atos do Poder Executivo, conforme previsão da Lei Orgânica daquele município. E aduz que esse fato é relevante porque não se trata de um particular em busca de informações pessoais, tampouco um meio de comunicação em busca de divulgar dados sensíveis. Mas sim de vereadores com respaldo em decisão unânime da Casa Legislativa, com vista à fiscalização de políticas públicas de interesse coletivo, em meio a um cenário de pandemia.

Afirmou a magistrada que em virtude do momento de crise sanitária, a impetração do *mandamus* configurou notório interesse público da Câmara de Lagoa Santa em prol da correta imunização naquele município, justificando o acesso completo dos dados das pessoas vacinadas a fim de averiguar se todas faziam parte dos grupos prioritários.

Por fim, pontuou que a justificativa apresentada pelo chefe do executivo municipal à Câmara de Vereadores para a disponibilização de dados apenas anonimizados, não tinham relevância processual naquele momento, vez que as informações completas foram prestadas em sede de concessão de liminar no Mandado de Segurança. Negou assim provimento ao recurso, voto esse seguido pelos demais desembargadores.

Percebe-se da decisão proferida pelo juiz de primeira instância e depois confirmada no TJMG que o principal embate havido se deu em torno da medida ou proporção

que deveria ser feita a divulgação dos dados solicitados pelos vereadores da cidade de Lagoa Santa. De um lado havia a Câmara Legislativa daquele município exercendo seu poder fiscalizador assegurado em lei, agindo assim em nome da coletividade. De outra sorte havia nessa busca de dados um aspecto igualmente assegurado em lei: o direito à privacidade dos dados sensíveis relacionados ao tema da saúde.

Ao solicitar do prefeito a lista com os dados sem anonimização, os vereadores almejavam ter conhecimento de quem estava devidamente imunizado e como se dera a obediência aos critérios estabelecidos pelos atos normativos daquele contexto pandêmico. Por uma questão de respeito aos grupos prioritários, tais como idosos e pessoas que laboravam na área de saúde, a necessidade de fiscalização se fazia evidente, não apenas por este aspecto, mas também para evitar desperdício dos lotes de vacinas, e a segurança de toda a sociedade que carecia de imunizantes como forma de amenizar os efeitos da pandemia na saúde das pessoas, em geral.

Ao fornecer a lista, o prefeito o fez enviando os dados sem as informações detalhadas, e justificou a anonimização da lista em nome do respeito à privacidade dos dados pessoais sensíveis, que em princípio só poderiam ser fornecidos com o consentimento do titular dos respectivos dados. Tal garantia visa evitar problemas diversos possíveis de ocorrerem quando da divulgação dessa espécie de informação, que podem repercutir em discriminações ou mesmo ações impeditivas em detrimento de quem teve seus dados divulgados indevidamente.

Esse parece ter sido o ponto nodal da situação levada ao crivo do Poder Judiciário: a colisão de direitos fundamentais e qual deles deveria ter maior preponderância. A lei magna brasileira não faz uma hierarquização quanto a estes direitos, e assim não é possível responder de maneira precisa à questão em debate. Para solucionar o dilema, socorreu-se do Judiciário, que por sua vez, precisou se valer de uma ponderação de direitos.

Trata-se de sopesar o interesse público contra o interesse na proteção da privacidade informativa dos titulares dos dados. Os argumentos utilizados pela desembargadora basearam-se na ideia de que nenhum desses direitos fosse sacrificado além da medida de proteção do outro.

Direitos relacionados à informação pública e à proteção de dados, geralmente, revelam uma tensão entre si, vez que não tem uma solução pré-definida, exigindo um julgamento e ponderação nos casos concretos em que ocorre. De um lado, o acesso à informação é essencial para garantir vários aspectos importantes na Administração

Pública, como é o caso da transparência, além de também proporcionar mecanismos de controle e fiscalização, como se deu no caso em tela.

Em outro viés, grande parte dos documentos e informações solicitadas para o exercício desse direito contém dados pessoais cuja proteção também é considerada um direito fundamental. Manter uma conciliação entre estes direitos não se revela em tarefa simples, especialmente quando se passa a considerar as implicações que podem decorrer de forma direta ou indireta para os titulares dos dados em questão.

6.5.1 Inferências acerca das decisões judiciais coletadas

Ao longo desta pesquisa, foram levantados diversos questionamentos quanto aos impactos da exposição da informação de saúde na vida prática do cidadão. A princípio, a combinação entre informação e tecnologias representa uma grande evolução que beneficia milhares de usuários dos sistemas público e privado de saúde. No entanto, há a necessidade de reflexão quanto as possíveis consequências da utilização indevida de dados sensíveis de saúde. Neste ponto, há indicação de riscos que não apenas permanecem à margem do exame pela via judiciária, como chegam a ser desconhecidos de forma geral, o que revela que Estado e sociedade, ainda se encontram no início de uma longa jornada para a compreensão real da dimensão dos efeitos da informação na esfera de saúde.

Em cada um dos julgados analisados, foi dedicado um esforço especial para enfatizar e apresentar os principais argumentos debatidos durante os processos judiciais, bem como os fundamentos que nortearam as decisões. Foram identificados desta forma, pontos críticos e as nuances jurídicas próprias das decisões sobre responsabilidade civil em casos de vazamento de dados sensíveis de saúde, que demandam um olhar mais cuidadoso.

O primeiro ponto de atenção a ser mencionado, reside na compreensão do conceito de dados sensíveis de saúde. Enquanto a LGPD apresenta a noção de dados sensíveis, a aplicação do conceito na esfera da saúde resulta em uma hipersensibilidade. Conforme verificado nos casos expostos, as informações pessoais de saúde são constituídas por uma gama de informações íntimas que revelam grandes vulnerabilidades do indivíduo e muitas vezes ultrapassam a sua figura individual, atingindo e vitimizando membros do grupo familiar.

A família base da sociedade e protegida constitucionalmente[530], representa uma unidade composta por indivíduos que compartilham conexões biológicas e socioafetivas dentro de sua linha de vida. É, portanto, uma configuração de dependência, partilha e solidariedade emocional, psicológica, social e financeira, que pode ser largamente afetada em virtude da exposição não autorizada de informações delicadas de saúde.

Em casos de doenças estigmatizadas socialmente, o vazamento de dados sensíveis de saúde pode gerar isolamento social, preconceito e discriminação, afetando não apenas o indivíduo diretamente envolvido, mas também outras pessoas de seu grupo familiar. Ademais, o constrangimento e o medo da exposição levam muitas vezes a desgastantes tentativas de ocultar a situação, o que pode comprometer ainda mais a saúde e bem-estar do paciente, bem como aqueles que o cercam.

Para finalizar este ponto é válido refletir ainda quanto ao impacto do vazamento de dados sensíveis de saúde em termos de segurança financeira da família. Conforme se aduz dos casos analisados, práticas de fraudes, golpes ou roubo de identidade podem ser consequências diretas do acesso não autorizado a essas informações eficazes, causando danos materiais que podem afetar o futuro do grupo familiar.

A discussão quanto ao sistema de responsabilidade a ser adotado nos casos de vazamento de dados de saúde é outra questão a ser destacada. Em que pese as argumentações a favor da aplicação da responsabilidade objetiva e subjetiva, o que se verificou nas decisões foi uma incerteza quanto ao melhor sistema e até mesmo uma junção de conceitos apoiada especialmente pela norma consumerista. Todavia, não se pode olvidar que na buscar por evitar o desequilíbrio social e a violação dos princípios da igualdade, liberdade e privacidade por meio da exposição indevida de dados sensíveis de saúde, um sistema híbrido proativo sem o devido assentamento normativo possivelmente não refletirá em uma tutela rigorosa para a questão dos dados sensíveis.

Neste sentido, desponta a responsabilidade civil objetiva como ferramenta mais viável para responder os conflitos sobre o tema. De acordo com as situações elencadas, está clara que a imposição legal de reparar danos atribuída aos agentes de tratamento dos dados de saúde deve prescindir o elemento culpa para que seja possível estabelecer uma reparação digna à vítima. Como já discutido, não há dúvidas quanto a configuração do risco na atividade desenvolvida pelo agente de tratamento, e nem sobre a possibilidade da violação de direitos fundamentais. Tal situação se agrava pelo

530 A Constituição Federal de 1988 dispõe em seu artigo nº 226: a família, base da sociedade, tem especial proteção do Estado. BRASIL, op. cit., 1988.

potencial lesivo dos dados de saúde e a dificuldade de prever as repercussões de um vazamento. Além disso, não se figura razoável adotar regras distintas para agentes de tratamento de dados públicos e privados.

Cada um dos julgados selecionados abordou diferentes desdobramentos da situação de exposição não autorizada de dados de saúde e contribuiu para a formação de um panorama que permite antever o raciocínio adotado pelas cortes estaduais por meio da diversidade de argumentos e fundamentos jurídicos apresentados sobre a matéria. Interessante constar que, ao serem aproximadas, as decisões convergiram para o reconhecimento do dever de indenizar face a configuração dano moral em seu viés mais tradicional. Mas ao enfrentar a problemática da indicação do *quantum* indenizatório não chegaram a precisar de forma clara os critérios utilizados.

Em reforço ao que se expôs previamente quanto a este tema, é importante refletir sobre a proporcionalidade e razoabilidade frente a condição econômica das instituições responsáveis pelo tratamento de dados de saúde, equacionada com a extensão da lesão e sua repercussão. Nos casos apresentados, as decisões em termos de valoração parecem não ter atingido o caráter pedagógico-punitivo que se espera de uma indenização.

Por fim, cabe registro a possibilidade da colisão entre o interesse público e as normas de proteção da privacidade informativa dos titulares dos dados de saúde, questão que depende delicada ponderação de direitos via Poder Judiciário, conforme exemplificado pelo terceiro julgado analisado. Acertadamente a decisão estudada demonstrou que embora não exista uma solução pré-definida, é preciso se pautar pela ideia de que nenhum desses direitos deve ser sacrificado além da medida necessária a proteção do outro. Mas encontrar este limite e especialmente assegurar a sua observação na prática constitui certamente um grande desafio.

É preciso lembrar que no cenário da saúde brasileira, muitas instituições ainda se encontram distantes das orientações dispostas na LGPD. Em fato, os planos de adequação têm se materializado de forma lenta, padecendo frente a dificuldades de recursos humanos e financeiros, o que facilita os ataques e invasões aos bandos de dados do setor. De outro lado, as fiscalizações e aplicações de sanções embora em pleno vigor, por diversas questões operacionais, práticas e jurídicas também não são aplicadas como esperado. Assim, a fragilidade da segurança do setor somada a qualidade das informações armazenadas justifica não apenas a preocupação, como uma atuação mais eficaz das autoridades competentes frente a necessidade de preservação dos dados sensíveis de saúde.

Sem pretensão de esgotar o tema, mas sim de realizar um primeiro movimento na compreensão mais aprofundada da temática complexa dos dados de saúde, que tem emergido nas cortes brasileiras nos últimos anos como um reflexo do recente cenário pandêmico e do aumento no interesse da comercialização de dados de saúde, a leitura dos julgados selecionados buscou contribuir com considerações e argumentos relevantes para a questão da privacidade dos usuários dos sistemas de saúde no Brasil. Dada a natureza dinâmica do direito, é fundamental acompanhar a evolução do posicionamento dos tribunais e aprimorar conhecimentos em torno das questões relacionadas à responsabilidade civil e proteção de dados sensíveis de saúde.

7 Conclusão

Ao propor uma reflexão quanto a proteção à saúde, no contexto de sua dimensão informativa, a partir do cenário desenhado pela LGPD, esta pesquisa buscou contribuir indicando questões e desdobramentos quanto a matéria. Estes, embora pouco explorados, sob o ponto de vista técnico-jurídico, tem sido materializados na vida prática do cidadão mediante o rápido avanço dos sistemas e atendimentos mediados por tecnologia no setor de saúde brasileiro.

Com a ideia de apresentar o panorama da construção e implementação da visão da saúde digital no Brasil, confrontando a base técnico-jurídica, constituída especialmente pelo arcabouço constitucional, LGPD e políticas públicas específicas, o texto procurou destacar os elementos da realidade de instituições públicas e privadas de saúde. Também destacou os principais desafios do processo de adequação às normas de segurança de dados, previstas em lei, para assegurar a proteção da privacidade dos dados sensíveis de saúde dos usuários do sistema.

A proteção de dados sensíveis prevista na LGPD no setor de saúde, requer a implementação dos processos de segurança em diferentes momentos do ciclo de atendimento e tratamento do paciente usuário dos sistemas de saúde. Há que se pensar em uma adequação global de todos os agentes envolvidos, sejam estes da rede pública ou privada, ao *compliance* exigido pela norma. Porém, múltiplos obstáculos como a ausência de protocolos claros e seguros para o compartilhamento de dados, de criptografia, a falta de treinamento dos profissionais de saúde em segurança cibernética e ausência de atualizações de softwares, acabam por prejudicar a efetivação da segurança pretendida e abrem margem para situações, cada vez mais frequentes, de vazamento de dados.

Embora a chegada da LGPD venha ao encontro da necessidade de um resguardo mais efetivo dos direitos fundamentais de liberdade, privacidade e autonomia informativa, apresentando um delineamento mais nítido no que tange à tutela da privacidade, bem como dos direitos da personalidade, foram verificadas a presença de lacunas que inviabilizam a garantia das proteções originalmente prometidas e necessárias para assegurar a privacidade e à dignidade da pessoa que se utiliza dos sistemas de saúde brasileiros.

Restou claro que o conteúdo dos dados de saúde contém peculiaridades muito específicas que os tornam alvo preferenciais de ataques e práticas ilícitas de

compartilhamento de informação para os mais diversos fins. Tal conteúdo, marcado por uma hipersensibilidade possui um alto poder de impacto tanto em via positiva, quanto negativa para o cidadão que hábusca o auxílio do setor de saúde. Se em uma via, se verifica uma aceleração de atendimentos e processos, maior precisão de diagnósticos e importantes colaborações para pesquisas na área de saúde; de outro lado, o cidadão se encontra exposto a riscos de ter seu direito à privacidade violado, frente à exposição indevida de informações de sua esfera mais íntima.

Para a análise do paradoxo constituído mediante o rigor das normas e políticas propostas para a proteção ao direito à privacidade, bem como para o tratamento de dados pessoais sensíveis de saúde, inicialmente foram apresentadas considerações sobre a aproximação das esferas público e privadas, ampliada pela influência das tecnologias. Tudo frente os recorrentes casos de divulgação, comercialização e vazamento destas informações. Ao se discutir sobre direitos como liberdade, privacidade e informação, restou clara a dificuldade de se vislumbrar um limite entre o que seria a privacidade individual e o interesse coletivo.

Neste sentido, a LGPD trouxe grande contribuição ao dispor sobre o conceito de dados pessoais e de dados pessoais sensíveis, indicando, precisamente, a necessidade do consentimento do titular para a realização das práticas de tratamento, bem como ao elencar as hipóteses legais nas quais este poderá ser dispensado. Por seu caráter generalista, a lei não apresenta maiores detalhes quanto aos dados especificamente relacionados à saúde, embora os tenha classificado como sensíveis e indicado a possibilidade de práticas de anonimização em diversas situações com o objetivo de resguardar a privacidade dos titulares.

Apontada como uma expressiva ferramenta de segurança, a prática de anonimização de dados é, na verdade, um caminho irreversível. Conforme a utilização de determinados sistemas e algoritmos é possível ordenar dados e acessar informações extremamente privadas do indivíduo, em um procedimento perigoso para o titular, porém igualmente lucrativo para dadas instituições. Logo, é preciso considerar até que ponto as medidas de segurança utilizadas, fazem frente aos recursos de leitura e organização de *big data* disponíveis. Há diversos riscos em propagar uma ideia de proteção que não pode ser efetivada na via prática.

Embora a LGPD apresente previsão expressa quanto ao direito que assiste ao titular de dados pessoais de ter conhecimento sobre as empresas privadas ou públicas com as quais o controlador de dados pessoais compartilhou os dados, foi constado através da

análise de diversos relatórios, notícias e demandas judiciais que a realidade dos dados de saúde tem sido conduzida de outra forma.

A indicação de que o compartilhamento de dados pessoais poderá ser regulamentado de forma específica pela ANPD, também resulta em outra fragilidade, vez que permite o surgimento de novas regulamentações as quais podem priorizar interesses distintos daqueles originalmente indicados na LGPD.

Conforme exposto, na realidade capitalista, os dados representam insumos de alto valor, que se convertem em instrumentos de poder para empresas e governos, mundo afora. Diante da ausência da materialização esperada das proteções previstas tanto na LGPD, como nas Estratégias de Saúde Digital para o Brasil e demais políticas públicas do setor, a segurança quanto as práticas de coleta, tratamento e armazenamento, dos dados de saúde se tornou, justificadamente, questionável.

Longe de disseminar um discurso de restrições quanto a utilização das tecnologias e as práticas de tratamento de dados de saúde, o que se pretendeu foi enfatizar a necessidade da busca por um equilíbrio entre os direitos individuais assegurados constitucionalmente, em especial o direito à privacidade e o tratamento das informações de saúde. Nesse sentido, uma medida importante é a assegurar a clareza quanto a finalidade dos dados coletados nos processos de saúde e a partir da motivação e direcionamento, a adoção medidas básicas de segurança dos sistemas, o que demanda investimentos consideráveis em recursos materiais e humanos.

Ademais, as proteções pretendidas para a saúde exigem uma urgente mudança de cultura no setor. No momento atual, não há como dissociar a saúde da informática, do *compliance* da LGPD e dos princípios e metas contidos nas Estratégias de Saúde Digital. Trata-se de uma interdisciplinaridade necessária para organização, segurança e operação do setor. Apesar disso, instituições públicas e privadas enfrentam dificuldades para se adequar a nova realidade, em muitos casos relutando em realizar as adequações necessárias.

A nova cultura da saúde digital no Brasil atinge igualmente profissionais da área e os cidadãos usuários dos sistemas. Resta a melhoria da compreensão dos dois grupos quanto aos procedimentos aptos a resguardar as informações pessoais dos titulares de dados, bem como no que se refere às possibilidades de prejuízos causados por uma exposição indevida de dados de saúde. Sem desconsiderar a importância do sigilo na relação forjada entre o profissional de saúde e o paciente, é urgente compreender os caminhos e acessos associados aos dados de saúde. Por este motivo, os conceitos

e procedimentos tradicionais explicados aos pacientes devem ser acrescidos da preocupação com o manuseio de dados.

É crucial trabalhar a questão do consentimento informacional em conformidade com a orientação da LGPD, o que depende especialmente do empenho de instituições e profissionais em se adequar aos padrões e criar protocolos eficientes. Em que pese a norma indicar definições de funções e meios para a elaboração de regras de controle das informações, no processo de tratamento de dados de saúde, ainda existem riscos que precisam ser considerados e que tem sido objeto de discussão pelo Estado brasileiro há mais de uma década.

A leitura dos principais documentos que tratam da questão da privacidade na esfera da saúde digital brasileira, permitiu a constatação dos esforços para implementar uma visão de saúde pautada na integração de informações, sejam estas oriundas de entidades públicas ou privadas, trabalhadas a partir de um arcabouço organizacional, legal, regulatório e de governança, que possibilite o desenvolvimento adequado de serviços e procedimentos da área.

Contudo, o aporte teórico apresentado não parece ter priorizado o aprofundamento das questões sobre privacidade em saúde, apresentando de forma superficial importantes temas associados a matéria, com por exemplo, a problemática dos sistemas permeáveis, que se utilizam de ferramentas de segurança menos efetivas e equipes despreparadas para identificar ameaças.

As políticas públicas e documentos direcionados a implementação da visão de saúde digital para o Brasil foram estruturados de modo a alcançar processos e práticas institucionalizadas, e dedicaram grande atenção a proposta de construção de um sistema integrado de informações de saúde. Tais políticas e documentos silenciaram sobre importantes desdobramentos, tais como orientações para evitar controle em massa dos cidadãos, reprodução falhas históricas que podem resultar em discriminações, além da delimitação clara das responsabilidades dos agentes de tratamentos de dados sensíveis de saúde.

Desta forma, os caminhos em busca de uma efetiva proteção de dados pessoais, na seara de saúde, demandam antes de tudo um trabalho de conscientização. É preciso compreender o que são e do que tratam esses dados e as regras para seu manuseio. Exemplos de boas práticas a partir da gestão, cursos, capacitações e outras ações que promovam conhecimento acerca do direito à privacidade e das normas de proteção de dados são essenciais para operadores, gestores e comunidade, configurando a base

sobre a qual deve se assentar essa nova cultura na qual saúde e tecnologia se apresentam de forma unificada.

Também é tempo de observar os impactos da falta de segurança dos bancos de dados de saúde, considerando a amplitude dos desdobramentos de eventuais situações de vazamento, como a ampliação dos alvos de discriminação. Restou evidenciada a possibilidade de que informações obtidas através dos bancos de dados de saúde venha a ser utilizada de forma seletiva, destacando aspectos negativos de um indivíduo ou grupo, capaz de gerar tratamento injusto, ou ainda servirem como base para crimes e ações de ódio. Á frente do combate as discriminações, é preciso considerar a abertura criada para a discriminação algorítmica, estatística e genética, práticas indesejáveis que refletem preconceitos enraizados na sociedade, e afetam principalmente grupos frágeis ou minoritários.

A discriminação oriunda dos dados de saúde pode ocorrer dentro e fora da esfera de cuidados e ocasionar mais do que prejuízos materiais. A mera ameaça de ter informações de foro íntimo, expostas na internet, podem ocasionar lesões permanentes na esfera psicológica da vítima de vazamento de dados, além de perpetuar um ciclo de vulnerabilidade e violação de privacidade, situação que dificilmente poderá ser mensurada.

A esta altura, retomando o questionamento inicial da pesquisa, ficam clara as lacunas nas normativas de proteção de dados sensíveis aplicados a saúde e o consequente comprometimento do direito à privacidade e à dignidade do usuário dos sistemas de saúde no Brasil. Em que pese os avanços realizados com a ESD28 e a LGPD, entre outros documentos normativos, a segurança informativa prometida ainda se encontra distante do cidadão.

Para além das vulnerabilidades mencionadas, ao analisar o impacto direto de um vazamento de dados de saúde para seu titular, foi possível verificar que a ausência da definição de um sistema de responsabilidade adequado prejudica o exercício do dever de reparação por parte dos responsáveis pela exposição indevida de dados sensíveis de saúde. Outra questão grave é a dimensão do dano ocasionado por este tipo de vazamento que, por sua natureza etérea e alto potencial lesivo, apresenta a possibilidade de reverberar no tempo e atingir outros indivíduos que tenha proximidade com o titular.

A visão do posicionamento das cortes brasileiras quanto a matéria, revelou os desafios enfrentados pelo Poder Judiciário, no momento de materializar as proteções

e indicar caminhos de reparação, para quem se viu lesado pela divulgação ilícita de dados de saúde. Embora haja clareza quanto a configuração do risco na atividade de tratamento de dados de saúde e sobre seu potencial de violar diretos fundamentais, pouco se fala sobre a dificuldade de prever as repercussões de um vazamento ou sobre a delicada questão do *quantum* indenizatório.

Por hora, se percebe a escolha do que aparenta ser o caminho mais seguro, com adoção da interpretação mais ampla e tradicional da responsabilidade civil, em um movimento que caso persista, pode representar o comprometimento da força da proteção jurídica ofertada aos titulares de dados no Brasil. Antevendo o risco intrínseco a toda ação de tratamento de dados, mediante a verificação de um considerável potencial danoso em caso de falha no tratamento ou vazamento de informações, é preciso buscar respostas claras e coerentes para o cidadão que age em confiança ao sistema de saúde.

Nos termos da LGPD, o agente de tratamento de dados, seja ente público ou privado, possui a obrigação de responder pelo dano causado decorrente de vazamento de dados. Ao se considerar a imposição da responsabilidade objetiva na seara pública, seria inadequado impor uma diferenciação do sistema de responsabilidade aplicado a um mesmo fato, gerando tratamento diferenciado conforme o agente envolvido e consequente insegurança jurídica.

Vazamentos não intencionais ou invasão de sistemas e bases de dados por terceiros não autorizados configuram incidentes de segurança que resultam na obrigação de indenizar os danos causados aos titulares de dados, sem que eles necessitem comprovar a conduta culposa por parte do controlador ou operador em virtude do potencial risco da atividade. Logo, a adoção da responsabilidade civil objetiva se afigura como mais adequada para prover a reparação de danos gerados pela exposição indevida de dados sensíveis de saúde.

Conforme visto do recente posicionamento do STJ, o vazamento de dados pessoais, não tem o condão, por si só, de gerar dano moral indenizável, não admitindo presunção, porém é válido refletir sobre a obrigação da comprovação de danos potenciais. O dano ocasionado por um vazamento de dados sensíveis, especialmente de saúde, não necessariamente será identificado de forma completa e a um só tempo. Não seria equivocado pensar que dados divulgados sem o devido consentimento do titular e expostos em meios digitais ficariam disponíveis por tempo indeterminado, podendo causar diferentes prejuízos em momentos distintos da vida do indivíduo e de seu grupo familiar.

Além disso, o baixo valor atribuído pelos tribunais a título de indenização em virtude do vazamento de dados de saúde não se afigura ato a cumprir o papel punitivo e educativo quando se considera o poder econômico das instituições responsáveis pelo tratamento de dados de saúde. A valoração das indenizações, tal como exemplificado pelos julgados apresentados, embora reconheça o dano moral, não se aproximam de critérios como dor psicológica, potencial discriminatório e repercussão para terceiros.

A questão dos dados ainda é considerada recente na sociedade brasileira, fato que a princípio, pode justificar a ausência de uma visão mais completa quanto a matéria e seus desdobramentos. Todavia, diariamente novos casos são lançados ao Poder Judiciário, demandando respostas no sentido de estabelecer uma tutela de preservação para os dados sensíveis, em especial aqueles aplicáveis à saúde. A análise de tais casos, deve partir de uma visão prática e interdisciplinar, na qual para além dos diplomas legais e documentos públicos, se considere temáticas correlatas, aptas a aclarar características e consequências oriundas do tratamento indevido dos dados de saúde.

Resta ainda, ao Estado como um todo, promover uma verdadeira conscientização quanto as práticas associadas as informações em saúde, a fim de que estas sejam regidas pela ética no contexto da privacidade e da confidencialidade. Todos os esforços devem ser empregados para que sejam preservados direitos fundamentais, tais como a dignidade, liberdade, informação e privacidade. A um só tempo se evita os efeitos comprometedores da exposição indevida de informações frente a necessidade de quem entrega seus dados em busca da possibilidade de restaurar o bem da saúde.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

ACETO, G.; PERSICO, V.; PESCAPÉ, A. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. Journal of Network and Computer Applications, [*S.l.*], v. 107, p. 125-154, 2018. Disponível em: https://doi.org/10.1016/j.jnca.2018.02.008. Acesso em: 18 fev. 2023.

ALBUQUERQUE, B. Brasil contabiliza 2,5 milhões de teleconsultas nos últimos 12 meses. Blog Abramge, São Paulo, 2021. Disponível em: https://blog.abramge.com.br/saude-suplementar/brasil-contabiliza-25-milhoes-de-teleconsultas-nos-ultimos-12-meses/. Acesso em: 12 jul. 2023.

ALEXY, R. Teoria dos Direitos Fundamentais. 2. ed. Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros, 2017.

ALMEIDA, B. A. *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. (2020). Ciência & Saúde Coletiva, Rio de Janeiro, v. 25, p. 2487–2492, 2020. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em: 9 jul. 2020.

AMARAL, A. C. C. Z. M. Responsabilidade civil pela perda da chance: natureza jurídica e quantificação do dano. Curitiba: Juruá, 2015.

ANDRADE, M. C. Direito Penal Médico, SIDA: testes arbitrários confidencialidade e segredo. Coimbra: Coimbra Editora, 2008.

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 20 jul. 2022.

ANS - AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. ANS registra recorde de consumidores em planos de assistência médica. ANS: Ministério da Saúde, 2023. Disponível em: https://www.gov.br/ans/pt-br/assuntos/noticias/numeros-do-setor/ans-registra-recorde-de-consumidores-em-planos-de-assistencia-medica. Acesso em: 11 jul. 2022.

ANVISA – AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. Página Inicial. Brasília, Ministério da Saúde, 2022. Disponível em: https://www.gov.br/anvisa/pt-br. Acesso em: 22 jul. 2022.

APURA CYBER INTELLIGENCE. Relatório anual de Segurança Cibernética Apura Cybersecurity S/A, 2021 O ano em resumo. São Paulo: Apura, 2021. Disponível em: https://www.linkedin.com/posts/apura_relat%C3%B3rio-anual-de-seguran%C3%A7a-cibern%C3%A9tica-activity-6885285395324571648-4v74/. Acesso em: 15 jun. 2023.

ARNER, D. W.; BARBERIS, J.; BUCKLEY, R. P. The evolution of Fintech: a new post-crisis paradigm. Georgetown Journal of International Law, [*S.l.*], v. 47, p. 1271, 2015. Disponível em: https://www.researchgate.net/publication/313365410_The_Evolution_of_Fintech_A_New_Post-Crisis_Paradigm. Acesso em: 22 jul. 2022.

ASSESPRO. Segurança da Informação e adequação à LGPD são para poucos na saúde no Brasil. Nic.br, 2021. Disponível em: https://www.nic.br/noticia/na-midia/seguranca-da-informacao-e-adequacao-a-lgpd-sao-para-poucos-na-saude-no-brasil. Acesso em: 7 abr. 2022.

AZEVEDO, A. J. Por uma nova categoria de dano na responsabilidade civil: o dano social. *In*: FILOMENO, J.G. B.; WAGNER JÚNIOR, L. G. C.; GONÇALVES, R. A. (coord.). O Código Civil e sua interdisciplinaridade. Belo Horizonte: Del Rey, 2004.

AZEVEDO, A. V.; LIGIERA, W. R. Direitos do paciente. 1. ed. São Paulo: Saraiva: 2012.

BACKES, D. A. P.; *et al*. Os efeitos da pandemia de COVID-19 sobre as organizações: um olhar para o futuro. Iberoamerican Journal of Strategic Management (IJSM), [*S.l.*], v. 19, n. 5, p. 1-10, 2020. Editorial. Disponível em:https://doi.org/10.5585/riae.v19i4.18987. Acesso em: 15 jun. 2023.

BARBOSA, L. M. M.; MACHADO, C. B. Glossário de Epidemiologia e Saúde. *In*: ROUQUAYROL, M. Z.; GURGEL, M. (eds.). Rouquayrol: Epidemiologia & Saúde. 7. ed. Rio de Janeiro: MedBook. 2013.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BARDIN, L. Análise de conteúdo. Tradução: Luís Antero Reto; Augusto Pinheiro. 1. ed. São Paulo: Edições 70, 2016.

BARROSO, L. R. A dignidade da pessoa humana no direito constitucional contemporâneo: a construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016.

BARROSO, L. R.; OSORIO, A. "Sabe com quem está falando?": Notas sobre o princípio da igualdade no Brasil contemporâneo. Revista Direito e Práxis, Rio de Janeiro, v. 7, n. 13, p. 204-232, 2016. Disponível em: https://www.redalyc.org/pdf/3509/350944882008.pdf. Acesso em: 7 abr. 2022.

BEAUCHAMP, T. L.; CHILDRESS, J. F. Princípios de Ética Biomédica. São Paulo: Loyola, 2002, p. 282.

BECKETT, A. The dark side of the internet: in the deep web, Freenet software allows users complete anonymity as they share viruses, criminal contacts and child pornography. The Gardian, London, 2009. Disponível em: http://www. guardian.co.uk/technology/2009/nov/26/dark-side-internetfreenet. Acesso em: 23 abr. 2023.

BEIER, M.; IANNOTTI, G. C. Algumas considerações sobre o Paternalismo Hipocrático. Revista Médica de Minas Gerais, Belo Horizonte, v. 20, n. 2, 2010. Disponível em: http://rmmg.org/artigo/detalhes/320. Acesso em: 1 abr. 2022.

BELCIC, I. Avast Academy: Segurança. Publ. 5 de fevereiro de 2020. Disponível em: https://www.avast.com/pt-br/cphishing#:~:text=Phishing%20nos%20sites%3A%20Os%20sites,login%20nas%20suas%20contas%20reais. Acesso em 15 jun. 2021.

BENNETT, C. Regulating Privacy: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992.

BESSA, L. R. Código de Defesa do Consumidor Comentado. 2. ed. rev., atual. e ampl. Rio de janeiro: Forense, 2022.

BESSA, L. R. O consumidor e os limites dos bancos de dados de proteção ao crédito. São Paulo: Revista dos Tribunais: 2003.

BIONI, B. Proteção de Dados Pessoais: o que você sabe sobre o assunto?. GEN Jurídico, 2018. Disponível em: https://blog.grupogen.com.br/juridico/areas-de-interesse/civil/bruno-bioni/. Acesso em: 24 mar. 2023.

BIONI, B. R. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos–Direito digital e proteção de dados pessoais, São Paulo, ano 21, n. 53, 2020b. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimiza%C3%A7%C3%A3o_e_dado.pdf. Acesso em: 12 jul. 2023.

BIONI, B. R. Proteção de Dados Pessoais - a função e os limites do consentimento. São Paulo: Editora Forense, 2020a.

BIONI, B. R. Proteção de Dados Pessoais: a função e os limites do consentimento. São Paulo: Forense, 2018.

BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com, Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Acesso em: 24 mar. 2023.

BORGES, R. C. B. Disponibilidade dos direitos de personalidade e autonomia privada. São Paulo: Saraiva, 2005.

BRASIL, Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência

da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 12 setembro 2022.

BRASIL, Plano Nacional de Saúde – PNS: 2016-2019. Brasília: Ministério da Saúde (MS), 2016.

BRASIL. A experiência brasileira em sistemas de informação em saúde. v. 2. Brasília: Editora do Ministério da Saúde, 2009.

BRASIL. Conselho Nacional de Justiça. Justiça em números. CNJ, Brasília, 2021. Disponível em: https://www.cnj.jus.br/programas-e-acoes/pj-justica-em-numeros/. Acesso em 20 de mai. 2023.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Emendas Constitucionais. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 06 out. 2020.

BRASIL. Decreto n. 10.212, de 30 de janeiro de 2020. Promulga o texto revisado do Regulamento Sanitário Internacional, acordado na 58ª Assembleia Geral da Organização Mundial de Saúde, em 23 de maio de 2005. Brasília: Presidência da República, 2020.

BRASIL. Decreto-Lei n. 3.689, de 3 de outubro de 1941. Código do processo penal. Rio de Janeiro: Presidência da República, 1941.

BRASIL. Emenda Constitucional nº 115/2022, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 30 ago. 2022.

BRASIL. Estratégia de Saúde Digital para o Brasil 2017. Brasília: Ministério da Saúde, 2017.

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

BRASIL. Guia de boas práticas Lei geral de Proteção de Dados (LGPD). Brasil: Governo, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 11 ago. 2022.

BRASIL. Lei n. 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, 9 jan. 1991. Disponível em: http://www.unesco.org/culture/natlaws/media/pdf/bresil/brazil_lei_8159_08_01_1991 _por_orof.pdf. Acesso

em: 21jun. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. 2002. Brasília: Presidência da República, Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 5 mar. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília – DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 set. 2022.

BRASIL. Lei nº 13.787 de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 14 fev. 2023.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 12 jul. 2022.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diário Oficial da União, Brasília, n. 1, 2021. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=14155&ano=2021&ato=3a4cXUU5UMZpWT48d. Acesso em: 12 jul. 2022.

BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nº s 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Diário Oficial da União, nº 3. Brasília: Presidência da República, 2022.

BRASIL. Lei nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 30 maio 2022.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência

da República, 1990a. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 9 mar. 2023.

BRASIL. Lei ordinária no 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal. Diário Oficial da União 2011; 18 nov. Brasília: Presidência da República, 2011.

BRASIL. Lei ordinária nº 8.080, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Diário Oficial da União, Brasília: Presidência da República, 1990b. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 5 mar. 2023.

BRASIL. **Mercado Brasileiro de Software**: panorama e tendências, 2020. 1.. ed. São Paulo: ABES - Associação Brasileira das Empresas de Software, 2020.

BRASIL. Ministério da Saúde. Relatório Final do Projeto Piloto Conecte SUS: análise dos avanços obtidos entre outubro/2019 e junho/2020. Brasília: Ministério da Saúde, 2020. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_projeto_piloto_conectesus_outubro.pdf. Acesso em: 30 maio 2022.

BRASIL. **O Comitê Gestor de Saúde Digital – CGSD**. Brasília: Ministério da Saúde, 2023. Disponível em: https://www.gov.br/saude/pt-br/composicao/seidigi/saude-digital/Comite-Gestor-de-Saude-Digital/Comite-Gestor-de-Saude-Digital. Acesso em: 3 jul. 2023.

BRASIL. O que é Prontuário Eletrônico do Cidadão? Ministério da saúde, Brasília, 2017. Disponível em: https://aps.saude.gov.br/noticia/2300. Acesso em: 12 jan. 2023.

BRASIL. Plano Diretor de Tecnologia da Informação e Comunicação – 2022/2024. Brasília – DF: Ministério da Saúde. 2022. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2022/06/PDTIC-2022a2024-25mai2022-Final-revisado2.pdf. Acesso em: 30 maio 2022.

BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2016. 56 p. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/plano_nacional_saude_2016_2019_30032015_final.pdf. Acesso em: 30 maio 2022.

BRASIL. Portaria GM/MS nº 1.768/2021, de 30 de julho de 2021. Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). Brasília: Ministério da Saúde, 2021. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2021/prt1768_02_08_2021.html. Acesso em: 12 jan. 2023.

BRASIL. Portaria GM/MS nº 3.632/2020, de 21 de dezembro de 2020. Altera a Portaria de Consolidação GM/MS nº 1, de 28 de setembro de 2017, para instituir a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28). Brasília: Ministério da

saúde, 2020a. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2020/prt3632_22_12_2020.html. Acesso em: 14 jul. 2023.

BRASIL. Portaria n. 1.139, de 10 de junho de 2013. Define, no âmbito do Sistema único de Saúde (SUS), as responsabilidades das esferas de gestão e estabelece as Diretrizes Nacionais para Planejamento, Execução e Avaliação das Ações de Vigilância e Assistência à Saúde em Eventos de Massa. Brasília: Ministério da Saúde, 2013. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2013/prt1139_10_06_2013.html. Acesso em: 24 mai. 2022.

BRASIL. Portaria n. 589/15, de 20 de maio de 2015. Institui a Política Nacional de Informação e Informática em Saúde (PNIIS). Diário Oficial da União (DOU), de 22 de maio de 2015. Brasília: Ministério da Saúde. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2015/prt0589_20_05_2015.html. Acesso em: 14 fev. 2023.

BRASIL. Portaria nº 1.434, de 28 de maio de 2020. Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. Diário Oficial da União, Publicado em: 29/05/2020, ed. 102, seção: 1, p. 231, Brasília: Ministério da Saúde/Gabinete do Ministro, 2020.

BRASIL. Portaria nº 2.510, de 19 de dezembro de 2005. Institui Comissão para Elaboração da Política de Gestão Tecnológica no âmbito do Sistema Único de Saúde - CPGT. Brasília: Ministério da Saúde.

BRASIL. Portaria nº 492/2020, de 23 de março de 2020. Institui a Ação Estratégica "O Brasil Conta Comigo", voltada aos alunos dos cursos da área de saúde, para o enfrentamento à pandemia do coronavírus (COVID-19). Diário Oficial da União, ed. 56-c, seção 1, p. 4, Brasília: Ministério da Saúde, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-492-de-23-de-marco-de-2020-249317442. Acesso em: 14 fev. 2023.

BRASIL. Projeto de Lei do Senado n° 330, de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Brasília: Senado, 2013. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947. Acesso em: 24 mar. 2023.

BRASIL. Projeto de Lei nº 4.060 de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 24 mar. 2023.

BRASIL. Projeto de Lei nº 5.276, de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília, DF: Câmara dos Deputados, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0q1d5lxsv6vat1f4w8rhsnjs9u9626721.node0?codteor=1457459&filename=PL+5276/2016. Acesso em: 24 mar. 2023.

BRASIL. **Relatório Final do Projeto Piloto Conecte SUS**: análise dos avanços obtidos entre outubro/2019 e junho/2020. Brasília: Ministério da Saúde, 2020a.

BRASIL. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília: Presidência da República, 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 27 jul. 2022.

BRASIL. Resolução CFM nº 2.271/2020, de 14 de fevereiro de 2020. Define as unidades de terapia intensiva e unidades de cuidado intermediário conforme sua complexidade e nível de cuidado, determinando a responsabilidade técnica médica, as responsabilidades éticas, habilitações e atribuições da equipe médica necessária para seu adequado funcionamento. Brasília: Associação Brasileira de Mantenedoras de Ensino Superior. Disponível em: https://abmes.org.br/arquivos/legislacoes/resolucao-CFM-2271-2020-02-14.pdf. Acesso em: 13 fev. 2022.

BRASIL. **Resolução CIT n. 6, de 6 de novembro de 2013**. Dispõe sobre as regras para implantação de novos aplicativos, sistemas de informação em saúde ou novas versões de sistemas e aplicativos já existentes no âmbito do Sistema Único de Saúde (SUS) e que envolvam a sua utilização pelo Ministério da Saúde e Secretarias Estaduais, do Distrito Federal e Municipais de Saúde. Brasília: Ministério da Saúde, 2013. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/cit/2013/res0006_06_11_2013.html. Acesso em: 3 jul. 2023.

BRASIL. Resolução nº 466, de 12 de dezembro de 2012. A presente Resolução incorpora, sob a ótica do indivíduo e das coletividades, referenciais da bioética, tais como, autonomia, não maleficência, beneficência, justiça e equidade, dentre outros, e visa a assegurar os direitos e deveres que dizem respeito aos participantes da pesquisa, à comunidade científica e ao Estado. Projetos de pesquisa envolvendo seres humanos deverão atender a esta Resolução. Brasília: Presidência da República, 2012. Disponível em: https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf. Acesso em: 30 maio 2022.

BRASIL. Superior Tribunal de Justiça (Quarta Turma). Recurso Especial nº 22.337-8/RS. Serviço de proteção ao crédito. Cancelamento do registro. Prazo (cinco anos). O registro de dados pessoais no SPC deve ser cancelado apís cinco anos. Art. 43, do Código de Defesa do Consumidor (Lei 8.07890). Relator: Ministro Ruy Rosado de Aguiar. Brasília, 1995, p. 6119. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=199200114466&dt_pu. Acesso em: 12 jan. 2023.

BRASIL. Superior Tribunal de Justiça. Recurso Especial 159527 RJ. Sigilo medico. Ética médica. Prontuário. Clinica. Seguradora. Viola a ética médica a entrega de prontuário de paciente internadoa companhia seguradora responsável pelo reembolso das despesas. recurso conhecido e provido. Recorrido: Clínica Médica Cirurgica Botafogo S/A Hospital Samaritano. Relator: Min. Ruy Rosado de Aguiar, 29 de junho de 1998. Disponível em:

https://stj.jusbrasil.com.br/jurisprudencia/19853876/recurso-especial-resp-159527-rj-1997-0091690-1?ref=juris-tabs. Acesso em: 18 maio 2022.

BRASIL. Superior Tribunal de Justiça. REsp nº 1.533.019 – SP. Relator: Ministro Paulo de Tarso Sanseverino, Julgamento em 08/08/2017. 2017.

BRASIL. Supremo Tribunal Federal – STF. Ação Direta de Inconstitucionalidade – ADI 6387. Medida cautelar na ação direta de inconstitucionalidade 6.387 Distrito Federal. Relatora Ministra Rosa Weber. Brasília: STF, 2020. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 30 maio 2022.

BRASIL. Supremo Tribunal Federal – STF. Reclamação 2040 QO / DF - Distrito Federal questão de ordem na reclamação. Reclamação. Reclamante submetida ao processo de Extradição n.º 783, à disposição do STF. Relator: Ministro Néri da Silveira. Diário do Judiciário – DJ, v. 2116, p. 129, 2003.

BRASIL. Tribunal de Justiça do Distrito Federal (5ª Turma). Apelação Civel - Processo nº 0708698-23.2021.8.07.0009. Apelante(s): Elissandra de Melo e Silva e Hospital Santa Marta LTDA. Apelado(s) Hospital Santa Marta LTDA e Elissandra de Melo E Silva. Relator: Desembargador Fábio Eduardo Marques. Acórdão Nº 1616700. Diário do Jornal Eletrônico, Brasília: TJDF, 2022.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. (8ª Turma Cível). Agravo de instrumento 0702702-37.2022.8.07.0000. Agravo de instrumento. Ação de obrigação de fazer. Contrato de prestação de serviços. Empresas. Hospital e plano de saúde. Auditoria. Contas. Provas. Juntada de documentos médico-hospitalares. Pacientes. Sigilo. Lei geral de proteção de dados. Informações pessoais. Intimidade. Privacidade. Dados sensíveis. Proteção. Necessidade. Agravante: Servicos Hospitalares Yuge S.A. Agravado(s): Santa Luzia Assistencia Medica S/A. Relator: Desembargador Diaulas Costa Ribeiro. Acórdão Nº 1414740. Brasília: Poder Judiciário da União, 2022. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&controladorId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao. ControladorBuscaAcordao&visaoAnterior=tjdf.sistj.acordaoeletronico.buscaindexada. apresentacao.VisaoBuscaAcordao&nomeDaPagina=resultado&comando=abrirDadosDoAcordao&endereco DoServlet=sistj&historicoDePaginas=buscaLivre&quantidadeDeRegistros=20&baseSelecionada=BASE_ACORDAOS&numero Da UltimaPagina=1&buscaIndexada=1&mostrarPaginaSelecao TipoResultado=false&totalHits=1&internet=1&numeroDoDocumento= 1414740. Acesso em: 11 ago. 2022.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. (2ª Turma Cível). Apelação Cível n. Processo: 20151410079609APC (0008397-15.2015.8.07.0014). Direito civil, do consumidor e processual civil. Ação de conhecimento com preceito cominatório. Reparação por danos morais. Plano de saúde. Súmula 469, stj. Recusa

de cobertura de cirurgia bariátrica (gastroplastia redutora). Doença peexistente. Migração de plano de saúde. Carência. Cobertura parcial temporária. Não incidência. Danos morais. Cabimento. Recurso improvido. Apelante(s) : Bradesco Saúde S/A Apelado(s) : Daise Rodrigues de Franca Relator: Desembargador João Egmont. Acórdão n.: 1080743. Brasília: Poder Judiciário da União, 2018. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao. VisaoBuscaAcordao&controladorId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao. ControladorBuscaAcordao&visaoAnterior=tjdf.sistj.acordaoeletronico. buscaindexada.apresentacao. VisaoBuscaAcordao&nomeDaPagina=resultado&comando=abrir Dados DoAcordao&enderecoDoServlet=sistj&historicoDePaginas=buscaLivre&quantidade DeRegistros=20&baseSelecionada= BASE_ACORDAOS&numero DaUltimaPagina=1&buscaIndexada=1&mostrarPaginaSelecao TipoResultado=false& totalHits=1&internet=1&numeroDoDocumento=1080743. Acesso em: 11 ago. 2022.

BRASIL. Vacinômetro. Conselho Nacional de Saúde, Brasília: Ministério da Saúde, 2023. Dsponível em: https://conselho.saude.gov.br/vacinometro. Acesso em: 15 ago. 2023.

BRÜGGEMEIER, G. Protection of personality rights in the Law of delict/torts in Europe: mapping out paradigms. *In*: BRÜGGEMEIER, G.; CIACCHI, A. C.; O'CALLAGHAN, P. (ed.). Personality rights in european tort law. Cambridge: Cambridge University Press, 2010.

BUCCI, M. P. D. O conceito de política pública em direito. *In*: BUCCI, M. P. D. Políticas Públicas: Reflexões sobre o Conceito Jurídico. São Paulo: Saraiva, 2006.

CAMPOS, C. F. C.; FÍGARO, R. A Relação Médico-Paciente vista sob o Olhar da Comunicação e Trabalho. Revista Brasileira de Medicina de Família e Comunidade, Rio de Janeiro, v. 16, n. 43, p. 2352, 2021. Disponível em: https://rbmfc.org.br/rbmfc/article/view/2352. Acesso em: 11 ago. 2022.

CARVALHAES, Andréia R. Schneider Nunes. Limites e aferição do controle judicial de políticas públicas. Tese (Doutorado em Direito Político e Econômico)- Universidade Presbiteriana Mackenzie, São Paulo, 2018.

CASSIANO, A. P. C.; MARCOLAN, J. F.; SILVA, D. A. Atenção primária à saúde: estigma a indivíduos com transtornos mentais. Revista de enfermagem da UFPE on line, Pernambuco, v. 13, 2019. Disponível em: https://periodicos.ufpe.br/revistas/revistaenfermagem/article/view/239668. Acesso em: 29 mar. 2023.

CASTELLS, M. A sociedade em rede. 2. ed. Tradução: Roneide Venancio Majer. São Paulo: Editora Paz e Terra, 1999.

CASTILHO, R. Justiça Social e Distributiva: desafios para concretizar direitos sociais. São Paulo: Saraiva, 2009.

CAVALCANTE, R. B.; PINHEIRO, M. M. K. Política nacional de informação e

informática em saúde: avanços e limites atuais. Perspectivas em Gestão & Conhecimento, João Pessoa, v. 1, n. 2, p. 91- 104, jul./dez. 2011. Disponível em: https://cetic.br/media/docs/publicacoes/2/20211130124545/tic_saude_2021_livroeletronico.pdf. Acesso em: 12 ago. 2022.

CAVALIERI FILHO, S. Programa de Responsabilidade Civil. 14. ed. São Paulo: Atlas, 2020. E-book. Disponível em: http://primo-pmtna01.hosted.exlibrisgroup.com/PUC01:PUC01:sfx26800000000061280. Acesso em: 04 mar. 2023.

CETIC - CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2021. São Paulo: Comitê Gestor da Internet no Brasil, 2021. Disponível em: https://cetic.br/media/docs/publicacoes/2/15303120191017-

CHECK POINT. **Cyber Security Report**. San Carlos: CPR Check Point Research, 2022. Disponível em: https://resources.checkpoint.com/cyber-security-resources/2022-cyber-security-report. Acesso em: 17 mar. 2023.

CITRON, D. K.; PASQUALE, F. The scored society: Due process for automated predictions. Washington Law Review, v. 89, n. 1, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 12 jul. 2023.

CÓDIGO DE ÉTICA MÉDICA. Resolução CFM nº 2.217, de 27 de setembro de 2018. Modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019 / Conselho Federal de Medicina. Brasília: Conselho Federal de Medicina, 2019. 108 p.

CONECT SUS APLICATIVO. Nota informativa ao titular de dados de saúde. 2022. Disponível em: https://conectesus-paciente.saude.gov.br/menu/termo-uso. Acesso em: 17 maio 2022.

CONECT SUS APLICATIVO. Termos de Uso de Aplicativo e Políticas de Privacidade. 2022. Disponível em: https://conectesus-paciente.saude.gov.br/menu/termo-uso. Acesso em: 17 mai. 2022.

CONECT SUS. Plataforma de saúde para o cidadão, profissionais e gestores de saúde do Sistema Único de Saúde Brasileiro, 2022. Disponível em: https://conectesus.saude.gov.br/home. Acesso em: 22 jan. 2023.

CONSELHO FEDERAL DE MEDICINA (CFM - Brasil). Código de ética médica. Resolução nº 1.246/88. Brasília: Tablóide, 1990.

CONSELHO FEDERAL DE MEDICINA. Parecer CFM nº 5/2020. Informações médicas são sigilosas e privativas do paciente, sendo que sua divulgação somente ocorre com seu consentimento formal, exceto em cumprimento de determinação judicial, quando, nesse caso, o sigilo ficará sob a guarda do Juízo solicitante. Brasília: CFM, 2020.

CONSELHO FEDERAL DE MEDICINA. Recomendação CFM nº 1/2016. Dispõe

sobre o processo de obtenção de consentimento livre e esclarecido na assistência médica. Disponível: https://bit.ly/2Pokq4y. Acesso em 26 ago. 2022.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 1.021/1980. O Conselho Federal de Medicina usando da atribuição que lhe confere a Lei nº 3.268, de 30 de setembro de 1957, regulamentada pelo Decreto nº 44.045, de 19 de julho de 1958. Publicada no Diário Oficial da União, de 22 de outubro de 1980, Seção I, Parte II. Brasília, 1980. Disponível em: https://bit.ly/36Dc5nP. Acesso em 23 ago. 2022.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 2.314, de 20 de abril de 2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. 2022. Disponível: https://www.in.gov.br/en/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852. Acesso em 23 ago. 2022.

CORONAVÍRUS SUS vai rastrear contatos de infectados com COVID-19/. Convergência Digital, 2020. Disponível em: https://www.convergenciadigital.com.br/Internet-Movel/Coronavirus-SUS-vai-rastrear-contatos-de-infectados-com-COVID-19-54394.html?UserActiveTemplate=mobile%2Csite&s+id=17. Acesso em: 17 maio 2023.

COTS, M.; OLIVEIRA, R. Lei Geral de Proteção de Dados Pessoais comentada. 2. ed. São Paulo: Editora Revista dos Tribunais, 2019.

CUNHA, F. J. A. P. Gestão de documentos, aprendizagem e inovação organizacional em hospitais. Informação Arquivística, Rio de Janeiro, v. 3, n. 2, 2014. Disponível em: http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/106. Acesso em: 21 jul. 2022.

CUSPIS, A. I diritti della personalità. Milano: A. Giuffre, 1982.

DADOS DE PACIENTES da Unimed é exposto na Internet. Allus, São Paulo, 2022. Disponível em: https://alus.com.br/dados-de-pacientes-da-unimed-e-exposto-na-internet/. Acesso em: 12 jan. 2023.

DATASUS. Histórico. Datasus – Departamento de Informática do SUS, 2011. Disponível em: https://datasus.saude.gov.br/sobre-o-datasus/. Acesso em: 11 jul. 2022.

DERLEGA, V. J.; CHAIKIN, A. L. Privacy and Self-Disclosure in Social Relationships. Journal of Social Issues, [*S.l.*], v. 33, n. 3, p. 102–115. Disponível em: https://doi.org/10.1111/j.1540-4560.1977.tb01885.x. Acesso em: 9 mar. 2022.

DI PIETRO, M. S. Z. Direito administrativo. 35. ed. São Paulo: Forense, 2022.

DINIZ, M. H. Curso de Direito Civil Brasileiro: Teoria Geral do Direito Civil. V. 1, São Paulo: Saraiva, 2022.

DOMINGOS, P. O algoritmo mestre: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Novatec, 2017.

DONEDA, D. Da privacidade à proteção de dados: Fundamentos da Lei Geral de Proteção de Dados. 3. ed. Rio de Janeiro: Editora Revista dos Tribunais, 2021.

DONEDA, D. Privacidade e transparência no acesso à informação pública. *In*: MEZZAROBA, O.; GALINDO, F. Democracia eletrônica. Zaragoza: Prensas Universitarias de Zaragoza, 2010. p.179-216.

DWORKIN, R. Levando os direitos a sério. Tradução: Nelson Boeira. São Paulo: Martins Fontes, 2002. Coleção direito e justiça.

EUROPA. Diretiva Europeia 95/46/CE do Parlamento Europeu e do Conselho. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.Luxemburgo: Parlamento Europeu Pelo Conselho, 24 de outubro de 1995. Disponível em: https://www.conjur.com.br/dl/diretiva-europeia.pdf. Acesso em: 27 ago. 2021.

EUROPA. Para que serve o Regulamento Geral sobre a Proteção de Dados (RGPD)? Comissão Europeia, 2016. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pt#refer%C3%AAncia. Disponível em: 1 maio 2023.

EUROPA. The working party on the protection of individuals with regard to the processing of personal data. Article 29 Working Party. Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017. p. 5. Disponível em: https://ec.europa.eu/newsroom/article29/items/623051. Acesso em: 27 ago. 2021.

EUROPA. Tribunal de Justiça da União Europeia. Processo C-131/12, de 13 de maio de 2014. Disponível em: https://curia.europa.eu/juris/liste.jsf?language=pt&num=C-131/12. Acesso em: 30 maio 2022.

FABER, S.; Van GEENHUIZEN, M.; REUVER, M. eHealth adoption factors in medical hospitals: A focus on the Netherlands. International Journal of Medical Informatics, [*S.l.*], v. 100, 2017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1386505617300096. Acesso em: 27 ago. 2022.

FALSA SUSPEITA sobre coronavírus em Foz inunda as redes sociais. H2Foz, Foz do Iguaçu, 2020. Disponível em: https://www.h2foz.com.br/sem-categoria/falsa-suspeita-sobre-coronavirus-em-foz-inunda-as-redes-sociais/. Acesso em: 12 jul. 2023.

FARIAS, E. P. Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2. ed. Porto Alegre: Sergio Antônio Fabris, 2000.

FERNANDES, M. Os direitos da personalidade: estudos jurídicos em homenagem ao Professor Caio Mário da Silva Pereira. Rio de Janeiro: Forense, 1984.

FERNANDES, R. G.; OLIVEIRA, L. P. S. Notas Sobre o Papel Da Herança Histórica Brasileira Na "Expansão" Do Poder Judiciário No Domínio Das Políticas Públicas. **Revista Direitos Culturais**, Santo Ângelo, v. 15, n. 37, p. 123-143, 2020. Disponível

em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/205. Acesso em: 23 abr. 2023.

FERNANDES, R. V. C.; COSTA, H. A.; CARVALHO, A. G. P. (Coord.) Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia. Belo Horizonte: Fórum, 2018.

FERRAZ JÚNIOR, T. S. A liberdade como autonomia recíproca de acesso à informação. *In*: MARTINS, Ives Gandra da Silva; GRECO, Marco Aurélio. Direito e Internet: relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001.

FERRAZ JUNIOR, T. S. **Introdução ao estudo do direito**: técnica, decisão, dominação. São Paulo: Atlas, 2003.

FERREIRA, A. A. O Brasil e o preconceito: uma análise teórica e crítica da Lei 7.716/89 frente à realidade brasileira. Âmbito Jurídico, Rio Grande, v. XVIII, n. 134, 2015.

FERREIRA, K. P.; RODRIGUES, Y.G. S. A Privacidade no Ambiente Virtual: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil. Revista do Direito do Consumidor, São Paulo, v. 28, n. 122, p. 181-202, 2019. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/131407. Acesso em: 30 maio 2022.

FERREIRA, L. R. G. Filosofia da Edição Genômica: reducionismo e experimentalismo em engenharia genética. 2022. Dissertação (Mestrado em Filosofia) - Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2022. Disponível em: https://doi.org/10.11606/D.8.2022.tde-28072022-180905. Acesso em: 11 maio 2023.

FINCK, M.; PALLAS, F. They who must not be identified: distinguishing personal from non-personal data under the GDPR. International Data Privacy Law, Oxford, v. 10, n. 1, p. 11-36, 2020. Disponível em: https://doi.org/10.1093/idpl/ipz026. Acesso em: 30 maio 2022.

FRANÇA, G. V. Comentários ao Código de Ética Médica. 7. ed. Rio de Janeiro: Grupo Gen, 2019.

FREEDMAN, D.; PISANI, R.; PURVES, R. Statistics. 4. ed. New York: W. W. Norton & Company, 2007.

FREITAS FILHO, R.; LIMA, T. M. Metodologia de Análise de Decisões – MAD. Universitas Jus, Brasília, n. 21, p. 1-17, jul./dez. 2010.

GAGLIANO, P. S.; PAMPLONA FILHO, R. M. V. Novo curso de direito civil: responsabilidade civil. 20. ed. São Paulo: SaraivaJur, 2022.

GALEFFI, D. A. Ética, privacidade e confidencialidade de informação em saúde. Informação em Pauta, Fortaleza, v. 5, n. especial, 2020. Disponível em: http://hdl.handle.net/20.500.11959/brapci/136594. Acesso em: 16 mar. 2023.

GAVA, M. LGPD para PME: minoria está totalmente adequada à legislação. Capterra, 2021. Disponível em: https://www.capterra.com.br/blog/2153/lgpd-pme. Acesso em: 22 dez. 2022.

GELLER, L. Current developments in genetic discrimination. *In*: ALPER, J. *et al* (Eds.). The doubleedged helix: social implications of genetics in a diverse society. Baltimore: The Johns Hopkins University Press, 2002.

GIL, A. C. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 2002.

GOFFMAN, E. Estigma: notas sobre a manipulação da identidade deteriorada. Rio de Janeiro: Zahar; 1982.

GOLDSCHMIDT, R.; PASSOS, E.; BEZERRA, E. Data mining: conceitos, técnicas, algoritmos, orientações e aplicações. Rio de Janeiro: Elsevier, 2015.

GONÇALVES, C. R. Direito Civil Brasileiro: responsabilidade civil. 16. ed. São Paulo: Editora Saraiva, 2021.

GONÇALVES, L. H. N.; *et al*. Dimensões subjetivas na Saúde Digital. Liinc em Revista, [*S.l.*], v. 18, n. 2, p. e6053, 2022. Disponível em: https://revista.ibict.br/liinc/article/view/6053. Acesso em: 15 jul. 2023.

GONÇALVES, L. H. N.; *et al*. Dimensões subjetivas na Saúde Digital. **Liinc em Revista**, [*S.l.*], v. 18, n. 2, p. e6053, 2022. Disponível em: https://revista.ibict.br/liinc/article/view/6053. Acesso em: 15 jul. 2023.

GONÇALVES, M. J. Adoção da tecnologia da informação em saúde sob a perspectiva do custo efetividade. 2019. 91 f. Dissertação (Mestrado em Engenharia Mecânica) - Centro Universitário FEI, São Bernardo do Campo, 2019. Disponível em: https://doi.org/10.31414/EM.2019.D.131097. Acesso em: 10 mar. 2022.

GONZÁLES, C. A. A.; MAMANI, S. L. Q. O dano existencial como contribuição da cultura jurídica italiana. Tradução: Fabiano Coulon. Canoas: Redes: Revista Eletrônica Direito e Sociedade, v. 6., n. 1, 2018.

GPO – GOVERNMENT PUBLISHING OFFICE. Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (usa patriot act) act of 2001. Congressional Record, Whashington, v. 147, 2001. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf. Acesso em: 14 fev. 2023.

GUEDES, C.; DINIZ, D. Um caso de discriminação genética: o traço falciforme no Brasil. Physis: Revista de Saúde Coletiva, Rio de Janeiro, v. 17, n. 3, p. 501-520, 2007. Disponível em: https://www.scielo.br/j/physis/a/HjmCfLJtKbMLBSdNZF3STSK/?format=pdf&lang=pt. Acesso em: 13 jan. 2023.

GUEDES, G. S. C.; MEIRELES, R. M. V. "Término do tratamento de dados". *In*:

Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoas. 2. ed. São Paulo: Editora RT, 2019.

GUEDES, P. Discriminação tecnológica: desmistificando a neutralidade da Inteligência Artificial em meio à crise de inclusão e de diversidade nas tecnologias emergentes. ITS Rio - Grupo de Pesquisa de Direito do Instituto de Tecnologia e Sociedade, Rio de Janeiro, 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/10/Discriminação-tecnológica_Paula_Guedes.pdf. Acesso em: 14 abr.2023.

HAMMERSCHMIDT, D.; OLIVEIRA, J. S. Direito à Intimidade Genética: um contributo ao estudo dos direitos da personalidade. Revista Jurídica Cesumar, Maringá, v. 6. n. 1. p. 421-455, 2006. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/320. Acesso em: 29 jun. 2023.

HANNAH, J. K.; BALL, M. J.; EDWARDS, M. J. A. Introdução a Informática em Enfermagem. 3. ed. Porto Alegre: Editora Artmed.

HINTZBERGEN, J. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport; 2018. Disponível em: https://pt.scribd.com/books. Acesso em 13 ago. 2022.

HUMMEL, G. Fatos e ações tecnológicas para mitigar o COVID-19. Digital Healthcare Hospitalar, 2020. Disponível em: https://digital.hospitalar.com/pt-br/ti-inovao/fatos-e-aes-tecnolgicas-para-mitigar-o-COVID-19. Acesso em: 11 jul. 2020.

INTI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC. Brasília: INTI, 2017. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/plano-diretor-de-tecnologia-da-informacao-e-comunicacao-pdtic. Acesso em: 12 jul. 2023.

JULIÃO, F. A cada 7 segundos, uma tentativa de fraude é registrada no Brasil; saiba se proteger. **CNN Brasil**, São Paulo, 2022. Disponível em: https://www.cnnbrasil.com.br/economia/a-cada-7-segundos-uma-tentativa-de-fraude-e-registrada-no-brasil-saiba-seproteger/#:~:text=Um%20levantamento%20da%20Serasa%20Experian,4%2C9%25%20nos%20casos. Acesso em: 22 jul. 2022.

KAY, J.; KING, M. Radical Uncertainty. Decision-making beyond the numbers. New York: W.W. Norton & Company, 2020.

LEME, R. S.; BLANK, M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. Cadernos IberoAmericanos de Direito Sanitário, Brasília, v. 9, n. 3, p. 210-224, 2020. Disponível em: https://doi.org/10.17566/ciads.v9i3.690. Acesso em: 29 ago. 2022.

LEONARDI, M. Tutela e privacidade na internet. São Paulo: Editora Saraiva, 2011.

LETTIERI, G. K. *et al*. Sigilo médico na era digital: análise da relação médico-paciente. Revista Bioética, Brasília, v. 29, n. 4. 2021. Disponível em: https://doi.org/10.1590/1983-

80422021294515. Acesso em: 20 ago. 2022.

LIMA NETO, F. V. O direito de não sofrer discriminação genética: uma nova expressão dos direitos de personalidade. Rio de Janeiro: Lumen Juris, 2008.

LINS, R. G. S. O consentimento e o tratamento de informações pessoais de trabalhadores subordinados: uma análise sob a ótica da proteção cooperativa de dados pessoais. 2021. 173f. Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Norte, Natal, 2021.

LOCATELI, C. C.; PANDOLFO, A. C. A intimidade genética: direito à intimidade e à informação na proteção dos dados genéticos. Revista do CEJUR/TJSC: Prestação Jurisdicional, Florianópolis, v. 1, n. 2, p. 92-119, 2014. Disponível em: https://doi.org/10.37497/revistacejur.v1i2.67. Acesso em: 13 abr. 2023.

LUPTON, D. The commodification of patient opinion: the digital patient experience economy in the age of big data. Sociology of Health & Illness, [*S.l.*], v. 36, n. 6, p. 856-869, 2014. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1467-9566.12109. Acesso em: 13 abr. 2023.

MACEDO, S. R. S. A gestão documental de prontuário do paciente em saúde pública municipal em Aracaju: da situação real para a ideal e sua inovação. 2019. 138 f. Dissertação (Mestrado Profissional em Gestão da Informação e do Conhecimento) - Universidade Federal de Sergipe, São Cristóvão, 2019.

MAIS DE 33 MILHÕES de brasileiros não têm acesso à internet, diz pesquisa. G1 Portal, São Paulo, 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/03/21/mais-de-33-milhoes-de-brasileiros-nao-tem-acesso-a-internet-diz-pesquisa.ghtml. Acesso em: 14 fev. 2023.

MARQUES, M. Grupo fraudava empréstimos de até R$ 500 mil com dados de servidores federais no DF; três foram presos. G1, São Paulo, 2019. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/01/09/grupo-fraudava-emprestimos-de-ate-r-500-mil-com-dados-de-servidores-federais-no-df-tres-foram-presos.ghtml. Acesso em: 29 mar. 2023.

MARTINS, A. Direito ao Esquecimento de Dados de Saúde. *In*: DALLARI, A.; MONACO, G. LGPD na Saúde. São Paulo: Editora Revista dos Tribunais, 2021.

MARTINS, L. (org.) Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005.

MARTINS, P. B. L. Dados pessoais sensíveis e inferências. DTIBR, 2019. Disponível em: https://www.dtibr.com/post/dados-pessoais-sens%C3%ADveis-einfer%C3%AAncias. Acesso em: 7 jun. 2022.

MASSIGNAM, F. M.; BASTOS, J. L. D.; NEDEL, F. B. Discriminação e saúde: um problema de acesso. Epidemiologia e Serviço de Saúde, v. 24, n. 3, p. 544-541, 2015.

Disponível em: http://dx.doi.org/10.5123/S1679-49742015000300020. Acesso em: 7 jun. 2022.

MATEUS, F. M. Q.; MENDONÇA, M. C. Machine learning na melhoria de processos internos: estudos de caso na indústria de varejo brasileira. 2020. 106 fl. Projeto de Graduação (Bacharel em Engenharia)- Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020.

MATSUMOTO, M. M. S. Seus dados médicos estão mais expostos do que você imagina: considerações sobre a questão da privacidade de dados de saúde, quem tem acesso a eles e quais os impactos para a saúde e inovação. IPEA - Centro de Pesquisa em Ciência, Tecnologia e Sociedade, Rio de Janeiro, 2020. Disponível em: https://www.ipea.gov.br/cts/pt/central-de-conteudo/artigos/artigos/105-seus-dados-medicos-estao-mais-expostos-do-que-voce-imagina Acesso em 24 maio 2023.

MEIRELLES, A. T. Medicina e Direito: Informação e Compreensão como pressupostos fundamentais à interface harmônica. CVMed – Direito Médico Comentado, [*S.l.*], 2019. Disponível em: http://cvmed.com.br/2019/09/16/medicina-e-direito-informacao-e-compreensao-como-pressupostos-fundamentais-a-interface-harmonica/. Acesso em: 08 mai 2022.

MEIRELLES, H. L. Direito Administrativo Brasileiro. 42. ed. São Paulo: Malheiros, 2016.

MELLO, C. A. B. Conteúdo jurídico do princípio da igualdade. 3. ed. São Paulo: Malheiros, 2017.

MELLO, C. A. B. Vazamento de dados na saúde coloca pacientes na mira de golpes. Medicina S/A, São Paulo, 2022. Disponível em: https://medicinasa.com.br/vazamento-dados-saude/. Acesso em: 30 ago. 2022.. Curso de direito administrativo. 35. ed. São Paulo: Malheiros, 2021.

MELO, A. N. Dano moral coletivo nas relações de consumo: aplicabilidade da função punitiva do dano. Rio de Janeiro: Lumen Juris, 2018.

MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. Revista de Ciências Jurídicas Pensar, Fortaleza, v. 25, n. 4, 2020. Disponível em: https://periodicos.unifor.br/rpen/article/view/10828/pdf. Acesso em 22 mai. 2023.

MENDES, L. S. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, L. S.; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. São Paulo: Revista dos Tribunais, v. 120, 2018, p. 469-483, nov.-dez.2018.

MENDES, L. S.; MATIUZZO, M. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. RDU, Porto Alegre, v. 16, n. 90, p. 39-64, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20

Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 17 jun. 2023.

MINAS GERAIS. Tribunal de Justiça e Minas Gerais - TJ-MG (5ª Câmara Cível). AC: 10000230016917001 MG. Relator: Áurea Brasil, Data de Julgamento: 02/03/2023, Câmaras Cíveis, 2023.

MINAYO, M. C. S. Análise qualitativa: teoria, passos e fidedignidade. Ciência & Saúde Coletiva, Rio de Janeiro, v. 17, n. 3, 2012, p. 621-626. Disponível em: https://www.scielo.br/j/csc/a/39YW8sMQhNzG5NmpGBtNMFf/?format=pdf&lang= pt. Acesso em: 30 set. 2022.

MINOSSI, J. G.; SILVA, A. L. Medicina defensiva: uma prática necessária? Revista do Colégio Brasileiro de Cirurgiões, Rio de Janeiro, v. 40, n. 6, p. 494-501, 2013. Disponível em: https://doi.org/10.1590/S0100-69912013000600013. Acesso em: 20 jul. 2023.

MORAES, M. C. B. Apresentação. *In*: RODOTÁ, S. A vida na sociedade de vigilância: privacidade hoje. Rio de Janeiro: Renovar,2008.

MORAES, M. C. B. Danos à Pessoa Humana: uma leitura civil - constitucional dos danos morais. Rio de janeiro: Renovar, 2009.

MOURA JÚNIOR, L. A. A Estratégia de Saúde Digital para o Brasil 2020 - 2028. Journal of Health Informatics, [*S.l.*], v. 13, n. 1, 2021. Disponível em: https://docs.bvsalud.org/biblioref/2022/03/1361371/editorial.pdf. Acesso em: 14 jun 2023.

MULHOLLAND, C. S. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? Migalhas, São Paulo, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso: 11. mar. 2023.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei nº 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, p. 159-180, 29 dez. 2018. Disponível em. http://dx.doi.org/10.18759/rdgf.v19i3.1603. Acesso: 11. mar. 2023.

MULHOLLAND, C.; GOMES, R. Encarregado empregado problemas de responsabilidade civil na LGPD. Migalhas de responsabilidade Civil, São Paulo, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de responsabilidadecivil/347010/encarregado-empregado-problemas-de-responsabilidade-civil-na-lgpd. Acesso em: 17 maio 2023.

MYSSIOR, B. A. P. A.; SILVA, L. E. G. Discriminação genética: uma questão jurídica ou biológica? Revista de Biodireito e Direito dos Animais, Curitiba, v. 2, n. 2, p. 159-174, 2016. Disponível em: f https://www.indexlaw.org/index.php/revistarbda/article/download/1381/pdf. Acesso em: 17 maio 2023.

NASCIMENTO, J. C. H. B. et al. (2020). Inteligência artificial na saúde e a proteção

de dados: reflexos na crise COVID-19. Revista Brasileira De Direitos Fundamentais & Justiça, Belo Horizonte, v. 14, n. 1, p. 207–230. Disponível em: https://doi.org/10.30899/dfj.v0i0.964. Acesso em: 11 mar. 2023.

NAVEGA, L. Expansão da Responsabilidade Civil Objetiva: Análise da (In)Adequação da Inserção no Ordenamento Jurídico de uma Cláusula Geral de Responsabilidade Objetiva. Revista do Ministério Público do Estado do Rio de Janeiro, Rio de Janeiro, n. 66, p. 109-127, 2017. Disponível em: https://www.mprj.mp.br/documents/20184/1246489/Leandro_Navega.pdf. Acesso em: 15 mar. 2021.

NAVES, B. T.O. Direitos de Personalidade e Dados Genéticos: Revisão crítico-discursiva dos direitos de personalidade à luz da natureza jurídica dos dados genéticos humanos. Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC. 2010.

NEGRI, S. M. C. Á.; KORKMAZ, M. R. D. C. R. A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana. Revista de Direito, Governança e Novas Tecnologias, Goiânia, v. 5, n. 1, p. 63-85, 2019. Disponível em https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 20 jun.2022.

NHS. We're here for you. 2023. Disponível em: https://www.nhs.uk/. Acesso em: 17 jun. 2023.

NISHIOKA, S. A. Confinamento (lockdown) na pandemia por COVID-19: ter\ês experiências, três interpretações. UNASUS, 2022. Disponível em: https://www.unasus.gov.br/especial/covid19/markdown/554. Avesso em: 17 jul. 2022.

NOVA FALHA do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. G1, 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 17 jul. 2022.

NOVAKOSKI, A. L. M.; NASPOLINI, S. H. D. F. Responsabilidade civil na LGPD: problemas e soluções. Conpedi Law Review, Florianópolis, v. 6, n. 1, 2020. Disponível em: https://indexlaw.org/index.php/conpedireview/article/view/7024. Acesso em: 18 fev. 2023.

NUNES, A. R. S. Políticas públicas. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017, Tomo: Direitos Difusos e Coletivos. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/376/edicao-1/politicas-publicas. Acesso em: 18 fev. 2023.

O PESADELO DOS PACIENTES chantageados após vazamento das sessões de terapia. G1, São Paulo, 2020. Disponível em: https://g1.globo.com/mundo/noticia/2020/10/27/o-pesadelo-dos-pacientes-chantageados-apos-vazamento-das-sessoes-de-terapia.ghtml. Acesso em: 2 jun 2023.

ODS – OFFICIAL DOCUMENTS SYSTEM OF THE UNITED STATE. Un Human

Rights Council. ODS, 2019. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/197/47/PDF/N2119747.pdf?OpenElement. Acesso em: 2 jun 2023.

OHL, N. G.; ANGELUCCI, C. B.; NICOLAU, A. M.; HONDA, C. Escolarização e preconceito: lembranças de jovens com e sem deficiência. Revista da Associação Brasileira de Psicologia Escolar e Educacional(ABRAPEE), São Paulo, v. 13, n. 2, p. 243-250, 2009.

OHM, P. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review, Rochester, v. 57, p. 1701-1777, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em: 20 jun. 2023.

OLIVEIRA, C. E. G. Credit scoring e big data no regime jurídico brasileiro. *In*: FERNANDES, R. V. C.; COSTA, H. A.; CARVALHO, A. G. P. (coord.). Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia – 2017. Belo Horizonte: Fórum, 2018, p. 223-240.

OLIVEIRA, J. N.; AMARAL, L. O papel da qualidade da informação nos sistemas de informação. *In*: CONFERÊNCIA ESPECIALIZADA EM SISTEMAS E TECNOLOGIAS DE INFORMAÇÃO, Lisboa, 1999. Anais [...] Sistemas e Tecnologias de Informação: Desafios para o Século XXI", Lisboa, 1999. Disponível em: https://repositorium.sdum.uminho.pt/handle/1822/2183. Acesso em: 11 ago. 2022.

OMS - ORGANIZAÇÃO MUNDIAL DA SAÚDE. Global strategy on digital health 2020-2025. Genebra: OMS; 2021.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Brasília: Unesco, 1948. Disponível em: http://unesdoc.unesco.org/images/0013/001394/139423por.pdf. Acesso em: 9 mar. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, CIÊNCIA E CULTURA. [Internet]. Declaração Universal sobre Bioética e Direitos Humanos. Paris: Unesco; 2006 Disponível: http://unesdoc.unesco.org/images/0014/001461/146180por.pdf. Acesso em 14 ago. 2022.

PACETE, L. G. Dados de saúde valem mais que informações financeiras na dark web. Forber, São Paulo, 2022. Disponível em: https://forbes.com.br/forbes-tech/2022/06/dados-de-saude-chegam-a-valer-mais-que-informacoes-financeiras-na-dark-web/. Acesso em: 22 jun. 2023.

PASQUALE, F. Redescribing Health Privacy: The Importance of Information Policy (November 3, 2015). Houston Journal of Health Law and Policy, Vol. 14. Disponível em: https://ssrn.com/abstract=2685696. Acesso em: 12 jun. 2022.

PINHEIRO, P. P. Pandemia: gestão de crise e proteção dos dados pessoais. *In*: PALHARES, F. (org.). Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil, 2020.

PIPER, D. *et al*. The impact of patient safety culture on handover in rural health facilities. BMC Health Services Research, [*S.l.*], v. 18, n.1, p.889, 2018. Disponível em: https://www.ncbi.nlm.nih.gov/pubmed/30477488. Acesso em 30 ago. 2022.

PORTES, R. Indústria 4.0: entenda o que é a quarta revolução industrial. Startse, 2021. Disponível em: https://www.startse.com/artigos/industria-40-entenda-o-que-e-a-quarta-revolucao-industrial/. Acesso em: 30 ago. 2022.

PORTUGAL. Convenção para a Protecção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina. Oviedo: Gabinete de Documentação e Direito Comparado. Procuradoria Geral da República, 1997.

PORTUGAL. Lei n.º 12/2005, de 26 de janeiro. Informação genética pessoal e informação de saúde. Lisboa: Assembleia da República; Procuradoria Geral de Lisboa, 2005. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1660&tabela=leis. Acesso em: 30 ago. 2022.

QUADROS, C. A. T.; VICTORA, C. G.; COSTA, J. S. D. Coverage and focus of a cervical cancer prevention program in southern Brazil. Revista Pan American Journal of Public Health, v. 16, n. 4, 2004. Disponível em: https://www.scielosp.org/pdf/rpsp/2004.v16n4/223-232. Acesso em: 30 ago. 2022.

RAYMOND, E. S. The new hack's dictionary (the jargon file). 3. ed. Cambridge: The MIT Press, 1996.

REBELO, T. Por que os profissionais e empresas de saúde precisam se adequar à Lei Geral de Proteção de Dados?. Revista Jus Navigandi, Teresina, ano 24, n. 5860, 2019. Disponível em: https://jus.com.br/artigos/74825. Acesso em: 15 ago. 2023..

REQUIÃO, M.; COSTA, D. C. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, Rio de Janeiro, a. 11, n. 3, 2022. Disponível em: http://civilistica.com/discriminacaoalgoritmica/. Acesso em: 19 maio 2023.

REZENDE, E. J. C.; *et al*. Ética e telessaúde: reflexões para uma prática segura. Revista Panamericana de Salud Publica, São Paulo, v. 28, n. 1, p. 58-65, 2010. Disponível em: https://scielosp.org/pdf/rpsp/2010.v28n1/58-65/pt. Acesso em: 27 jul. 2022.

RGPD - REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Acesso em: 19 maio 2023.

RIO DE JANEIRO Tribunal de Justiça do Rio de Janeiro - TJ-RJ (21ª Câmara Cível). Apelação - APL: 00313968920168190208. Relator: Des(a). REGINA LUCIA PASSOS, Data de Julgamento: 09/07/2020, 2020.

RODOTÀ, S. A vida na sociedade de vigilância: privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES, M.; *et al*. Diferenciais na adequação das informações de eventos vitais nos municípios de Pernambuco, 2006-2008. Revista Brasileira de Epidemiologia, São Paulo, v. 15, n. 2, 2012. Disponível em: https://doi.org/10.1590/S1415-790X2012000200005. Acesso em: 22 jul. 2022.

RODRIGUES, P. M. A inteligência artificial médica e o uso de dados pessoais no atendimento aos pacientes. Migalhas, São Paulo, 2020. Disponível em: https://www.migalhas.com.br/depeso/ 325245/a-inteligencia-artificial-medica-e-o-uso-de-dados-pessoais-no-atendimento-aos-pacientes. Acesso em: 08 jul. 2022.

ROSSI, A. T. Direito ao esquecimento e a decisão do STF no RE 1.010.606/RJ. Migalhas, São Paulo, 2021. Disponível em: https://www.migalhas.com.br/depeso/340982/direito-ao-esquecimento-e-a-decisao-do-stf-no-re-1-010-606-rj. Acesso em: 30 ago. 2022.

SALDANHA, R. F. Da aquisição à visualização de dados: aplicações da ciência de dados em saúde. 2021. 167f. Tese (Doutorado em Informação e Comunicação em Saúde)-Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, Fundação Oswaldo Cruz, Rio de Janeiro, 2021.

SANDRIN, P. J. P. B.; SILVA, J. X. R. Possíveis reflexos penais da Lei Geral de Proteção de Dados. Migalhas, São Paulo, 2020. Disponível em: https://www.migalhas.com.br/depeso/320959/possiveis-reflexos-penais-da-lei-geral-de-protecao-de-dados. Acesso em: 16 jun. 2023.

SANTOS, L. N. Biodireito E Princípios Bioéticos Fundamentais. Revista Clóvis Moura de Humanidades, Teresina, v. 5, n. 1, 2019. Disponível em: https://www.tjpi.jus.br/revistaejud/index.php/escolajudiciariapiaui/article/download/105/93/409. Acesso em: 22 jan. 2023.

SANTOS, Lirton Nogueira. Biodireito e Princípios Bioéticos Fundamentais. Revista Clóvis Moura de Humanidades. v.5, nº 1. Teresina-PI: UESPI, 2019.

SÃO PAULO. Procuradoria-Geral do Estado de São Paulo. TJSP reconhece legalidade do Sistema de Monitora-mento Inteligente (SIMI). São Paulo: PGE, 2020. Disponível em: http://www.pge.sp.gov.br/visualizanoticia.aspx?id=4175. Acesso em: 8 jul. 2020

SÃO PAULO. Tribunal de Contas do Estado de São Paulo. Resolução nº 03/2020, de 29 de março de 2020. Dispõe sobre a redução do número de processos e otimização da tramitação dos feitos pelo Tribunal de Contas do Estado de São Paulo. São Paulo: TCESP, 2020. Disponível em: https://www.tce.sp.gov.br/sites/default/files/legislacao/RESOLUCAO-03-2020.pdf. Acesso em: 22 jan. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Apelação Cível nº 1016844-03.2020.8.26.0068 - TJ/SP**. o, informações essas de fácil acesso. Ausência de senha de acesso que torna a informação, na prática, pública. O vazamento do prontuário

médico do requerente (fls. 31/35), ao indicar ser ele portador do vírus do HIV, gerou situação embaraçosa e degradante no ambiente de trabalho. A responsabilidade civil objetiva exige apenas a ocorrência do dano, a existência de nexo causal entre a conduta e este dano e a ausência de culpa excludente da vítima (art. 37, § 6º CF). O sigilo dos dados pessoais ganha contornos cada vez mais sensíveis, sendo matéria cada dia mais regulada na seara legislativa. Eventuais vazamentos de dados particulares são evidentes fatos geradores de danos, seja de ordem moral ou material, e o legislador tende a protegê-los, especialmente quando digam respeito aos direitos de personalidade. Art. 5º, X, Constituição Federal, art. 42 da Lei nº 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018. Danos morais configurados. Quantum indenizatório majorado. Danos materiais não configurados. Ausência de prova de nexo de causalidade entre a exposição dos dados médicos e a efetiva demissão do autor. Honorários advocatícios readequados. Recurso do autor parcialmente provido. Recurso do réu desprovido. Relator(a): Heloísa Mimessi. São Paulo: Tribunal de Justiça de São Paulo. Disponível em: https://esaj.tjsp.jus.br/cjsg/resultadoSimples.do;jsessionid=AE02A84D72A777156E9E282400D39571.cjsg2?conversationId=&nuProcOrigem=+1016844-03.2020.8.26.0068.&nuRegistro=. Acesso em 12 de julho de 2023.

SARLET, G. B. S.; CALDEIRA, C. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. Civilistica.com – Revista Eletrônica de Direito Civil, Rio de Janeiro, v. 8, n. 1, 29 abr. 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 22 jan. 2023.

SARLET, I. W.; KEINERT, T. M. M. O direito fundamental à privacidade e as informações em saúde: alguns desafios. *In*: KEINERT, T. M. M.; et al. (Orgs.). Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

SARLET, I. W.; MOLINARO, C. A. Direito à informação e direito de acesso à informação como direitos fundamentais na constituição brasileira. Revista da AGU, Brasília, ano XIII, n. 42, p. 9-38, out./dez. 2014. Disponível em: https://doi.org/10.25109/2525-328X.v.13.n.42.2014.542. Acesso em 30 ago. 2022.

SCHREIBER, A. Direitos da Personalidade. Rio de Janeiro: Atlas, 2011.

SCHREIBER, A. Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais: Tratado de Proteção de Dados Pessoais. São Paulo: Editora Forense, 2020.

SECCHI, L. Políticas Públicas: conceitos, esquemas de análise, casos práticos. São Paulo: Cengage Learning, 2012.

SETZER, V. W. Dado, Informação, Conhecimento e Competência. Data Grama Zero - Revista de Ciência da Informação, v. 0, n. 0, 2015. Disponível em: https://www.ime.usp.br/~vwsetzer/dado-info.html. Acesso em 30 ago. 2022.

SHIPPERS, L. M. Algoritmos que discriminam: uma análise jurídica da discriminação

no âmbito das decisões automatizadas e seus mitigadores. Monografia (Bacharel em Direito)- Fundação Getúlio Vargas, São Paulo. 2018.

SILVA, D. F.; OLIVEIRA, M. L. Epidemiologia da COVID-19: comparação entre boletins epidemiológicos. Comunicação em Ciências da Saúde, Brasília, v. 31, n. 1, 2020. Disponível em: http://10.233.90.10:8080/jspui/handle/prefix/188. Acesso em: 11 abr. 2023.

SILVA, H. O. Uma abordagem baseada em anonimização para privacidade de dados em plataformas analíticas. 2019. 117 f. Dissertação (Mestrado em Tecnologia)– Universidade Estadual de Campinas, Limeira, 2019.

SILVEIRA, S. A. Segurança da informação e proteção de pessoas: estudo de caso e proposta de dados de governança para serviços de saúde. 2021. Dissertação (Mestrado Profissional em Inovação Tecnológica) - Universidade Federal de São Paulo, São José dos Campos, 2021.

SIQUEIRA, M. C. Gestão Estratégica da Informação. Rio de Janeiro: Brasport, 2005.

SISTEMA DE RECONHECIMENTO facial da PM do RJ falha, e mulher é detida por engano. G1, Rio de Janeiro, 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 23 jun. 2023.

SONDA, F. T. A sociedade em rede e a informação em saúde: um direito em construção no Brasil. Revista da Defensoria Pública do Estado do Rio Grande do Sul, Porto Alegre, n. 24, 2019. Disponível em: https://revista.defensoria.rs.def.br/defensoria/article/view/72. Acesso em: 30 ago. 2022.

SPÍNOLA, L. M. C. O Compliance no Setor Saúde. Revistas de Ciências Médicas e Biológicas, Salvador, v. 16, n. 2, p131-132, maio/ago. 2017. Disponível em: https://doi.org/10.9771/cmbio.v16i2.24558. Acesso em: 30 ago. 2022.

STROME, T. Healthcare analytics for quality and performance improvement. Hobbken: John Wiley & Sons; 2013.

SURFSHARK. Data breach statistics by country: first quarter of 2022. Q1'2022 data breach statistics by origin, TOP 20, 2022. Disponível em: https://surfshark.com/blog/data-breach-statistics-by-country. Acesso em: 28 ago. 2022.

SZTAJN, R. A responsabilidade civil do médico: visão bioética. Revista de direito mercantil, industrial, econômico e financeiro, São Paulo, v. 36, n. 108, 1997. Disponível em https://repositorio.usp.br/item/000986240. Acesso em 16 mai. 2022.

TASSO, F. A. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 97-115, 2020. Disponível em: http://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf?

d=637250344175953621. Acesso em: 30 mar. 2023.

TAURION, C. Big data. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2013.

TEPEDINO, G.; TERRA, A. M. V.; GUEDES, G. S. C. Fundamentos do direito civil: responsabilidade civil. 2. ed. Rio de Janeiro: Forense, 2021. E-book. Disponível em: http://primopmtna01.hosted.exlibrisgroup.com/PUC01:PUC01:sfx26800000000062157. Acesso em: 6 mar. 2023.

TREVIZAN, T. C.; SILVA, V. B. O dano social como reflexo das novas tendências da responsabilidade civil. Revista Científica-Faculdade Pio XII, Campo Grande, v. 6, 2007.

UNESCO - ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, CIÊNCIA E CULTURA. Declaração internacional sobre os dados genéticos humanos. Portugal: Unesco, 2004. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_inter_dados_genericos.pdf. Acesso em Acesso em: 29 jun. 2023.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Seção). Parecer ECLI:EU:C:2017:592. 26 jul. 2017. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2017%3A592. Acesso em: 15 jun. 2022.

UNITED STATES. Annual report pursuant to section 13 or 15(d) of the securities exchange act of 1934. Washington D.C.: Securities and Exchange Commission, 2022. Disponível em: https://www.checkpoint.com/downloads/investor/2021-CHKP-form-20F.pdf. Acesso em: 15 jun. 2022.

VAINZOF, R. Disposições preliminares. *In*: BLUM, R. O.; MALDONADO, V. N. (coord.). LGPD – Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019.

VALENTIM, M. L. P. Informação e conhecimento em organizações complexas. *In:* VALENTIN, M. (org.). Gestão da informação e do conhecimento no âmbito da ciência da informação. São Paulo: Polis, 2008.

VENOSA, S. S. Direito Civil: obrigações e responsabilidade civil. 21. ed., v. 2. São Paulo: Atlas, 2021. E-book. Disponível em: http://primopmtna01.hosted.exlibrisgroup.com/PUC01:PUC01:sfx26800000000062317. Acesso em: 3 jun 2023.

WANG, R. Y.; STRONG, D. M. Beyond accuracy: what data qaulity means to data consumers. Journal of management information systems, [*S.l.*], v. 12, n. 4, 1996. Disponível em: http://mitiq.mit.edu/documents/publications/tdqmpub/14_beyond_accuracy.pdf. Acesso em: 15 jun. 2022.

WANSSA, M. C. D. Autonomia versus beneficência. Revista Bioética, Brasília, v. 19, n. 1, p. 105-117, 2011. Disponível em: https://revistabioetica.cfm.org.br/index.php/revista_bioetica/article/download/611/627. Acesso em: 6 maio 2022.

WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. Harvard Law Review,

New York, v. 4, n. 5, dec. 1890. Disponível em: http://www.jstor.org/stable/1321160. Acesso em: 06 abr. 2022.

WEN, C. L. Telemedicina e Telessaúde: oportunidade de novos serviços e da melhoria da logística em saúde. **Revista Panorama Hospitalar**, [*S. l.*], p. 24-26, 2015. Disponível em: https://nuvemdoconhecimento.org.br/wp-content/uploads/2015/03/03132015_Revista_Panorama_Hospitalar_Fev_2015_pag24a26.pdf. Acesso em: 14 maio 2023.

WHO - WORLD HEALTH ORGANIZATION. Coronavirus disease (COVID-19) pandemic. WHO, 2019. Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019. Acesso em 20 ago. 2022.

WHO - WORLD HEALTH ORGANIZATION. World health statistics 2012. Geneva: World Health Organization, 2012. Disponível em: https://apps.who.int/iris/handle/10665/44844. Acesso em: 25 jan. 2023.

Anexos

Anexo 1 - Política de privacidade

Como anexo, propõe-se a leitura da Política de Privacidade apresenta da aos usuários do aplicativo "Conecte SUS", afim de exemplificar como as regras e conceitos da LGPD tem sido utilizadas em via prática e do quadro resumo das ações propostas nas Estratégias de Saúde Digital para o Brasil 2017.



Política de Privacidade

Quais informações estão presentes neste documento?

Nesta Política de Privacidade, o usuário do Aplicativo encontrará informações sobre: o funcionamento do serviço e as regras aplicáveis a ele; o arcabouço legal relacionado à prestação do serviço; as responsabilidades do usuário ao utilizar o serviço; as responsabilidades da administração pública ao prover o serviço; informações para contato, caso exista alguma dúvida ou seja necessário atualizar informações; e o foro responsável por eventuais reclamações caso questões desta Política tenham sido violadas.

Além disso, na Política de Privacidade, o usuário do Aplicativo encontrará informações sobre: qual o tratamento dos dados pessoais realizados, de forma automatizada ou não, e a sua finalidade; os dados pessoais dos usuários necessários para a prestação do serviço; a forma como eles são coletados; se há o compartilhamento de dados com terceiros; e quais as medidas de segurança implementadas para proteger os dados.

Aceitação da Política de Privacidade

Ao utilizar os serviços, o usuário confirma que leu e compreendeu as Políticas aplicáveis ao Aplicativo e concorda em ficar vinculado a eles.

Definições

Para melhor compreensão deste documento, nesta Política de Privacidade, consideram-se: Agentes de tratamento: o controlador e o operador.

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

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.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Encarregado de Dados: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O Ministério da Saúde não tem um encarregado nomeado até o presente momento.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entes privados. Lei Geral de Proteção de Dados: Lei Federal n. 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger

os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Usuários (ou "Usuário", quando individualmente considerado): todas as pessoas naturais que utilizarem o Aplicativo.

ANPD: autoridade nacional de proteção de dados pessoais é órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Quais são as leis e normativos aplicáveis a esse serviço?

- Lei nº 12.527, de 18 de novembro de 2011: Lei de Acesso à Informação – Regula o acesso a informações previsto na Constituição Federal.
- Lei nº 13.460, de 26 de junho de 2017: Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.
- Lei nº 13.709, de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- Decreto nº 7.724, de 16 de maio de 2012: Regulamenta a Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso a informações previsto na Constituição.
- Lei nº 13.853, de 8 de julho de 2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.
- Decreto nº 10.046, de 09 de outubro de 2019: Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
- Decreto nº 9.637, de 26 de dezembro de 2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.
- Portaria GM/MS nº 69, de 14 de Janeiro de 2021: Institui a obrigatoriedade de registro de aplicação de vacinas contra a COVID-19 nos sistemas de informação do Ministério da Saúde.
- Portaria GM/MS nº 1.434, de 28 de maio de 2020: Institui o Aplicativo e

altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde.

- Portaria GM/MS nº 1.792, de 17 de julho de 2020: Altera a Portaria nº 356/GM/MS, de 11 de março de 2020, para dispor sobre a obrigatoriedade de notificação ao Ministério da Saúde de todos os resultados de testes diagnóstico para SARS-CoV-2 realizados por laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional.
- Portaria GM/MS nº 1.768, de 30 de julho de 2021: Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS).
- Portaria GM/MS nº 3.632, de 21 de dezembro de 2020: Altera a Portaria de Consolidação GM/MS nº 1, de 28 de setembro de 2017, para instituir a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28)

Descrição do serviço

O aplicativo oficial do Ministério da Saúde que permite ao cidadão acompanhar na palma de sua mão o seu histórico clínico, a partir das informações de saúde do Sistema Único de Saúde (SUS). Atualmente o aplicativo apresenta o registro de vacinas aplicadas e exames laboratoriais de COVID-19 realizados, internações, medicamentos dispensados e, mais recentemente, permite a emissão do Certificado Nacional de Vacinação COVID-19. Os dados do aplicativo são em sua maioria provenientes da Rede Nacional de Dados em Saúde (RNDS), plataforma nacional de interoperabilidade de dados em saúde, que integra diferentes sistemas de informação alimentados por profissionais de saúde. Instituída pela portaria GM/MS n. 1.434, de 28 de maio de 2020, a Rede é um projeto estruturante do programa do Governo Federal para a transformação digital da saúde no Brasil e tem o objetivo de promover a troca de informações entre os pontos da Rede de Atenção à Saúde, permitindo a transição e continuidade do cuidado nos setores público e privado.

Quais são os direitos do usuário do serviço?

O usuário do serviço possui os seguintes direitos, conferidos pela Lei de Proteção de Dados Pessoais:

- **Direito de confirmação e acesso (Art. 18, I e II):** é o direito do usuário de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais.

- **Direito de retificação** (Art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.
- **Direito à limitação do tratamento dos dados** (Art. 18, IV): é o direito do usuário de limitar o tratamento de seus dados pessoais, podendo exigir a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados.
- **Direito de oposição (Art. 18, § 2º):** é o direito do usuário de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados.
- **Direito de portabilidade dos dados (Art. 18, V):** é o direito do usuário de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
- **Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD):** o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Quais são as obrigações dos usuários que utilizam o serviço?

O usuário se responsabiliza pela precisão e veracidade dos dados informados e reconhece que a inconsistência destes poderá implicar a impossibilidade de se utilizar Aplicativo. Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e não os de terceiros. O login e senha só poderão ser utilizados pelo usuário cadastrado. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento. O usuário do serviço é responsável pela atualização das suas informações pessoais e consequências na omissão ou erros nas informações pessoais cadastradas. Não é possível realizar retificação de informação pelo Aplicativo, salvo aquelas consideradas como "Registros e Contatos", que se referem a informações auto declaradas de Índice de Massa Corpórea (IMC), Alergias, Pressão Arterial, Glicose e Doações de Sangue. Dados cadastrais, como nome, data de nascimento, sexo, e-mail, inclusão/exclusão de nome social, são recebidos pelo sistema Cadastro Nacional de Usuários do SUS - CadSUS, onde, a partir do Cartão Nacional de Saúde – CNS, são validados com as

informações disponíveis na Receita Federal. Para a correção desses dados, o cidadão deverá atualizar as informações na Receita Federal e/ou solicitar junto a qualquer estabelecimento de saúde (Alteração de dados na Receita Federal pode ser realizado em: https://servicos.receita.fazenda.gov.br/Servicos/CPF/alterar/default.asp). Os dados de saúde são inseridos nos sistemas de informação diretamente por profissionais de saúde, nos estabelecimentos assistenciais. A visualização das informações no Aplicativo é possível após o devido envio destes dados à Rede Nacional de Dados em Saúde (RNDS). Para qualquer tipo de correção e alteração de dados de saúde, deve-se entrar em contato com o estabelecimento onde foi realizada a ação ou serviço de saúde, ou secretaria estadual ou municipal de saúde e solicitar a correção do registro. Compete ao gestor local de saúde, responsável pela coleta dos dados, a correção de dados incompletos, inexatos ou desatualizados, requisitada pelo cidadão, conforme Inciso III do Art. 18 da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais.

O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública, a qualquer outro Usuário, ou, ainda, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nesta Política de Privacidade ou de qualquer ato praticado a partir de seu acesso ao serviço.

- O Órgão não poderá ser responsabilizado pelos seguintes fatos:
  a. Equipamento infectado ou invadido por atacantes;
  b. Equipamento avariado no momento do consumo de serviços;
  c. Proteção do computador;
  d. Proteção das informações baseadas nos computadores dos usuários;
  e. Abuso de uso dos computadores dos usuários;
  f. Monitoração clandestina do computador dos usuários;
  g. Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;
  h. Perímetro inseguro;

O uso comercial das expressões utilizadas em aplicativos como marca, nome empresarial ou nome de domínio, além dos conteúdos do serviço, assim como os programas, bancos de dados, redes, arquivos que permitem que o usuário acesse sua conta estão protegidos pelas leis e tratados internacionais de direito autoral, marcas, patentes, modelos e desenhos industriais. Ao acessar o aplicativo, os usuários declaram que irão respeitar todos os direitos de propriedade intelectual e os decorrentes da proteção de marcas, patentes e/ou desenhos industriais, depositados ou registrados em, bem como todos os direitos referentes

a terceiros que porventura estejam, ou estiverem de alguma forma, disponíveis no serviço. O simples acesso ao serviço não confere aos usuários qualquer direito ao uso dos nomes, títulos, palavras, frases, marcas, patentes, imagens, dados e informações, dentre outras, que nele estejam ou estiverem disponíveis.

A reprodução de conteúdo descritos anteriormente está proibida, salvo com prévia autorização por escrito ou caso se destinem ao uso exclusivamente pessoal e sem que em nenhuma circunstância os usuários adquiram qualquer direito sobre esses conteúdos.

É vedada a utilização do serviço para finalidades comerciais, publicitárias ou qualquer outra que contrarie a finalidade para a qual foi concebido, conforme definido neste documento, sob pena de sujeição às sanções cabíveis na Lei nº 9.610/1998, que protege os direitos autorais no Brasil.

Os visitantes e usuários assumem toda e qualquer responsabilidade, de caráter civil e/ou criminal, pela utilização indevida das informações, textos, gráficos, marcas, imagens, enfim, todo e qualquer direito de propriedade intelectual ou industrial do serviço. Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

Quais são as responsabilidades da administração pública com meus dados?

A Administração Pública, no papel de custodiante das informações pessoais dos Usuários, deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados na plataforma. Publicar e informar ao Usuário as futuras alterações a esta Política de Privacidade por meio do sítio (https://sso.acesso.gov.br/), conforme o princípio da publicidade estabelecido no artigo 37, caput, da Constituição Federal.

Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário. Em hipótese alguma, o serviço e seus colaboradores responsabilizam-se por eventuais danos diretos, indiretos, emergentes, especiais, imprevistos ou multas causadas, em qualquer matéria de responsabilidade, seja contratual, objetiva ou civil (inclusive

negligência ou outras), decorrentes de qualquer forma de uso do serviço, mesmo que advertida a possibilidade de tais danos.

Tendo em vista que o serviço lida com informações pessoais, o usuário concorda que não usará robôs, sistemas de varredura e armazenamento de dados (como "spiders" ou "scrapers"), links escondidos ou qualquer outro recurso escuso, ferramenta, programa, algoritmo ou método coletor/extrator de dados automático para acessar, adquirir, copiar ou monitorar o serviço, sem permissão expressa por escrito do órgão. Em se tratando de aplicativos em dispositivos móveis sua comercialização é expressamente proibida. Ao concordar com esta Política e utilizar o aplicativo móvel, o usuário receberá uma permissão do órgão para uso não comercial dos serviços oferecidos pelo aplicativo, o que, em nenhuma hipótese, fará dele proprietário do aplicativo móvel.

Caso o usuário descumpra a Política de Privacidade, ou seja investigado em razão de má conduta, o órgão poderá restringir seu acesso. O usuário também deverá responder legalmente por essa conduta.

A Administração Pública poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações ou tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço ou de outra forma necessária para cumprir com as obrigações legais. Caso ocorra, a Administração Pública notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.
A Administração pública se compromete a preservar a funcionalidade do serviço ou aplicativo, utilizando um layout que respeite a usabilidade e navegabilidade, facilitando a navegação sempre que possível, e exibir as funcionalidades de maneira completa, precisa e suficiente, de modo que as operações realizadas no serviço sejam claras.

Qual o contato pelo qual o usuário do serviço pode tirar suas dúvidas?

Caso o usuário tenha alguma dúvida sobre esta Política de Privacidade, ele poderá entrar em contato pelo e-mail suporte.conectesus@saude.gov.br.

Esta Política de Privacidade foi elaborada em conformidade com a Lei Federal n. 12.965 de 23 de abril de 2014 (Marco Civil da Internet) e com a Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados Pessoais).

Esta Política de Privacidade poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual se convida o usuário a consultar periodicamente esta seção.

O site se compromete a cumprir as normas previstas na Lei Geral de Proteção de Dados (LGPD), e respeitar os princípios dispostos no Art. 6º:

- **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.

Agentes de tratamento

A quem compete as decisões referentes ao tratamento de dados pessoais realizado no Aplicativo (Controlador)?

A Lei Geral de Proteção de Dados define como controlador, em seu artigo 5º:

Art. 5º, VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Para o Aplicativo, as decisões referentes ao tratamento de dados pessoais são de responsabilidade do Ministério da Saúde.

Endereço: Ministério da Saúde - Esplanada dos Ministérios Bloco G, Zona Cívico-Administrativa, Brasília - DF - CEP 70058900.

E-mail: datasus@saude.gov.br.

Telefone: 61 3315 3900.

As secretarias municipais e estaduais de saúde exercem o papel de controladores de dados, devido as mesmas terem suas próprias legislações e realizarem também o tratamento de dados de saúde.

Quem realiza o tratamento de dados (Operador)?

A Lei Geral de Proteção de Dados define como operador, em seu artigo 5º: Art. 5º, VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Para o Aplicativo, o Controlador Ministério da Saúde também atua como operador, ou seja, além de ser responsável pelas decisões referentes ao tratamento de dados pessoais, também realiza o tratamento de dados pessoais.
O Aplicativo compartilha dados com uma empresa terceirizada, desenvolvedora da aplicação, sendo assim, é um operador de dados. Todos os controles administrativos e lógicos de segurança foram exigidos à empresa terceirizada. O Aplicativo armazena seus dados em nuvem privada, sendo assim o serviço de nuvem também se configura como operador de dados.

Quais dados pessoais são tratados pelo serviço?

A utilização, pelo usuário, de determinadas funcionalidades do serviço dependerá do tratamento dos seguintes dados pessoais:

- Nome completo
- Data de nascimento
- Sexo
- Filiação
- Nacionalidade
- Número de inscrição no CPF
- Endereço de e-mail
- Endereço
- Número de telefone
- Localização do usuário

- Foto do usuário
- Dados de Saúde (Alergias, IMC, Pressão Arterial, Glicose, Doações de Sangue)
- Vacinação COVID-19
- Resultado de Exame COVID-19
- Internações Hospitalares
- Contatos de emergência e de profissionais de saúde (Nome e Telefone)
- Medicamentos Dispensados (Programa Farmácia Popular)
- Situação Cadastral no Sistema Nacional de Transplantes

O Aplicativo realiza o tratamento de dados de crianças e adolescentes e se compromete a fornecer maior proteção a esses dados. Além disso, o Aplicativo se compromete a cumprir todas as disposições legais pertinentes, como o Estatuto da Criança e do Adolescente. Alguns recursos ou informações, quando necessários pela primeira vez ou mesmo na instalação, serão solicitados por este aplicativo e notificados por meio do sistema operacional do seu dispositivo móvel, por exemplo:

- Acesso à rede (internet móvel ou WiFi);
- Acesso à identificação do dispositivo;
- Acesso à câmera e fotos, mídia e arquivos de áudio e vídeo de seu aparelho.

Como os dados são coletados?

- **Nome completo:** Obtido de terceiros (Login Único, Cadastro Nacional de Usuários do SUS - CADSUS)
- **Data de nascimento**
- **Sexo**
- **Filiação:** Obtido de terceiros (CADSUS)
- **Nacionalidade:** Obtido de terceiros (CADSUS)
- **Número de inscrição no CPF:** Obtido de terceiros (CADSUS)
- **Endereço de e-mail:** Obtido de terceiros (CADSUS)
- **Endereço:** Obtido de terceiros (CADSUS)
- **Número de telefone:** Obtido de terceiros (CADSUS)
- **Localização do usuário:** Obtida pelo dispositivo de acesso, após autorização do usuário
- **Foto do usuário:** câmera e fotos, mídia e arquivos de áudio e vídeo do dispositivo, após autorização do usuário
- **Dados de Saúde (Alergias, IMC, Pressão, Glicose, Doações de Sangue):** Informado pelo usuário
- **Vacinação COVID-19:** Obtido de terceiros (Rede Nacional de Dados em Saúde - RNDS)
- **Resultado de Exame COVID-19:** Obtido de terceiros (RNDS)
- **Internações Hospitalares:** Obtido de terceiros (RNDS)

- **Contatos de emergência e de profissionais de saúde (Nome e Telefone):** Informado pelo usuário
- **Medicamentos Dispensados (Programa Farmácia Popular – Sistema Horus):** Obtido de terceiros
- **Situação Cadastral no Sistema Nacional de Transplantes:** Obtido de terceiros (Sistema Nacional de Transplantes)

Para que fim utilizamos seus dados?

- Nome completo : O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação COVID-19.
- Data de nascimento : O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação COVID-19.
- Sexo : O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação COVID-19.
- Filiação : O dado é necessário para melhorar e personalizar a experiência do usuário. O aplicativo permite adicionar outras contas. O nome da mãe é apresentado na Carteira Nacional de Vacinação e no Certificado Nacional de Vacinação COVID-19.
- Nacionalidade: O dado é necessário para identificação do usuário dentro do serviço, e apresentado nos documentos de Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação COVID-19.
- Número de inscrição no CPF: O dado é necessário para manter o usuário logado.
- Endereço de e-mail: O dado é necessário para identificação do usuário dentro do serviço e envio de notificações.
- Endereço: O dado é necessário para identificação do usuário dentro do serviço.
- Número de telefone: O dado é necessário para envio de notificações.
- Localização do usuário: O dado é necessário para melhorar e personalizar a experiência do usuário. A localização do usuário é acionada na funcionalidade Serviços que apresenta a geolocalização dos estabelecimentos de saúde mais próximos. Dado opcional.
- Foto do usuário: O dado é necessário para melhorar e personalizar a experiência do usuário no menu do aplicativo. A câmera e fotos, mídia e arquivos de áudio e vídeo do dispositivo também é utilizada para escanear códigos QR para autenticação e validação dos documentos emitidos pelo aplicativo.
- Dados de Saúde (Alergias, IMC, Pressão, Glicose, Doações de Sangue): O

dado é necessário para melhorar e personalizar a experiência do usuário. Dados registrados pelo próprio usuário.

- Vacinação COVID-19: O dado é necessário para melhorar e personalizar a experiência do usuário. São dados da RNDS, coletados por profissionais de saúde nos serviços de vacinação, sob gestão de secretarias municipal ou estadual de saúde. Dados: nome da vacina; tipo de dose aplicada; data da vacinação; número do lote da vacina; nome do fabricante; identificação do vacinador; e identificação do serviço de vacinação.
- Resultado de Exame COVID-19: O dado é necessário para melhorar e personalizar a experiência do usuário. Dados da RNDS, coletados por profissionais de saúde de laboratórios da rede pública, rede privada, universitários e quaisquer outros, em todo território nacional.
- Internações Hospitalares: O dado é necessário para melhorar e personalizar a experiência do usuário. Dados da RNDS, coletados por profissionais de saúde da atenção hospitalar.
- Contatos de emergência e de profissionais de saúde (Nome e Telefone): O dado é necessário para melhorar e personalizar a experiência do usuário. Dados registrados pelo próprio usuário.
- Medicamentos Dispensados (Programa Farmácia Popular e Sistema Horus): O dado é necessário para melhorar e personalizar a experiência do usuário. Dados coletados por profissionais de saúde para dispensação de medicamento do Programa Farmácia Popular.
- Situação Cadastral no Sistema Nacional de Transplantes: O dado é necessário para melhorar e personalizar a experiência do usuário. Dados coletados pelas Secretarias Estaduais de Transplantes (Centrais Estaduais de Transplantes) que apresentam informações sobre o status e posição do usuário na lista de espera para transplante de órgão e tecido.

Qual o tratamento realizado com os dados pessoais?

- Nome Completo: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Data De Nascimento: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Sexo: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Filiação: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle,

Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção

- Nacionalidade: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Número de Inscrição no CPF: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Endereço de e-mail: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Endereço: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Número De Telefone: Acesso, Armazenamento, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Localização Do Usuário: Acesso, Coleta
- Foto Do Usuário: Acesso, Coleta
- Dados De Saúde (Alergias, IMC, Pressão, Glicose, Doações De Sangue): Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Vacinação COVID-19: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Resultado De Exame COVID-19: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Internações Hospitalares: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Contatos De Emergência E De Profissionais De Saúde (Nome E Telefone): Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Medicamentos Dispensados (Programa Farmácia Popular e Sistema Horus): Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão, Distribuição, Eliminação, Extração, Processamento, Produção, Recepção
- Situação Cadastral No Sistema Nacional De Transplantes: Acesso, Armazenamento, Avaliação, Coleta, Comunicação, Controle, Difusão,

Distribuição, Eliminação, Extração, Processamento, Produção, Recepção

Os dados pessoais utilizados no serviço são compartilhados?

Os dados pessoais do usuário poderão ser compartilhados com as seguintes pessoas ou empresas: Secretarias Estaduais e Municipais de Saúde, Agência Nacional de Vigilância Sanitária (ANVISA), Controladoria-Geral da União (CGU), Tribunal de Contas da união (TCU), Operador que desenvolve o Aplicativo e o serviço de nuvem que armazena os dados.

Segurança no tratamento dos dados pessoais do usuário

O Aplicativo se compromete a aplicar as medidas técnicas e organizativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão de tais dados.

Para a garantia da segurança, serão adotadas soluções que levem em consideração: as técnicas adequadas; os custos de aplicação; a natureza, o âmbito, o contexto e as finalidades do tratamento; e os riscos para os direitos e liberdades do usuário.

O site utiliza criptografia para que os dados sejam transmitidos de forma segura e confidencial, de maneira que a transmissão dos dados entre o servidor e o usuário, e em retroalimentação, ocorra de maneira totalmente cifrada ou encriptada.

No entanto, o site se exime de responsabilidade por culpa exclusiva de terceiro, como em caso de ataque de hackers ou crackers, ou culpa exclusiva do usuário, como no caso em que ele mesmo transfere seus dados a terceiro. O Aplicativo se compromete, ainda, a comunicar o usuário em prazo adequado caso ocorra algum tipo de violação da segurança de seus dados pessoais que possa lhe causar um alto risco para seus direitos e liberdades pessoais.

A violação de dados pessoais é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Por fim, o site se compromete a tratar os dados pessoais do usuário com confidencialidade, dentro dos limites legais.

O Aplicativo utiliza cookies?

Cookies são pequenos arquivos de texto enviados pelo site ao computador do usuário e que nele ficam armazenados, com informações relacionadas à navegação do site. Por meio dos cookies, pequenas quantidades de informação são armazenadas

pelo navegador do usuário para que nosso servidor possa lê-las posteriormente. Podem ser armazenados, por exemplo, dados sobre o dispositivo utilizado pelo usuário, bem como seu local e horário de acesso ao site.

É importante ressaltar que nem todo cookie contém dados pessoais do usuário, já que determinados tipos de cookies podem ser utilizados somente para que o serviço funcione corretamente.

As informações eventualmente armazenadas em cookies também são consideradas dados pessoais e todas as regras previstas nesta Política de Privacidade também são aplicáveis a eles.

O Aplicativo não utiliza cookies.

Esta Política de Privacidade pode ser alterada?

A presente versão desta Política de Privacidade foi atualizada pela última vez em: 12/08/2021.

O editor se reserva o direito de modificar, a qualquer momento o site as presentes normas, especialmente para adaptá-las às evoluções do Aplicativo, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Qualquer alteração e/ou atualização desta Política de Privacidade passará a vigorar a partir da data de sua publicação no sítio do serviço e deverá ser integralmente observada pelos Usuários.

Qual o foro aplicável caso o usuário queira realizar alguma reclamação?

Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm direito a apresentar reclamação à Autoridade Nacional de Proteção de Dados. Este Termo será regido pela legislação brasileira. Qualquer reclamação ou controvérsia com base neste Termo será dirimida exclusivamente pela Justiça Federal, na seção judiciária do domicílio do usuário, por previsão do artigo 109, §§ 1º, 2º e 3º, da Constituição Federal.

Anexo 2 - Resumo das ações propostas na estratégia de saúde digital

Quadro - Resumo das Ações Propostas na Estratégia de Saúde Digital para o Brasil 2017

Ação Estratégica	Objetivo	Resultados Esperados
Reduzir a fragmentação das iniciativas no SUS e aprimorar a governança da estratégia de e-Saúde	Fortalecer as instâncias de governança da informação no SUS/MS e promover o alinhamento das suas ações. Organizar o ambiente de implantação da Visão de e-Saúde. Construir um arcabouço institucional capaz de orquestrar as inúmeras ações em curso no âmbito da e-Saúde.	Redução das barreiras para interoperabilidade entre os sistemas; Redução da instabilidade administrativa a cada ciclo de gestão; Existência de ambiente favorável à definição de políticas e a gestão de mudanças; Estratégia de construção coletiva de e-Saúde consolidada; Uso corrente de melhores práticas para a construção da e- Saúde.
Fortalecer a intersetorialidade de governança de e-Saúde	Dar uma dimensão nacional à Visão de e-Saúde para o Brasil, integrando programas e agregando recursos de todos os setores de governo, da sociedade civil e da iniciativa privada para viabilizar a Visão de e-Saúde proposta neste documento.	Ações intersetoriais desenvolvidas para viabilizar a Visão de e-Saúde; Alinhamento estratégico dos programas de governo, com definição de investimento para e-Saúde; Rede Nacional de Centros de Pesquisa e Ensino em e-Saúde consolidada como componente complexo de P&D em e-Saúde; Existência de entidades de referência consolidadas para os demais componentes de e-Saúde; Modelos definidos e avaliados para a gestão de investimento em e-Saúde: pesquisa, inovação, manutenção, infraestrutura, e eixos correlacionados; Existência de cultura e prática de intersetorialidade das ações governamentais; Estratégia de construção coletiva de e-Saúde consolidada.
Elaborar o marco legal de e-Saúde no País	Adequar o marco legal para suportar as inovações do campo da atenção à saúde	Existência de um marco legal para e-Saúde, flexível e robusto, capaz de suportar o modelo de governança descentralizada, característica fundamental do SUS; Existência de legislação que favoreça o desenvolvimento das ações estratégicas propostas; Existência de interlocução permanente com a sociedade, por meio do qual os descompassos entre os avanços tecnológicos e a legislação são equacionados e tratados de maneira sistemática; Redução dos custos decorrentes de liminares judiciais por de ausência de legislação; Redução da ingerência na gestão das informações de saúde; Existência de condições legais para o investimento necessário à

		implantação da e-Saúde no país; Clareza regulatória para o planejamento e investimento de longo prazo; □ Garantia da privacidade e proteção contra o uso indevido.
Definir e implantar uma arquitetura para a e-Saúde	Construir uma arquitetura de e- Saúde composta ao menos pelos seguintes blocos reutilizáveis: Modelos de informação e artefatos de conhecimento, modelo para interoperabilidade de serviços de terminologia, cadastros nacionais de identificação, consentimento, serviços e sistemas de segurança e privacidade, e arquitetura de intercâmbio de informações de saúde.	□ Arquitetura de e-Saúde definida em blocos construtores em uso corrente pelas três esferas de governo e iniciativa privada, após ter sido exaustivamente avaliada em ambientes controlados; □ Acesso ao RES e a outros serviços e sistemas de e-Saúde é feito de rotina, em ambiente seguro, com respeito à privacidade do indivíduo e trânsito intenso de dados clínicos com foco nos suporte à atenção.
Definir e implantar os sistemas e serviços de e-Saúde	Garantir que a infraestrutura computacional, necessária para a implantação da Visão de e-Saúde para o Brasil, esteja disponível e evolua de acordo com as necessidades e oportunidades advindas da evolução tecnológica.	Infraestrutura computacional □ adequada à demanda de e-Saúde; □ Infraestrutura de gestão de TIC ampliada, compatível com o alcance proposto para a e-Saúde e baseada em melhores práticas de mercado; □ Utilização da infraestrutura proposta pelo Plano Nacional de Banda Larga (PNLB) para atender as necessidades de e-Saúde; □ Infraestrutura computacional adequada para disponibilizar os serviços de segurança, identificação e autenticação, necessários para a e-Saúde; □ Infraestrutura adequada para a coleta e armazenamento de dados individualizados para a e-Saúde; □ Racionalização do investimento por meio da prática de compartilhamento responsável de recursos de infraestrutura entre os entes do SUS.
Criar arquitetura de referência para sustentação dos serviços de infraestrutura	Desenvolver e estabelecer uma arquitetura de referência para infraestrutura, visando à plena sustentação dos serviços de TIC para e-Saúde.	Arquitetura tecnológica de referência para infraestrutura □ definida, testada e validada, oferecida como modelo para todos os atores da saúde, com amplo respaldo da legislação da cultura e da prática de gestão de TI.
Criar a certificação em e-Saúde para trabalhadores do SUS	Implantar um processo de certificação baseado na formação e atualização profissional em e-Saúde no SUS, como fator estruturante e orientador da qualificação dos profissionais do SUS para a implantação da Visão de e-Saúde.	Carreira do profissional de e-Saúde, cargos, funções e salários, □ criada testada e validada; e-Saúde reconhecida como área do conhecimento e de P&D pelos os órgãos de fomento à pesquisa; Existência de uma base legal e normativa para e-Saúde; Cultura □ de articulação e interlocução com os conselhos e representação de classe para a promoção das boas práticas da e-Saúde;

		□ Publicação da política de RH para e-Saúde, a partir da PNIIS, e considerando as diferenças regionais; □ Base de conhecimento em uso corrente a partir dos documentos de referência de RH para e-Saúde; □ Cultura implantada de moni toramento e avaliação (M&A) das práticas de e-Saúde dos profissionais; □ Perfis profissionais de e-Saúde definidos e em uso, nos cadastros nacionais de profissionais do SUS; □ Existência de redes consolidadas de colaboração entre produtores, entre usuários, e entre produtores e usuários.
Promover a facilitação do acesso à informação em saúde para a população	Implantar recursos de e-Saúde que promovam a facilitação do acesso da população à informação em saúde de qualidade, estimulando o acesso à informação em saúde para a população.	□ Existência de uma variedade de recursos de e-Saúde, acessados por usuários, profissionais, e gestores que buscam informação em saúde; □ Presença da e-Saúde no dia a dia da mídia aberta, tanto na TV como na mídia impressa e *on-line*; □ Presença da e-Saúde na mídia interna das organizações de saúde; □ Redes colaborativas como Telessaúde Brasil, RUTE, RHEMO, e outras, promovem a e- Saúde de forma consistente e sistemática; □ O Portal do Cidadão é considerado útil pelo cidadão e pelo paciente.